COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.**Do not** submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Mr. Dennis Kalma	
Organization:	Alberta Electric System Operator	
Telephone:	403-539-2584	
Email:	dennis.kalma@aeso.ca	
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT**	☐	1 - Transmission Owners

☐ **ECAR** ☐ **FRCC** ☐ **MAAC** ☐ **MAIN** ☐ **MAPP** ☐ **NPCC** ☐ **SERC** ☐ **SPP** ☒ **WECC** ☐ **NA - Not Applicable**	☒	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this

standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes
☒ No
Comments
See attached document.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes
☒ No

If No, what are the most significant issues the drafting team must reconsider?
See attached document

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
All comments in attached document.

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 subnetworks (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 resulted in an incident, are known to cause, or could have resulted in, an incident.	**Comments** **FAQ was an excellent document. It was the best part of all. In some cases we could not understand the standard without reference to the FAQ. Maybe something lacking the standard.** **The standard does not identify "key cyber personnel" nor contemplate any assurance measures around them.** **We would like to see a better definition here for Incident. Should the words Major/minor be used here?**

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~~ Interconnection, or would cause significant risk to public health and safety. Those critical bulk electric system assets include assets performing the following:	Suggest use of Interconnection rather than electric grid for consistency among other reliability standards.

(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.	The FAQ doesn't reflect this section very well. FAQ should better define the electronic perimeter in substations.
(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 riskbased 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.	We would like to see some guidance in the FAQ about how to handle any negative results from a background check especially suggested tolerance levels. We find it unusual that with this level of scrutiny, the standard has not addressed random drug and alcohol testing of serving employees.
(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.	For Canada – Social Insurance Number (SIN)
(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.	The team needs to reconsider this part in view of the volume of work associated to this section.

(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).	Should the standard refer to the remaining two sides not referred to here, i.e.: the roof and the floor?
(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 nonproduction 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 semiannually. 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.	Compliance in legacy systems may not be possible and replacement systems may be the only solution.
(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 ensure ~~review~~ access permissions are reviewed within 5 working days. For involuntary terminations, management must review access permissions within no more than 24 hours.	It is not reasonable to expect a manager to sit at a terminal or otherwise review all access permissions.

(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.	Should contain specific retention periods.
(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 operator, 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 90 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.	90 days would be consistent with other sections and more reasonable.

(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 90 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.	90 days would be consistent with other sections and more reasonable.
(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.	

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Bill Wagner	
Organization:	Calpine	
Telephone:	916-608-3799	
Email:	wwagner@calpine.com	
NERC Region		**Registered Ballot Body Segment**
☒ **ERCOT** ☒ **ECAR** ☒ **FRCC** ☒ **MAAC** ☒ **MAIN** ☒ **MAPP** ☒ **NPCC** ☒ **SERC** ☒ **SPP** ☒ **WECC** ☐ **NA - Not Applicable**	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☒	3 - Load-serving Entities
	☒	4 - Transmission-dependent Utilities
	☒	5 - Electric Generators
	☒	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☒ Yes

☐ No

Comments

I recommend including more information regarding definitions and/or reference to definitions, at least in the FAQ's if not in the standard itself. For example include document links to the following definitions: Functional Model, Bulk Electric System Asset, Interconnection Reliability Operating Limits (IROL), NERC Policy 1.B, guidance for background checks, risk-based assessment methodology.

Identifying specific definitions provides important context from which to interpret the appropriate application of the standard. Even in the event of multiple definitions, e.g., Bulk Electric System Asset, identifying the applicable definition for this standard provides the reference point from which to interpret the authors intent.

Question 2: Do you believe this standard is ready to go to ballot?

☒ Yes

☐ No

If No, what are the most significant issues the drafting team must reconsider?
I agree with the Requirements and Measures sections. There are several editorial errors (e.g., erroreous list numberings), and the Compliance Monitoring and Levels of Noncompliance sections are very different between all of the sections. This makes for a very awkward if not impractical standard to actually audit and enforce.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
Page 3, Section 1301 Security Management Controls, (a) Requirements, (2) Information Protection, (i) Identification: Add requirement/clarification for meaningfully identifying information. For example, if a row in a database table records information about a critical cyber asset, must that row be idnetified in any specific way, or is it sufficient to simply say that information is documented in the asset inventory database?

Page 3, Section 1301 Security Management Controls, subsection (3) Roles and Responsibilities, I recommend using critical cyber asset administrator rather than custodian to refer to someone that is responsible for day-to-day operation of the cyber asset (i.e., making sure the computer stays up and running, has adequate disc space, backups are made, etc.).

Page 4, Section 1301 Security Management Controls, (a) Requirements (5) Access Authorization (iv) Access Revocation/Changes - in some cases 24 hours to revoke access may be unacceptable, in which case additional security and/or survellance may be required until normal access is resecured.

Page 5, Section 1301 Security Management (b) Measures (5) Access Authorization (iii) - remove or clarify (which) address of designated person.

Page 17, 1304 Electronic Security, (a) Requirements, (2) Electronic Access Controls, last sentence in first paragraph of this section "strong procedural or technical measures" provide definition or for meaning of "strong."

Page 17, 1304 Electronic Security, (a) Requirements, (3) Monitoring Electronic Access Control: It may be useful to differentiate between Active Monitoring (real-time) as opposed to Passive Monitoring. This paragraph could be interpreted as 24x7 Passive Monitoring (where records of incidents are written to logs but are not reviewed in real time). It seems the intent is for active 24x7 monitoring where the event is proactively detected and responded to in near real time.

Page 26, 1306 Systems Security Management, (2) Account and Password Management: Some organizations may implement an authentication system that is stronger than passwords but does not require a password (e.g., Certificate-based or bio-metirc authentication). It may be useful to explicitly mention that Account Password Management is only pertinent to accounts that actually use a password for authentication.

Page 29, Section 1306 Systems Security Management, (b) Measures, (7) Change Control and Configuration Management, clarify last sentence by striking "all" after "The documentation shall verify that"

General: Standardize the Compliance Monitoring and Levels of Noncompliance subsections. For example, Section 1304 Electronic Security has a very straight forward approach for Compliance Monitoring and Levels of Noncompliance. Note, this may require revising the individual "Measures" sections to ensure the proper documentation is required/created such that it can be monitored.

Editorial: Please have a tech writer review the document to standardize on formating, grammar, and consistent style as much as possible. For example, there are several spots were lists are erroneously numbered, e.g., page 16, sub-section o.3.v should be sub-section o.4 and the items

under it appropriately renumbered as well; page 32 restart numbering under item (b) from (1) rather than (5). Also on page 32, there are two (2) item (b)'s at the top list level, resume numbering from (c) Regoinal Differences (d) Compliance Monitoring Process (e) Levels of Noncompliance (f) Sanctions rather than (b) (c) (d) (e) respectively.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Michael R. Anderson	
Organization:	Midwest ISO	
Telephone:	(317) 249-5272	
Email:	manderson@midwestiso.org	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☒	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☐ No

Comments

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☐ No

If No, what are the most significant issues the drafting team must reconsider?

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
Classification Issues – Could the Term "critical cyber assets" be clearly defined as each company will likely define these differently?

Timing Issues – Could requirement timetables be better defined and perhaps more aligned with today's requirements? Specifically there are multiple references in different places of the document to the 30 days, 90 days, 12 months, etc… Could a matrix of requirements be developed to help make this clearer?

Background Checks – Can a recommendation be made on how to handle the background screenings for contractors with critical system access? Is it enough to have a trusted relationship with the vendor and utilize their background screen information for their employees or must each individual contractor employee be screened by the individual company?

Training Requirements – Can the requirement for training of personnel with access to critical systems assets be made clearer? The document implies that employees with access to critical cyber assets be held to a different standard and receive a different set of training.

Physical Security – Can the requirement for physical security logging be expanded? Specifically can the section on video logging be expanded?

Logical Security Assessment/Physical Security - Why is the assessment requirement specifically described for logical security but not for physical security? Can this item be addressed with equal diligence?

System Logs - Can the requirement for system log retention be made clearer? The requirement appears to be 3 years with a 90 day incident window. How is the 3 years measured? From the start or midpoint of the 90 days?

Archived Materials – Could the requirement of archived materials testing be made clearer? If we are retaining 3 years of data and using a medium like off-line tape it could take a huge amount of time if we must for example completely test all tapes. Does a header check suffice as a sufficient test?

Incident Reporting – Could the definition of suspected vs. validated incident be made extremely clear? Why the change in reporting to include the ESISAC?

Business Continuity – Can this section be modified to include plans that are not developed around particular assets instead of being developed for critical business functions?

The continuity plans address if some or all of the critical functions are lost for an extended period of time, on how the business must react to maintain system wide safety and reliability in varying conditions. They do not particularly address any one critical asset. Can assets be more directly addressed?

Also the alteration or change out of a particular asset does not always warrant a change to a function that is addressed within a particular business continuity plan. Why would a procedural

change require posting of new contact information? It may require some alteration to a particular contingency plan but would not necessarily warrant making any change to contact information.

Test Procedures – Can this section of the document be made to address specific layers of testing? For example the way that this is written I would assume that all Microsoft Windows Patches would have to be applied in a multi-faceted test environment to ensure that there would be no issues.

Password/Account Management – Can the section regarding auditing of user activity be expanded? Most companies have the ability to maintain audits logs at the OS level, however few applications are written with this type of functionality.

Security Patch Management – Can the term "compensating measure" be further explained?

Integrity Software – This section is clear about the need but does not address a requirement for logging or maintaining a patched/unpatched list. Should it?

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Gary H. Campbell	
Organization:	Individual	
Telephone:	630-261-2656	
Email:	ghc@maininc.org	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☒ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☒ Yes

☐ No

Comments

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
Each requirement seems to take a different approach to the content and flow of the document. The team needs to specifiy and be aware of how the content of the three sections (requirements, measures and compliance levels) are to be developed and interrelate and maintian the approach throughout the standards. Each requirement to me seems to have a different appoach or may be diferrent authoring team. The "requirements" section sets the minimum at least or define what is acceptable, the "measures" section tell me what to go and look for and "levels of compliance"section tell me the degree of severity for not having the requirements met. The authors of these standard requirenments in some cases intertwined these three area, expecially the requirements and measures sections. In some of the requirements section, it is used as an introductory section explaining what is menat by a specific term presented.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
General:

The individual requirements should be reviewed with the followin approach in mind:

I believe the "requirements" section set the minimum at least or define what is acceptable, the "measures" section tell me what to go and look for and "levels of compliance"section tell me the degree of severity for not having the requirements met. The authors of these requirenments in some cases intertwined these three area, expecially the requirements and measures sections. In some of the requirements section, it is used as an introductory section explaining what is menat by a specific term presented.

Compliance Monitor - CM

Compliance Monitoring Process: In the keeping of audit records by the Compliance Monitor, it shoud be defined as to what records are to be kept (completed audit reports). The vaque statement of keeping audit records may lead some to think they should retain the documentation observed which could lead to additional security problems.

Measures and levels of compliance need to be explicitly defined. By that I mean to be definiteve: do not use vague terms or assume the reader knows what you are talking about. Tell the reader exactly how a plan is to be defined, what is to be in the content of the requirement etc.

1301

The requirement is very large and should be consider to be divided into additional requirements. The complexity makes it difficult to focus on a particular subject matter in any great detail which would be helpful to the entity and CM

Roles and Responsibilites:

Why are we allowing roles and responsibilites to be defined by the entity? There will not be any consistency across the interconnection then.

Measures:

Many of the measures should be part of the requirements. In requirements, i believe you should be setting the minimum you want the entity to have in order to ensure protection of the cyber infastructure. Then a measure would be to " have the policy" or "have the policy reviewed in accordance with the requirement".

Levels of Noncomplance

There are to many or statements in the levels of non compliance and this is another reason to consider futher division of the requirement. In some parts, it seems the the requirements may be restated. An approach would be to state the requirements of procedures, processes or plans in the requirements section, designate in the measure section which requiremetns should be monitored by

the CM and in the levels of compliance then assign levels of non-compliacne to the number of missing requirements

Level 3

Roles and Resposibilites are not clearly defined. I do not know what clearly defined means and what clearly defined for one person may not be the same for another individual.

1302:

Requirements:

The word inventory in the first paragraph seems to mean action. Rewording so as to require documentation of this inventory may be more appropriate

There is no requirement to update the lists and I believe this would an improtant part of the process.

Measures:

What does "a properly dated" record mean in #5 ? Could be omitted?

Levels of non-compliance:

The level description should be more explicit. Many questions and uncertainty can arise when tems like "required documents" and "known changes" are used to define what the CM is to look for. Also, how is the CM to know if he has classified all the right documents as required. It should not be up to the CM to make these decisions.

Level 3 and 4 seem to be imbalanced? If I have one document missing out of, lets say 7 documents, I will be level 3 but if I don't do anyhing I am level 4.

1303

This requirement again has requirements imbedded within the measures. I believe the "requirements" set the minimum, the "measures" tell me what to go and look for and "levels of compliance" tell me the degree of severity for not having the minimum requirements met.

Levels of compliance;

Level 1

I do not think checking for consistent selection criteria is a function of reliability compliance. Wouldn't it be a human resource issue?

Please define key personnel? Define applied consisitently?

Level 2

iii - Are we refering to speciifc items in requirements?
iv - if any Awareness program does not exist how can it be imlemented?

Level 3

iii - I would think this item should be quite severe. I suggest movint to level 4

1304

Measures

A document is not required in the sections under requiements but here we are measuring for it.

1 - How can document verify that all critical assests are within the electronic security perimeter? Suggest rethinking.

4 Are the number references used correct? I can not follow them easily.

Levels of Compliance

Please define documents. Which or what documents am I looking for.

Level 4

Please be more explanantory.

1305

Measures

Items 3,4,5 where the spceific types of acess and acesss controls are specified, these items should be in requirements specified as acceptable methods to complete the requirement in my opinion.

Compliance monitoring Process

What is the reasoning for the CM keeping audit records for 90 days? The only record the CM should keep is if the entity passed or failed and any mitigation plans associated with non-compliance.

Levels of compliance

Level 1

How does the CM know the known changes? As level 3 (i) has been written, this would be more appropriate.

1306

General : Where the word "must" has been used, rewrite to incorportate "shall and should" as appropriate. This is keeping with the NERC direction for standards, I believe.

the "requirements" section set the minimum at least or define what is acceptable, the "measures" section tell me what to go and look for and "levels of compliance"section tell me the degree of severity for not having the requirements met. The authors of these requirenments in some cases

intertwined these three area, expecially the requirements and measures sections. In some are of the requirements section, it is used as an introductory section explaining what is menat by a specific term presented.

Levels of Compliance

(i) What documents are to exist, the CM shoud not be deciding what encompases this statement, nor should the CM be trying to dtermine the spcific items. We need to be more definitive and less vague

3 (iii) What does this mean? Some CM may not in depth knowledge of cyber security or it some the specifics must be clearly defined.

3(iv) What consititutes incomplete. If one item of those mention can not be found is the entity incomplete?

3(v) How can a document verify that all critical cyber assts are being kept up to date?

3(ix & x) What does N/A mean? Not applicabe or not available? We need to be more explicit.

4 No document exists. What documents? None of the documents or one of the documents, exactly which documents if they do not exist will be level 4. Do alternate plans qualify for existing dicumentation?

1307

Requirements

1 This requirement should also provide language to maintain the described incident response plan.

4 What does "all incidents " mean? If it is not Cyber related then should it be included here?

Measures

5 I suggest the wording be changed to read " The responsible entity shall have and maintain documentation ……." This will then follow the requirements.

6 I do not believe the requirements stated that entities shall retain records so then how can we measure them on this item? Maybe we should look at ensuring the procedures are in place? This could then become part of the Compliance Monitoring Process section?

7 This statement could be reworded to say " the responsible entity shall have evidence of reporting incidents to the ESISAC …….". The statement as written should then be moved to the Compliance Monitoring Process section.

Compliance Monitoring Process

2 (i,ii,iii,iv,v) Should these be included under the requirements section as you are defining what should be included as part of the documentation and therfore somewhere this should be identified in a procedure?

Levels of Noncompliance

1 What are known changes? How is the CM to know if he has a these known changes? If the documented is to be updated periodically is should specified in the requirements and then measured. It can then be reviewed for updates and accessed accordingly.

2 (i) It was not required to update or review the incident response plan. Nor do we really have measure for this item.

(ii) I think we go past what has been required and measured. I can not find what the records should contain in this document or what records specifically. Isn't this standard to ensure cyber security? We should leave the record keeping for ESIAC to that group.

3 (i) Be mor specific as to what incomplete means?

(ii) As read this statement could leave an entity level 4 noncompliant if in all actuallity there were no incidencs to report to ESIAC. It sort of makes the statement that there must be an incident.

4 Does this statement mean there was no plan, no records etc? And to be level 4, does the entity have to have every document missing?

1308

Measures

1 I suggest the statement be changed to " The responsible entity shall have recovery plans and maintain ……." This is simple and to the point.

2 It is hard to measure "as necessary". This should be dropped.

4 The term " at least once every three years or as necessary" should be removed. Training records as required by P8T3 should maintained and auditable on an on-going basis. This requirement should keep with that language.

Levels of noncompliance

1 Adequately is to vague of a term. If the items in sentence two are important then they should be needs to defined in requirement and measured with a definitve measure.

2 Need to reword the term " performed appropriately" is to vague and carries many meanings.

3 Where in the document can the CM find the types of events that are necessary?

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:		
Organization:		
Telephone:		
Email:		
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT** ☐ **ECAR** ☐ **FRCC** ☐ **MAAC** ☐ **MAIN** ☐ **MAPP** ☐ **NPCC** ☐ **SERC** ☐ **SPP** ☐ **WECC** ☐ **NA - Not Applicable**	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name: WECC EMS Work Group

Lead Contact: **Jim Hiebert**

Contact Organization: **CAISO**

Contact Segment: **2**

Contact Telephone: **916-608-1254**

Contact Email: **jhiebert@caiso.com**

Additional Member Name	Additional Member Organization	Region*	Segment*
Erika Ferguson	**IPCO**	**WECC**	**1**
Terry Doern	**BPA**	**WECC**	**9**
James Sample	**CAISO**	**WECC**	**2**
Robert Matthews	**PG&E**	**WECC**	**1**
Gary Nielson	**TEP**	**WECC**	**1**
Chuck Nichols	**BCTC**	**WECC**	**1**
Jim Hansen	**SCL**	**WECC**	**1**
Larry Shivers	**Tri-State G&T**	**WECC**	**1**
Jagjit Singh	**SRP**	**WECC**	**1**
Arnie Cook	**Northwestern Energy**	**WECC**	**1**
Gray Wright	**SPPC**	**WECC**	**1**
Arquimedes Dennis	**IID**	**WECC**	**1**
Bill Miller	**PG&E**	**WECC**	**1**
Alan Firth	**AESO**	**WECC**	**1**

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

See attached WORD Document.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
See attached WORD Document.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
See attached WORD Document.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Critical Cyber Assets – The term “adversely impact” needs to be defined more clearly.

Bulk Electric System Asset – Should be retitled as “Critical Bulk Electric System Asset” and the definition should be defined by the NERC Operating Committee.

Bulk Electric System Asset – The terms “significant impact”, “large quantities of customers’, “extended period of time”, “detrimental impact”, and “significant risk” all need to be clearly defined.

Incident – This definition should be removed based on existing operation reporting requirements, which are already in existence.

Security Incident – This definition should read; “Any malicious or suspicious activity which is known to have caused or would have resulted in an outage or loss of control of a Critical Cyber and/or Critical Bulk Electric Asset.”

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?

Format inconsistencies exist throughout the document between each section. These inconsistencies results in difficulty in determining what the true requirements are. In several instances, more than one section calls for the same requirement with different time periods. The document needs a professional tech writer to review and make each section consistent and homogenous. It is understandable that the drafting team cannot provide this level of review and consideration must strongly be given to hiring a professional tech writer prior to the next publication.

In addition to the format inconsistencies, there seems to be a lot of typos and incomplete sentences.

Due to the formatting inconsistency mentioned above in several sections it is difficult to differentiate between the section introduction paragraph, requirements, and measurements sections. In many cases they each seem to define requirements.

In all sections, compliance monitoring doesn't appear to synchronize with the section introduction paragraph, requirements, and measurements sections.

The compliance section is very difficult to understand. Multiple compliance levels are complex and should just be that you are compliant or non-compliant.

It is difficult to comment on the compliance section without understanding how the sanctions and fines are going to be imposed.

Consider removing all timeframe references (e.g. quarterly, annually, etc.) and replace with: to ensure compliance with the entities document processes. This would achieve the goal of ensuring that the entity documents their processes and procedures and would provide them the flexibility to define their own auditable/measurable business rules.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

In addition to the comments listed in Question 1 and 2, the following comments are provided. Also note, based on comments in Question 2 about the measurements and compliance, little to no comments about these sections will be documented below. The focus was on the introduction paragraph and requirements sections.

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.	**The term Reliability Authority was recently removed in the creation of the NERC Standard 0. Should be reflected here.**
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.	**Change Information Protection to Information Protection Program to be aligned with the references within the measurement section.** **Remove "used by", the pertaining to is defined below.**
(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.	**Remove "all", minimum requirements is defined.**

(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.	**The use of unauthenticated personnel is anomalous to the rest of the document. Unauthorized is a better term. Even some authenticated personnel may not necessarily be authorized.**
(iii) Protection Responsible entities must identify the information access limitations related to critical cyber assets based on classification level.	**"as defined by the individual entity" should be included after classification level to read "…classification level as defined by the individual entity."**
(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.	**Where is 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.	**Remove "or used by".** **Access Revocation/Changes: Should be reworded to read: Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished in a time frame that ensures critical cyber assets are not compromised.**

(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.	**Policies are supposed to be broad with a life cycle of 3-5 years. This should be changed to "reviewed as needed with a minimum review of every 5 years".**
(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.	**To be consistent, change title to Information Protection Program.**
(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.	**Remove "within five days" from section (i). The effort required to make this an auditable function only creates unnecessary administrative overhead and distracts from the intent of the control.** **The review periods seem to be to often and don't seem to synchronize with each other in this section.**
(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.	**Remove the last line. The effort required to make this an auditable function only creates unnecessary administrative overhead and distracts from the intent of the control.**
(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.	**Should be worded in a way that would enable identification by category, not just individual asset. Example would be that any device placed within the Energy Management System environment would automatically be covered and would not have to go to senior management.**
(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 riskbased 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.	**Replace "personnel subject to the standard " to "personnel having access to critical cyber assets".**
(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.	**Access revocation is covered within other sections of this standard. Should be reconciled to ensure consistency.** **In Canada, the equivalent is the Social Insurance Number (SIN) and should be added.**
(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.	**Strong is a subjective term and needs to be clearly defined.** **Add "where equipment supports banners" to the end of the last sentence to read "…use banner upon interactive access attempts, where equipment supports banners."**
(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 orprevents 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 nonproduction environment. All testing must be performed	**Remove "Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment. The last sentence is an adequate statement.**

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 semiannually. 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.	**Should qualify "strong password" as to where it is technically supported. Not all technology allows for this.** **Access Reviews is covered within other sections of this standard. Should be reconciled to ensure consistency.**
(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.	**The word 'timely' does not adequately reflect the risk management approach that should be used in applying patches.**
(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.	**Needs to state that it will exist "where applicable as defined by the entity".**
(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 of three (3) years in an exportable format, for possible use in further event analysis.	**The first sentence needs to be changed to reflect that audit trails need to be generated, but not necessarily by the asset as described within the first sentence. Not all devices have this capability. Additionally, should state "where technically feasible".** **What is the definition of "security related system events"?**
(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.	**This section sound very much like section 1301, authorization to place into production. Should be reconciled to ensure consistency.** **What is the definition of a "controlled environment"? Could be interrupted as a separate test environment, is this what is intended?**
(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.	**This section is not about archival, it is about back-up and recovery, so the last sentence should be removed.**
(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.	**The introduction paragraphs read more like requirements and should be in the appropriate section. Goes back to the formatting inconsistencies.** **Annual testing of low probability events is to frequent, focus on training our operators on higher probability events has more value and allows them to focus on the job at hand.** **The last paragraph is very wordy and could be reworded to be clearer.**
(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.	

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:		
Organization:		
Telephone:		
Email:		
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT**	☐	1 - Transmission Owners
☐ **ECAR**	☐	2 - RTOs, ISOs, Regional Reliability Councils
☐ **FRCC**	☐	3 - Load-serving Entities
☐ **MAAC**	☐	4 - Transmission-dependent Utilities
☐ **MAIN**	☐	5 - Electric Generators
☐ **MAPP**	☐	6 - Electricity Brokers, Aggregators, and Marketers
☐ **NPCC**	☐	7 - Large Electricity End Users
☐ **SERC**	☐	8 - Small Electricity End Users
☐ **SPP**	☐	9 - Federal, State, Provincial Regulatory or other Government Entities
☐ **WECC**		
☐ **NA - Not Applicable**		

Group Comments (Complete this page if comments are from a group.)

Group Name: MAPP Regional Reliability Council, assisted by the MAPP Operating Subcommittee

Lead Contact: **Lloyd Linke**

Contact Organization: **WAPA**

Contact Segment: **2**

Contact Telephone: **605-882-7500**

Contact Email: **Lloyd@wapa.gov**

Additional Member Name	Additional Member Organization	Region*	Segment*
Darrick Moe	**WAPA**	**MAPP**	**1**
John Swanson	**Nebraska Public Power District**	**MAPP**	**1**
Paul Koskela	**Minnesota Power**	**MAPP**	**1**
Larry Larson	**Otter Tail Power**	**MAPP**	**1**
Dick Pursley	**Great River Energy**	**MAPP**	**1**
Martin Trence	**Xcel Energy**	**MAPP**	**1**
Todd Gosnell	**Omaha Public Power District**	**MAPP**	**1**
Robert Coish	**Manitoba Hydro**	**MAPP**	**1**
Joe Knight	**MAPPCOR**	**MAPP**	**2**

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

See attached comment form.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
See attached comment form.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
See attached comment form.

Standard 1300 Round 1 Comments From MAPP RRC

Comments for Question 1:

Critical Cyber Assets definition. The later part of the first sentence "such as…at a minimum" implies that all these assets perform critical bulk electric system functions, which is not consistent with criteria in 1302 (for example, small generators). Removing it is recommended since specifics are addressed in 1302.

The definition of Critical Bulk Electric System assets in 1302 should also be modified, by eliminating item ii), item B) under iv), and item vi). Including substation equipment in a blanket fashion for the industry in this standard is not workable for numerous reasons. NERC should establish a cyber security standard that will advance the cause of security AND be workable to implement. Substation equipment should be captured by utilities under item vii (risk-based assesment) as they believe it is needed/justified.

Need to inlude definitions of the terms: Owners, Custodians, and Users. It would be a good idea to include a definition of "Sensitive Information" or something similar that refers to "information pertaining to critical cyber assets…". The idea is to be more definitive about what information should be protected pursuant to 1301 (a)(2).

For the definition of Incident, recommend the phrase "or could have lead to a disruption of" be removed. How would one measure/determine if it "could have" lead to a disruption? It would be interpretted differently by each entity.

For the definition of Incident, the phrase "or was an attempt to compromise" should be eliminated. This would be interpretted differently by each individual entity and may result in thousands of reports daily.

For the definition of Security Incident, recommend the phrases "are known to" and "or could have resulted in" be removed. They are vague, and would be interpretted differently by each entity.

For the definition of “Responsible Entity” - since definitions are to be included in a separate glossary, rewording the last part of the sentence "as identified in the Reliability Function table of the Standard Authorization Request for this standard" is suggested.

Comments for Question 2:

1302 Critical Cyber Assets, (a) (1). The standard is not clear whether the Largest Single Contingency for a Reportable Disturbance is specifically for the Entity or the Reserve Sharing Group (as an Entity may belong to a Reserve Sharing Group).

Question: The FAQ defines the MOST SEVERE SINGLE CONTINGENCY as the largest single generator in the system. Does this mean only a single generating unit and not a generating station? What about greater single contingency losses as represented by the transmission facilities (subs, high voltage lines) that carry aggregated power from multiple units in a single station, and therefore carry more power than any individual generators in a Reserve Sharing Group? Wouldn't those facilities then represent the most severe single contingency?

1302 Critical Cyber Assets, (a) (2). The logistics for Items A-E should be clarified; it is confusing.

1302 Critical Cyber Assets, (a) (2). There should be more clarification/restatement of requirements for dial-up cyber assets that do and do not support routable protocols (what requires a physical perimeter and what does not, and what requires an electronic

perimeter, and what does not?). Is there a typo in 1302 (a) (2) (i) (D): it reads "which do use a routable protocol" - should is say "which do NOT use a routable protocol"?

All required minimum review periods should be a standard period of one year. Having so many review periods with numerous periodicities is not practicable.

NERC should lean on existing standards including National Institute of Standards and Technology (NIST) Cyber Security standards (See series 800, Computer Security) that are already well-developed and tested, instead of having electric utility people create a whole new set of such standards. Also, the NERC standard seems to have redundancy with other security compliance requirements such as Sarbanes-Oxley, etc, but seems not to be well coordinated with these other standards.

Under 1301 (a) (3), the sentence that says "This person must authorize any deviation or exception from the requirements of this standard." should be changed to read "The person that must authorize any deviation or exception from the requirements of this standard must be specified in the responsible entity's governance documentation."

In several places in the standard, the issue of authorized access and tracking that access is discussed. It is usually unclear if this is meant to include only those that have access with administrative privileges, or if it extends to those that utilize the assets as users (Dispatchers using an EMS, for example). One example of such a gray area can be found in 1301 (a) (5) (ii), for example - but there are many such areas. NERC should not focus on access by those that only have rights to use the system, and should clarify in all such contexts that the reference is only to those with administrative access.

Section 1303, under Measures (4) (iv) is one of many examples of too much proscriptive detail. At least one entity in MAPP is not allowed to do criminal back-ground checks with local law enforcement, and so requiring that be done for the last seven years is not acceptable. The background screening criteria should all be altered/simplified to only say that a utility must have a policy related to the screening, and must follow that policy and be able to show the records that it was followed.

Section 1303, Requirement (4) the phrase "prior to being granted unrestricted access to critical assets" should be removed since it conflicts with Section 1303, Measure (4) (iv).

This standard is an expansion to standard 1200; implementation resource requirements look to be very significant. It would be helpful if the implementation plan were provided. Will there be an expanded implementation timeframe in which to address the standard (beyond the first quarter of 2006)?

Under 1301 (d) (3) (ii), remove the word "and" at the end of the sentence.

Under 1301 (e) (1). What is the difference between (iv) and (v)?

Under 1306 (a) (2), please rephrase the 2nd sentence (The responsible entity must establish…) to make it clear.

Comments for Question 3:

Generally agree with the thought and principles behind the new standard; however, are concerned about the considerable expansion in the number and types of critical cyber assets, as well as the increased specificity throughout the standard. The standard requires a significant amount of diligence (especially in the tracking, authorization and management of sensitive information) and will undoubtedly lead to staffing increases.

Standard 1300 refers to certain sections (1302.1.1,1302.1.2, etc.) but no such section exists since the document appears to use a different section numbering scheme.

1302 Critical Cyber Assets. Section headings are out of sequence (a..g).

1300 Cyber Security, Page 2. The items in the text box aren't consistent with this standard (refers to Purchasing/Selling Entity which is not applicable, but omits Transmission Operator, etc).

Section 1303, under Requirements (1). It appears like the phase "Responsible entity shall comply with the following requirements of this standard" should preceed items 1 through 4, not be part of item 1.

1307 Incident Response Planning. The meaning of the acrynom ESISAC should be stated. It would also be helpful to state how to access ESISAC.

The formatting requirments to translate this data (for submission to NERC for this Standard review) into a database are difficult to achieve. This commenting process should be designed to work effectvely for the industry, and not hindered by such difficult formatting requirements.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Joe Weiss	
Organization:	KEMA	
Telephone:	(408) 253-7934	
Email:	jweiss@kemaconsulting.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☒	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Bulk Electric System Asset is defined as: “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.” There are numerous distribution facilities that meet this definition. In fact, some critical distribution facilities would meet all three criteria. Since NERC’s charter does not address distribution, I recognize that NERC cannot specify distribution should be included in 1300. However, NERC should encourage responsible entities to apply the standard to additional assets that are found to be critical upon the execution of a vulnerability and risk assessment. One possible approach would be through the Frequently Asked Questions (FAQ)

Security Incident is defined as any malicious or suspicious activities which are known to cause, or could have resulted in an incident. An incident s defined as any physical or cyber event that dirupts, or could have lead to a disruption of the functional operation of a critical cyber asset. An unintentional event such as IT perfomed an unauthroized scan can, and has caused disruption of the functional operation of a critical cyber asset. Consequently, Security Incident should have the verbage "any malicious or suspicious" removed.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
Security policies should acknowledge and consider the unique requirements of control systems. There are significant portions of traditional IT security policies that apply to control systems. However, there are other portions of traditional IT security policies that may not adequately address control system-unique issues. NERC 1300 is meant to address critical cyber assets (control systems). It has been documented that inadequate control system policies and procedures have led to many control system denial-of-service events. These events would not have been mitigated using traditional IT security policies and procedures. ISA SP99 Technical Report 2 should be explicitly referenced as it has been developed specifically for process control system security. Additonally, requirements for awareness and training should be expanded to include control system cyber security awareness and training.

Wireless security for control system applications has not been included. Wireless security was specifically identified in the Final Report of the Northeast Blackout. Additionally, telecom security as it impacts control system operation also has not been included. Telecom issues have impacted critical control systems operations (eg, as documented by NERC, control centers, substations, and power plant operations were significantly impacted when the Slammer worm impacted frame relays, etc.).

Access authorization should include internal employees and those non-utility employees that also require access such as control system vendors, system integrators, etc. Access authorization may not be able to be extended to control systems as the technology may not be currently available for certain plant and substation equipment.

Requirements on Antivirus, patching, default access, etc should have a disclaimer that it be applied to the extent practical. Depending on the version and capability of the control system, some of these applications can actually shutdown or inhibit control system functionality.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
1302.a.2.i.D should read Dial-up accessible critical cyber assets, which to not use a routeable protocol. The not is missing.
1305 should refer to six-wall boundaries for physical protection, not four-wall (reference appears twice)
There are numerous outline numbering errors included in the PDF version of the standard that must be corrected.
Standard section internal reference notation does not match the outline formatting used in the document.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:		
Organization:		
Telephone:		
Email:		
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT**	☐	1 - Transmission Owners
☐ **ECAR**	☒	2 - RTOs, ISOs, Regional Reliability Councils
☐ **FRCC**	☐	3 - Load-serving Entities
☐ **MAAC**	☐	4 - Transmission-dependent Utilities
☐ **MAIN**	☐	5 - Electric Generators
☐ **MAPP**	☐	6 - Electricity Brokers, Aggregators, and Marketers
☒ **NPCC**	☐	7 - Large Electricity End Users
☐ **SERC**	☐	8 - Small Electricity End Users
☐ **SPP**	☐	9 - Federal, State, Provincial Regulatory or other Government Entities
☐ **WECC**		
☐ **NA - Not Applicable**		

Group Comments (Complete this page if comments are from a group.)

Group Name: NPCC CP9, Reliability Standards Working Group

Lead Contact: **Guy V. Zito**

Contact Organization: **Northeast Power Coordinating Council (NPCC)**

Contact Segment: **2**

Contact Telephone: **212-840-1070**

Contact Email: **gzito@npcc.org**

Additional Member Name	Additional Member Organization	Region*	Segment*
Guy V. Zito	NPCC	NPCC	2
Ralph Rufrano	New York Power Authority, NYPA	NPCC	1
David Kiguel	Hydro One Networks	NPCC	1
David Little	Nova Scotia Power	NPCC	1
Greg Campoli	New York ISO	NPCC	2
Bob Pelligrini	United Illuminating	NPCC	1
Frank Flynn	National Grid US	NPCC	1
Peter Lebro	National Grid US	NPCC	1
Al Adamson	New York State Reliability Cncl.	NPCC	2
Khaqan Khan	The IMO , Ontario	NPCC	2
Ron Falsetti	The IMO , Ontario	NPCC	2
Joe Perierra	ISO New England	NPCC	2
Seamus McGovern	ISO New England	NPCC	2
Kathleen Goodman	ISO New England	NPCC	2
Paul Gatt	The IMO, Ontario	NPCC	2
Ian Bradley	Hydro One Networks	NPCC	1
Brian Hogue	NPCC	NPCC	2
Alan Martin	New York Power Authority (NYPA)	NPCC	1
Chuck Nobel	ISO New England	NPCC	2
James Begin	Central Maine Power Co.	NPCC	1
Ken Schlessler	Central Maine Power Co.	NPCC	1

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

NPCC's participating members recommend that the definition of Critical Cyber Assets be;

"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).

NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.

NPCC's participating members recommend changing the Incident definition from

"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."

to

"Incident: Any physical or cyber event that:

disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?

NPCC's participating members feel there is much redrafting to be done to the standard and that the following items may be considered "show stoppers" by some.

Standard 1300 is based on what the critical BES assets are, which is defined in 1302.a.1. Per question 1, NPCC's participating members do not agree with that definition and have made suggestions as to what the Drafting Team may do to address the issue.

NPCC's participating members also believe the need to change the Incident definition, to the one shown in Question 1 is important.

As previously discussed and commented on in various forums, NPCC supports the NERC decision to move away from monetary sanctions.

NPCC's participating members have also expressed concern over the incremental administrative tasks and documentation requirements to be compliant with this standard and hopes the Standard Drafting Team will consider this during the development of the associated "Implementation Plan".

Throughout the document, the compliance levels should be updated to measure the proposed revisions suggested below. NPCC has made some recommendations in this regard.

There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected and recognized with consideration of this Standard.

The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to gauge the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. It is NPCC's hope that this will be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.

NPCC’s participating members agrees with the intent of Section 1303. The term “background screening” however has too many issues for NPCC participating members and recommend that this section’s title become “Personnel Risk Assessment”. Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk and have made recommendations later in the form that will make this Section acceptable.

The references within the standard made to other portions of Standard 1300 are not correct. Without clear references, NPCC cannot determine if the document is acceptable or not. For

example, 1301.a.3 says "as identified and classified in section 1.2." Where is this section? Each one of these incorrect references must be corrected.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

Correct references as covered in question 2.

Request clarification on what "information" is protected in 1301.a.2.

Change 1301.a.2 from;

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

to

"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets." (NPCC's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)

Change 1301.a.2.i from;

"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."

to

"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well." (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)

Change 1301.a.3 from;

"….entity's implementation of…"

to

"…entity's implementation and adherence of…"(NPCC's participating members believe it is important to stress that not only is it important to implement this Standard but to adhere to it as well.

The “24 hours” in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.

Change 1301.a.5.iv from;

"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."

to

"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven calendar days for all other users of a change in user access status. All access revocations/changes must be authorized and documented." (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)

change 1301.b.5.i from;

"5 days"

to

"7 calendar days" (NPCC's participating members believe that the 5 days may be not be sufficient time especially when considering holiday seasons)

1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency in the reference for retention of audit records.

1301.d.3.iv, request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor

1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii to ensure the protection of the identity/personal information of the affected individuals

Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor

1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.

1301.e.2.iii, change from;

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

to

"An authorizing authority has been designated but a formal process does not exist to

test, validate and deploy systems into production, or" (NPCC believes it was the drafting team's itent to deploy the system rather than promote which has a different connotation associated with it,)

Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change "Executive Management" to "Senior Management" for consistency and clarity.

1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).

NPCC Participating Members believe that the concept of the Bulk Electric System and association "definitions" may not be appropriate to capture the intent of the standard. NPCC suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.

Replace the 1302 preamble and 1302.a.1 and 1302.a.2 as shown below, with;

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 which support the reliable operation of the bulk electric system.

The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.

(a) Requirements
Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.

(1) Critical Bulk Electric System Operating Functions and Tasks

The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:

- monitoring and control
- load and frequency control
- emergency actions
- contingency analysis
- arming of special protection systems
- power plant control
- substation control
- real-time information exchange

(2) Critical Cyber Assets

(i) In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:

A) The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.

B) The consequences of the Operating Function or Task being compromised (i.e. “highjacked”) for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.

C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.

D) Known risks associated with particular technologies

Change 1302.g.1 from;

"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."

to

"1 Critical Bulk Electric System Operating Functions and Tasks
(i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."

Change 1302.g.2.i from;

"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."

to

"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure." (NPCC believes the use of the word additional is of no value as used here and recommends removal).

Change 1302.g.5 from;

"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"

to

"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval" (NPCC believes that it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations of operations is lost.)

Change 1302.g.5.i from;

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

to

"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."

Change 1302;
"critical bulk electric system assets"

to

"critical bulk electric system operating functions and tasks"

1303, NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for the NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk.

The FAQ describes supervised access, 1303 does not touch upon this topic.

Change 1303.a.4 from "unrestricted access" to "authorized access".

Change 1303.a.4 title to "Personnel Risk Assessment."

Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."

Change 1303.a.2 from;

"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."

to

"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"

1303.a.4 from;

"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."

to

"Personnel Risk Assessment: There must be a documented company personnel risk assessment process."

Add to 1303 Measures.2, a training measures for disaster recovery (1308) and incident response planning (1307).

The numbering of 1303 starting with Measures needs correction.

1303 Measures 4.i, request clarification. Does this include third party personnel?

Change 1303.Measures.4.i from;

"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)."

to

"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 respective security perimeter(s)." (NPCC believes there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)

Change 1303.Measures.4.ii from;

"two business days"

to

"seven calendar days", per earlier comments and to keep consistent with FERC Order.

1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days", per earlier comments

1303.Measure.4., remove;

Subsections iv, v and vi.

and replace with

"There must be a documented company personnel risk assessment process." NPCC's participating members feel these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities."

1303.Compliance Monitoring Process.2, NPCC's participating members do not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria
is not applied, or" to "Personnel risk assement program is practiced, but not properly documented, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."

Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii

From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.

Change 1304 a.2 Electronic Access Controls:
to

"The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" 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)."

Change 1304 a.3 Monitoring Electronic Access Control:
to
"The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."

Change 1304 a.4 from;

"The responsible entity shall ensure that all documentation reflect current configurations and processes."

to

The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.

1304.a.4 Remove -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. (This is a measure and should be removed here)

Compliance Monitoring Process;
Change 1304.d.3 from;

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

to

"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"

Level of non compliance
"Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.

1305 Physical Security;

Eliminate the bulleted items in the Preamble to Section 1305-they appear in the Requirement section.

Replace 1305 a.1 with;
"Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.
• The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),

• The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and
• The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."

Change the following - (a) Requirements;
"(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."

to

"(3) Physical Access Controls: The responsible entity shall implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.
(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.
(5) (We recommend deleting this bullet as the intent is captured in bullet "4").
(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."

Change Measures;

"(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."

to

"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility." (NPCC believes the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)

In 1306.a.1, last paragraph, modify the second sentence to read as follows;

"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."

1306.a.2.ii change "pooding" and "puffing" to "putting" (it appears a pdf translation problem as some documents the group printed have it and others did not)

1306.a.2.ii remove "Generic" from the title

1306.a.2.iii, use "at least annually" instead of "at least semi-annually"

Change 1306.a.3 from;
"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."

to

"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets." (NPCC believes that it upgrades are a subset of the applicable security patches.)

Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."

Change 1306.a.4 from;

"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."

to

"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."

1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).

Change 1306.a.6 from

"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."

to

"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three calendar years in an exportable format, for possible use in further event analysis."

1306.a.7 Remove "Configuration Management" from the title

1303.a.8 Remove the word "inherent" it is not clear what is meant by it.

1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.

1306, remove 1306.a.11 since 1308 addresses back-up and recovery.

1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.

1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days".

1306.b.3, remove;

"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."

and change

"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."

to

"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."

1306 b.3 first sentence-eliminate the word "management".

1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.

1306.b.4 third sentence Change
"..so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."

to

"..mitigate risk of malicious software".

1306.b.4 Remove the second sentence.

1306.b.4 Replace the fourth sentence with;

"Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."

1306.b.5 remove the first sentence.
Based on the common use of third parties for outsourcing of this associated work of vulnerabilty assessment, it is not reasonable to maintain the information called for in sentence one.

Change 1306.b.6 from;

"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."

to

"Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis."

1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"

Remove 1306.b.11, since 1306.a.11 was removed.

1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."

1306.d.3.iii, change "system log files" to "audit trails"

1306.e.2, change "the monthly/quarterly reviews" to "the reviews"

1306.e.2.ii.C, change "anti-virus" to "malicious"

1306, the Compliance levels should be updated to match the above measures.

1307, spell out and provide clarification on the acronyms throughout.

Change 1307, from;

"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."

to

"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."

1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;

"Incident and Cyber Security Incident Reporting"

to

"Security Incident Reporting".

and also Change from;

"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

to

"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

Refer to our definition of a "security incident", change 1307.b.5 from;

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

to

"The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements."

Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."

to

"The responsible entity shall retain records of security incidents for three calendar years."

Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."

to

"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."

1307.d.1 there is a 90 day reference that does not appear in the measures.

In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.

Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Edward C. Stein	
Organization:	FirstEnergy Services	
Telephone:	330.315.7480	
Email:	steine@firstenergycorp.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☒ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☒	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Definition for Bulk Electric System Asset is not consistent with it's intent. This is a highlevel component that is really facility based and should be reflected as "Bulk Electric System Facility".

There is definition or criteria stated for the Risk Assessment. There should be three definative levels for the risk assessment starting at the top with Bulk Electric System Facility, then Critical Cyber Assets (System Functions) and Cyber Assets. This should be spelled out in the standard and not added as a FAQ.

Applicability: Should contain a disclaimer that the NUKES are not included, currently if you want that information you have to go to the SAR.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
See response to question 3

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

Definitions: Bulk Definitions need to be clear and consistent from one NERC document to the next if a true “consensus” throughout the industry is desired by NERC prior to balloting.

By placing additional security restrictions/costs on routable (IP) technology, NERC will (in effect) slow the migration from older technologies to more flexible future technologies involving (IP).

During the Standard 1200 process, the NERC Responses to the Ballot Comments provided a different definition than the language contained in Standard 1200 in some cases. Example: Standard 1200 clearly stated an “isolated” test environment was required. NERC Responses clearly stated that an “isolated” test environment was NOT required. This led to mis-understandings about what the real requirements were. Although the Standard 1300 process is young, there appears to be too much reliance on the FAQ’s to embellish the requirements. Documents, such as the FAQ’s, should be used to provide examples. The intent of the requirements should be fully explained in the Standard 1300 language, not the FAQ’s.

ABC is concerned that requirements, such as excessive documentation, will mean that resources are utilized to comply with requirements that do not truly enhance actual security.

ABC believes that some estimate of the costs vs. the benefit of the requirements must be understood before moving toward implementation.

General Question

If a company goes through the process and finds that it has NO critical cyber assets, does that company have any additional obligations under Standard 1300? If so, please explain.

Definitions Section

Page 1
The definition of "Cyber Assets" (on page 1 of the draft) is vague and leaves room for interpretation, and how it is interpreted could have drastic impact. The term "cyber" in the heading implies computerized equipment, particularly that which can be networked together via electronic communications, however the definition does not specifically state that. ABC seeks clarification from NERC regarding "non-computer" devices such as protective relays, solid-state transducers, etc. that are not networked nor communicated to in any way.

Definitions section needs to clearly define “routable protocol” in the definitions including what is a routable protocol and what is not a routable protocol. While the definition may be familiar to many, this concept is key to identifying the critical cyber assets, yet no definition is provided.

Definitions section also needs to define “dial up accessible” for same reasons noted above.

1301 Security Management Controls Section

Page 3: Several sections of 1301 will require coordination at executive level across business units throughout corporations. These types of sweeping administrative documentation requirements will prove extremely time consuming and, therefore, expensive to implement under the proposed 1300 language. Some are already inherent in the organization charts, operating procedures, and job descriptions of the corporation. Standard 1300, as proposed, will simply create redundant corporate documentation in these cases because (while documentation may exist) it may not be in a format readily available for Standard 1300 audit review. If no relevant threat information exists or the costs and benefits do not warrant implementation, ABC recommends section such as those listed below be eliminated or modified.

Governance section, which requires entities to document structure for decision making at executive level.
o The Cyber Security Policy section of 1301 requires that senior management acknowledge responsibility for cyber security. Therefore the 'decision making' at the executive level is covered in the Policy section, making the governance section un-necessary.

Roles & Responsibilities requiring participants to "maintain in its policy the defined roles & responsibilities…"
o If The Roles & Responsibilities section is not deleted entirely, then at least delete the second paragraph: 'The responsible entity shall also define the roles and responsibilities of critical cyber asset owners, custodians, and users…identified and classified in section 1.2'. From the existing numbering system used, it is not clear what "1.2" refers to.

Page 4: "Authorization to Place into Production," part of Section 1301, requires entities to "identify the controls for testing…and document that a system has passed testing criteria." ABC agrees that a testing procedure is required. However 1301 language as proposed requires redundant documentation over and above requirements as spelled out on p. 26 and 28 in the "Test Procedures" part of Section 1306. Section 1306, "Test Procedures" (p. 28) states "…change control documentation shall include records of test procedures, results of acceptance of successful completion…documentation shall verify that all changes to critical cyber assets were successfully tested…prior to being rolled into production…" Recommendation: Section 1301 authorization to Place into Production section (for the most part) is redundant to Section 1306 Test Procedures. If the following sentence was added to Section 1306, Test Procedures, then all of "Authorization to Place into Production" section could be eliminated. "Responsible entities shall designate approving authority that will formally authorize that a system has passed testing criteria." Appropriate references to associated non-compliance items would also have to be eliminated.

NERC's recently published FAQ's on Standard 1300 actually adds additional issues. Standard 1300 calls for "…entities to...identify controls…designate approving authorities that will formally authorize and document that a system has passed testing criteria….approving authority shall be responsible for verifying that a system meet minimum security configurations standards." There is nothing in the Standard 1300 which states the approving party cannot be an operator, programmer, or owner of the system. Yet in the FAQ for Standard 1300, NERC states " …assign accountability to someone other than the operator, programmer, or owner of the systems to ensure that …" testing has been completed. It appears that NERC is adding yet more requirements, ie., (separation of duties,) through the use of FAQ posting. ABC recommends that if requirements are not spelled out in the Standard language, additional requirements (such as this type of separation of duties) should not be introduced via the FAQ publications.

Page 4: Access Changes: By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 & 1306)
Need clarification & consistency from NERC on exactly WHAT the access change requirements are.
- 1301 states: "Responsible entities shall… ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."
- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)… and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.
- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who…are not allowed access…(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.
- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations…24 hours.

Further on the subject of Access requirements, commentors stated that the 24-hour access limitation for updating records was un-duly severe in the Standard 1200 comments. NERC Responses to Cyber Security Standard 1200 Ballot Comments 6-11-03 posted to the NERC website provided the following:

"NERC acknowledges the validity of these comments and will address them more fully in the final standard... we will expect that a system will be in place to periodically update access authorization lists on at least a quarterly basis. That protocol will also ensure that access be suspended as soon as possible and no later than 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems. Routine administrative changes resulting from retirements, resignations, leaves, etc. should be handled within the normal course of business but not in excess of three business days after occurrence…."

While ABC acknowledges that Standard 1300 is a different standard from 1200, we wish to remind NERC of the statement that they will address objections to the excessively stringent 24 hour access update requirement in the 'final standard." Since objections have not been addressed, NERC still needs to do this.

Regarding requirements for updating access records, ABC recommends:
(1) The requirement should be stated as recommended by NERC above 'Access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat…Routine administrative changes …should be handled within three business days after occurrence."
(2) The requirement should only be defined in one section of the document rather than currently proposed language which includes multiple conflicting requirements within the same Standard.
(3) If the item is used to identify non-compliance, all references throughout the document should reflect the revised requirements.

Page 3: (a) (2) (i) "The responsible entity shall identify "all" information, regardless of media type, related to critical cyber assets." It is impossible to certify that ALL information is identified and protected. ABC recommends that the word "all" should be deleted and language changed to: "The responsible entity shall identify information related to critical cyber assets."

Page 3: ABC seeks guidance from NERC regarding the minimum levels of 'protection' to be afforded this information.

Page 7: Levels of non-compliance, particularly for Level four are excessive. There are eleven (11) different items identified that can trigger a non-compliance item. This is far too many non-compliance triggers, and too burdensome. Recommendation: If the sections on Governance and Roles & Responsibilities are omitted as suggested above, then these items will also be omitted from Levels of Non-compliance, making the document manageable: Level 2 delete (iii); Level 3 delete (iv); Level 4 delete (iv), (v), (vi), (viii). If Governance and Roles & Responsibilities sections remain part of the document, then NERC should select 2 to 4 items from the list of 11 Level 4 triggers that will provide an indication of compliance and delete the remainder.

Page 7 (4) (xi) The item which seeks a violation if one access change is not accomplished within 24 hours needs to be either eliminated or else modified to reflect the above recommendation that a violation is only warranted if the access is not suspended in 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems.
1302 – Critical cyber assets
Page 10: Critical Cyber Assets: "…the cyber asset supports a critical bulk electric system asset." Examples: Environmental and performance software supports generation assets but is not critical to continuation of power. In the 10/18 Webcast, NERC used the word "control" rather than "supports". ABC recommends that the word "supports" be changed to reflect the intent that the cyber asset is essential to continued operation of the critical bulk electric system asset, i.e., loss of that cyber assets causes loss of the critical bulk electric system asset.
Page 10: "Critical Cyber Assets", as defined on page 10 of the draft, narrows the definition to cyber assets that "support critical bulk electric system assets" AND "uses a routable protocol" or "is dial-up accessible". Because a proper understanding of what constitutes a critical cyber asset, ABC has several questions and seeks clarification from NERC on protocols in use throughout the organization today as well as protocol proposed for the next generation of communication from remote locations to ABC's Energy Management System.
ABC interprets Standard 1300 to exclude devices such as remote terminal units that communicate over dedicated point to point communication circuits. An example of this would include RTU's communicating via Landis & Gyr 8979 RTU protocol over 4-wire dedicated Bell 3002 circuits. ABC seeks clarification on the following:

ABC currently uses a "non-routable" protocol (e.g. ABC's current Landis & Gyr 8979 RTU protocol) that are communicated using PVCs (private virtual circuits) over a frame relay network. ABC seeks clarification on routable protocol reference and how NERC believes it applies here.

ABC needs clarification on 'routable protocol' reference and how requirements apply to proposed use of "DNP over IP" using frame relay.

ABC seeks clarification of the 'dial up accessible' reference regarding DNP.

Is an electronic relay interpreted by NERC to be a computerized cyber asset?

If a relay is constructed to allow remote data retrieval but prohibit any configuration changes, is it excluded from the requirements?

Page 9 Generation: Proposed Standard 1300 references other documents (Policy 1) that are open to interpretation by Regional Councils. Rather than spelling out the rules for generation that needs to be considered a Critical Bulk Electric System Assets, Standard 1300 refers to another document (Policy 1.B). ECAR has modified the definition of "Most severe single contingency".

Using the proposed Std 1300 language from the multiple documents and regional definitions mean that almost all ABC's generating facilities fall under the rules of Standard 1300.

Is it NERC's intent that all generating stations should be subject to the rules of Standard 1300? If this is not NERC's intent, then the proposed language needs to be changed.

ABC recommends that all of the rules for identifying the critical bulk electric system assets and the critical cyber assets should be identified in one document, rather than using multiple documents subject to regional interpretations as used in Std 1300 version 1. Recommendation: On page 9, eliminate reference to NERC Policy 1.B in (iii) (A) and replace with this language: "…greater than or equal to 80% of the most severe single contingency loss."

ABC seeks clarification from NERC of the term "Most severe single contingency". Please use the following example:

Utility owns approximately 600 MW of a total 1300 MW generation site all in ECAR

Same utility owns 100 % of a 635 MW generation site

Which of the above should be identified as the largest "single contingency"? If the 635 MW site is used, generating units, which ABC does not consider critical, will be included in the list of "critical cyber assets."

ABC recommends that a good use for the FAQ's would be to provide additional examples, including some examples using how the requirements apply to jointly owned units (JOU's).

Page 9: Either fully explain or eliminate (iii) Generation (B) "…generating resources that when summed meet the criteria…"

Page 10: ABC believes the level of documentation and administrative control required by proposed Standard 1300 is extensive and imposes a significant operating cost on participants. Once again, this section contains requirements without any documented evidence that the expense to implement will enhance security or that there is a relevant threat, which will be mitigated by this level of documentation. Parts of the section are redundant to other requirements. ABC has designated two company officers that are responsible for the Cyber Security Policy and implementation. "Critical Bulk Electric system Asset and Critical Cyber Asset List Approval section," requires a properly dated record of senior management officer's approval of the list of critical bulk electric system assets. ABC recommends that requirements such as this be deleted unless evidence is shown which indicates direct security benefit. Recommendation: Eliminate Requirement (a) (3) " …A sr. management officer must approve the list of…" and also eliminate corresponding "Compliance Monitoring Process" (i) (3) (iv) page 11. The senior officers are responsible for implementation of the program and should not be required to sign off on each section of the document as each section is updated.

In the October 18 Webcast, NERC slides indicated a "3 step" approach to identifying the critical cyber assets. Standard 1300 lists (#1) Identify the Critical Bulk Electric System Assets and (#2) Identify Critical Cyber Assets. ABC seeks clarification from NERC regarding the three (3) steps referred to in the Webcast.

1303 – Personnel & Training

Page 13 "Awareness Program": Once again, this section contains requirements without any documented evidence that such requirements will enhance security. Requiring both training program and awareness program seems redundant and burdensome. ABC recommends that the awareness in inherent in training and is part of the training requirements. We recommend that the separate "Awareness" section be deleted.

Page 14 Access Changes:
By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1301 & 1306)
Need clarification & consistency from NERC on exactly WHAT the access change requirements are.
- 1301 states: "Responsible entities shall… ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."
- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)… and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.
- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who…are not allowed access…(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.
- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations…24 hours.

Regarding requirements for updating access records, ABC recommends:
1. The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat…Routine administrative changes …should be handled within three business days after occurrence."
2. The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.
3. If the item is used to identify non-compliance, all references throughout the document should reflect the revised requirements.

Page 14: Background Screening. The entire section on background screening, as written in Standard 1300, is problematic. For example:
- "…A minimum of Social Security Number verification…" Language as written will deny access to anyone except U.S. citizens. ABC recommends that the language requiring a social security number be deleted unless it is NERC's intent that only U.S. citizens and no one else is granted electronic or physical access.

NERC showed insight when, in their Responses to comments submitted during the balloting of the Urgent Action Cyber Security Standard 1200, NERC wrote: "…organizations are NOT required to conduct background investigations of existing employees given the fact that they have had the opportunity to observe and evaluate the behavior and work performance of those employees after they have been employed for a period of time." ABC again recognizes that Standard 1300 is a different standard from Standard 1200; however, the logic that provided the foundation for the previous NERC comment is sound. If the company has had an opportunity to observe the long service employee, the background screen requirement should be relaxed.

ABC recommends one of the following to replace proposed Standard 1300 language:
A. The requirement should include background screening for all individuals (employees and vendors) who seek approval for new permanent access to critical cyber assets.

Background screening on existing employees, previously approved for access, is appropriate if there is cause to suspect the individual of suspicious behavior.

Requiring the screening of all personnel every 5 years should be deleted.

B. If the above proposed language is not acceptable as an alternative by NERC, then ABC recommends language be inserted indicating that background screening requirements will be evaluated by the company involved, and the policy toward such screenings will be documented by that company. Company will be free to document policies such as: At Company's discretion, long service employees, which the Company has observed, may be grandfathered and background checks will not be done on these employees. Company will not be found in non-compliance for such a policy.

Page 13: Language states that a "higher level of background screening" should be conducted on personnel with access. ABC's background screening for new hires complies with the NERC requirements and other legal requirements. ABC does not agree that multiple levels of background screening are required. ABC recommends that the reference to multiple levels of background screening be deleted.

Page 13: Records: " …background screening of all personnel having access to critical cyber assets shall be provided for authorized inspection upon request." ABC does not agree that the background screen information obtained on all its employees will be provided to NERC inspectors. In the 10/18 Webcast NERC stated that it is not their intent that the contents of the background screening be provided to the inspectors. Recommendation: Improve language so that it is clear that contents of background screen need not be divulged to inspectors.

Page 15 (i) Standard 1300 language implies that background check lists & verifications are kept by operations groups responsible for the cyber security implementation. Such records will continue to be maintained by the Human Resource Department at ABC.

Page 13: Background screening: Proposed language states: "…contractors and service vendors, shall be subject to background screen prior to being granted unrestricted access to critical assets." Is it NERC's intention that they be granted unrestricted access after completing a background screen as stated in 1300?

1304 – Electronic Perimeter

Page 17 (a) (1) Electronic Security perimeter: Proposed language states "Communication links …are NOT part of the secured perimeter…However, end points of the communication links… are considered access points to the perimeter. Where there are non critical assets within the defined perimeter these non-critical assets must comply with the requirements…" Language is contradictory and confusing. Proposed language makes the asset and the end point critical assets and within the perimeter, but language excludes the communication line between them. The next sentence implies the communication line needs to be treated as though it is part of the perimeter. ABC seeks clarification.

Page 18: (b) (1) Electronic Security Perimeter:
ABC seeks clarification regarding from NERC regarding Frame Relay Access Devices (FRAD's) and modems connected to cyber assets. Are these considered "access points to the electronic security perimeter"?

If the FRAD's are considered 'within the perimeter' with the resulting requirements extending to the FRAD's, this is an excessive and unnecessary level of detail and will prove costly and burdensome without proven corresponding benefit.

Page 18: Measures (3): Monitoring Electronic Access Controls: Wording of this section, particularly the last sentence, is very confusing and needs clarification regarding exact requirements for documentation and for implementation of monitoring the access controls.
P. 19 (e) (3) Electronic Access Controls: Page 19 identifies a non-compliance item if "…not all transactions documented have records." ABC seeks clarification. If a transaction is documented, by definition, doesn't that mean the transaction has a record?
Page 17 Electronic Access Controls: "…non critical cyber assets (within the perimeter) must comply with the requirements of this standard." Different departments within the organization will handle different functions. Current language implies one rigid process to apply to both critical assets and non-critical assets, which may exist within the perimeter. Recommend that this be changed to: non-critical cyber assets within the perimeter must utilize similar electronic access controls.
1305 – Physical Perimeter

While ABC acknowledges that controls may be required, it does not seem appropriate for NERC to dictate the controls to be implemented. Example: Implement CCTV or Alarm System.

ABC's interpretation of current draft language in Section 1302 will result in almost all ABC generating plants being subject to these rules. Section 1305 then seeks to name the controls, which must be implemented at each asset location. No mention to a review of costs associated with such sweeping changes is even mentioned in any of the language. ABC believes it is appropriate to address the costs and corresponding benefits before moving forward with such a sweeping and costly initiative. ABC recommends that participants and NERC develop an estimate of the proposed cost to the industry before finalizing these requirements.

Generating plants control rooms may be manned 24 hours a day seven days a week. ABC seeks clarification and evidence of the need for the many controls, such as CCTV, which are specified in the document in these cases where facilities are manned.

Page 24 (6) Maintenance and testing of security systems to be retained for 1 yr. This involves corp. wide – Equipment Maintenance area. This is one more example of the costs, which must be considered before moving forward. These types of requirements are very costly to large organization because they impose enterprise wide requirements. Maintenance records on the security installation equipment will not be kept in Electric Operations areas. Requirements will need to be coordinated across groups responsible for equipment maintenance.

1306 – System Security management

While the list of physical controls to be implemented in the proposed section 1305 language represents a huge, solid, and obvious cost burden, requirements in section 1306 represent a less obvious but huge cost burden as well.

Once again, there is no evidence presented that there is a relevant threat, which will be mitigated, if these types of controls/documentation requirements are implemented. Also, once again, there is no indication if the idea of associated costs was even contemplated prior to writing the language requiring the controls/documentation.

ABC requests that evidence needs to be presented showing (1) a relevant threat will be mitigated if the controls outlined in this section are implemented (2) costs and benefits associated with requirements have been identified.

ABC is concerned that if money and resources are required for documentation requirements that yield no real enhancement to security, then less money and resources will be available for security measures that could truly yield benefit. Recommendation: Either significantly lessen requirements or eliminate many of the following.

Page 28: Archive backup information for a prolonged period of time and then test it annually to ensure it is recoverable. A definition of 'information' and 'archival information' should be provided. Archived information looses its value in time and may become irrelevant. Is NERC dictating records retention policy? What is the consequence if this does not occur? Requires extra work, but what is the point? Need better understanding of costs vs. benefits.

Page 28: Create Operating Status Monitoring tools. This section indicates the tools gauge 'performance.' Standard 1300 language contains no statement as to what these performance-monitoring tools are trying to gauge nor are any performance goals indicated. This would be costly to implement with no defined benefit or even goals for the tools. Requires extra work, but what is the point?

Page 28: Create Operating Status Monitoring tools: Language in the section implies that performance documentation is to be kept for every asset. This is not reasonable.

Page 27: Retention of system Logs: "All critical cyber security assets must generate an audit trail for all security related system events." In the case of local RTU's this is probably not possible.

Page 26: Test Procedure language as written is overly burdensome. Language implies that EVERYTHING needs to be tested. It is not realistic that EVERY minor change is documented in formal testing. FAQ's seem to conflict with Std. 1300 proposed language. Recommendation: Modify Standard 1300 language to imply levels similar to NERC's recent Standard 1300 FAQ posting.

Page 27: Testing "…provide a controlled environment for modifying ALL hardware and software for critical cyber assets." Since the Energy Management System is by nature a critical cyber asset, the language implies that EVERYTHING must be modified in a separate controlled environment. Current language is burdensome and not practical. Recommendation: Indicate a reasonable level for testing within the controlled environment. Use levels similar to those identified in NERC's recent Standard 1300 FAQ posting.

Page: 27 Test Procedure Measures: Language states, " …Critical cyber assets were tested for potential security vulnerabilities prior to be rolled into production…" It is unclear what 'potential vulnerabilities' are to be tested or how the tester is to know about them. Recommendation: Explain clearly or delete the reference.

Page 29: Integrity software: ABC is pursuing a course of isolating the Energy Management System from the corporate network. This path of isolation reduces threat from email, Internet use, etc. The language requires anti-virus versions be kept immediately up to date. In practice, this

conflicts with the work to isolate the EMS and presents un-necessary requirements since the EMS will be isolated from the source of the viruses.

Page 27: Security Patch Management: ABC seeks clarification of " …upgrades to critical cyber assets." If this language includes every upgrade, it is costly and over-burdensome without resulting security benefit.

Page 27: Created formalized change control & configuration management process: Entire section creates un-necessary and redundant requirements that are included in the Test Procedures requirements section of 1306.

Section 1306 Security Patch Management section presents additional problems for power plant control systems. For example,

Security Patch Management language (page 27) requires timely installation of applicable security patches and operating system upgrades.

Patches and upgrades (at the power plant) at ABC can only be applied during an outage of the control system.

ABC seeks clarification from NERC as to how all of Section 1306, including Security Patch Management, applies to power plant control systems. Will plants be expected to create more outages to keep up with requirements?

Page 28 (2) Account Management: "review access permissions within 5 working days. For involuntary terminations, …no more than 24 hours". By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 & 1301)

Need clarification & consistency from NERC on exactly WHAT the access change requirements are.

- 1301 states: "Responsible entities shall… ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."
- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)… and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.
- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who…are not allowed access…(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.
- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations…24 hours.

ABC recommends:

- The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat…Routine administrative changes …should be handled within three business days after occurrence."
- The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.
- If the requirement is used in the non-compliance section, then the non-compliance section should be consistent with revised requirements.

1307 & 1308- Response & Recovery Plans

Page 34:
1300 Language seems to imply NERC expects multiple plans to be created for Cyber Security. " …recovery plans associated with control centers will differ from those associated with power plants and substations." This level of detail may become too onerous. ABC seeks clarification from NERC if multiple plans are required. Once again, this will involve time, money and resources to create documentation at an un-precedented detail level with no indication that such a measure will increase real security.

If entities strictly follow the language proposed for 1307, they will be forced to create un-necessary documentation for very brief interruptions and for events, which were not malicious and did not create a disruption. NERC definitions provided the following:
NERC defines an "incident" as ANY physical or cyber event that disrupts or could lead to a disruption of the critical cyber assets.
Same section defines a "cyber security incident" as malicious or suspicious activities, which cause or may cause an incident.
Definition section does NOT include a definition of a "reportable incident"

The language of the entire 1307 section is written to apply to both incidents and cyber security incidents.
Once again, as we have seen in other sections, companies that attempt to follow these requirements will create costly levels of detail and documentation (for every incident which either creates a slight disruption or could lead to a disruption) with no proven direct benefit to security. Here are some examples:
Page 32 states, "…retain records of incidents and cyber security incidents for 3 calendar years." This includes but is not limited to:
o System and application log files
o Video and or physical access records
o Investigations and analysis performed
o Records of any action taken including recovery actions
o Records of all reportable incidents and subsequent reports
…make all records and documentation available for inspection."
Recommendation: Re-work the language so that it is clear at what level this degree of detailed documentation needs to be retained.

Page 34 (a) (3) "…update the recovery plans within 30 days of a system or procedural change and post the recovery plan contact information." This language is problematic in 2 areas:
1. It is not realistic to expect that the plan will be updated within 30 days of each procedural or system change.
2. ABC does not "post" contact information. NERC does not specify what type of "posting" they require. Further this requirement is contradictory to other NERC cyber security requirements. ABC regards emergency plans and contact information as critical cyber asset information. Information is treated as such.
ABC recommends that plans be updated annually and that contact information should be treated consistent with other information related to critical cyber assets.

Additional Comments on Format
- The numbering sequence is not accurate throughout the document, making it difficult to follow in some sections. Recommendation: A different consistent numbering system should be used or, at the least, the entire document should be reviewed for appropriate numbering. Examples include but are not limited to:
o See Page 9 (a) Requirements then Page 10 (g) Measures. Where are items (b), (c), (d), (e), & (f)?
o Page 13: All of Section 1303 need review
- Typing mistakes need to be corrected. Example: Page 15 "…doesn't not cover one of the …"

FAQ's Recently Posted by NERC

In addition to inserting requirements regarding separation of duties noted above, question 3 on page 9 of the FAQ document seeks to limit the definition of RTU's, that use a non-routable protocol. Standard 1300 implies that non-routable protocols are excluded. However, the answer to question 3 tightens the definition of what is excluded by adding additional requirements that may not apply to all non-routable protocols: "…have a master/slave synchronous polling method that cannot be used to access anything on the EMS and they use SBO command…" As noted above, it is not appropriate to introduce additional restrictions to the Standard language via the FAQ posting process.

ABC Implementation Timeline

After the Standard 1300 language and requirements are finalized, ABC estimates:

o 1.5 to 2 years to evaluate standard impact and what is to be included in compliance.
o This is dependent upon how much guidance is given by NERC in regards to specifics for equipment and facilities to be included.

o 3.5 to 4 years to implement and become compliant.

o Total of 5 to 6 years from acceptance of the standard until compliance is reached.
of the standard until compliance is reached.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:		
Organization:		
Telephone:		
Email:		
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT**	☒	1 - Transmission Owners
☐ **ECAR**	☐	2 - RTOs, ISOs, Regional Reliability Councils
☐ **FRCC**	☒	3 - Load-serving Entities
☐ **MAAC**	☐	4 - Transmission-dependent Utilities
☐ **MAIN**	☒	5 - Electric Generators
☐ **MAPP**	☐	6 - Electricity Brokers, Aggregators, and Marketers
☐ **NPCC**	☐	7 - Large Electricity End Users
☐ **SERC**	☐	8 - Small Electricity End Users
☒ **SPP**	☐	9 - Federal, State, Provincial Regulatory or other Government Entities
☐ **WECC**		
☐ **NA - Not Applicable**		

Group Comments (Complete this page if comments are from a group.)

Group Name: Cyber Security Task Force

Lead Contact: **Dave McCoy**

Contact Organization: **Great Plains Energy**

Contact Segment: **5**

Contact Telephone: **(816) 420-4707**

Contact Email: **david.mccoy@gp-power.com**

Additional Member Name	Additional Member Organization	Region*	Segment*
Bob Brewer	**GPE**	**SPP**	**3**
Pat Brown	**GPE**	**SPP**	**1**
Sharon Cruz	**GPE**	**SPP**	**3**
Stephen Diebold	**GPE**	**SPP**	**1**
Joe Doetzl	**GPE**	**SPP**	**3**
Ken Geier	**GPE**	**SPP**	**3**
Scott Harris	**GPE**	**SPP**	**3**
Laura LeDesma	**GPE**	**SPP**	**3**
Pat Lowe	**Celeritas**		**1**
Alana Pierce	**GPE**	**SPP**	**3**
Trudy Smith	**GPE**	**SPP**	**5**
Ron Spicer	**GPE**	**SPP**	**5**
Rogers Tuck	**GPE**	**SPP**	**5**
Richard Spring	**GPE**	**SPP**	**1**
Steve Easley	**GPE**	**SPP**	**5**
Chuck Tickles	**GPE**	**SPP**	**3**
Larry Dolci	**GPE**	**SPP**	**3**
Gerry Burrows	**GPE**	**SPP**	**1**

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☒ Yes

☐ No

Comments

Question 2: Do you believe this standard is ready to go to ballot?

☒ Yes

☐ No

If No, what are the most significant issues the drafting team must reconsider?

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

Comment 1. Reference to specific line items throughout the standard uses inconsistent formats. In 1302 under the provision for Critical Cyber Assets in item E) a reference is made to 1302.1.2.1. I believe this is referring to 1302 (a) (2) (i). It would make more sense to change to format of the standard to the numerical format for consistency.

Comment 2. Your FAQ's are great and perhaps this question could be addressed in an addition to this list. Please give examples of what is anticipated in terms of risk-based assessments. These are referred to in several places and it would be helpful to know if this is load flow studies or something else.

Comment 3. The Compliance Monitoring Process appears to be almost identical in each standard. Perhaps at least a portion of it could be stated in a separate standard and not repeated eight times.

Comment 4. A Compliance Schedule is needed for SAR 1300. It should state that compliance should not take effect until the certification in the first quarter of 2007. This is necessary, because most NERC members have already developed their 2005 budgets, and it would be very difficult to pursue compliance before 2006. SAR 1200 should continue to rule in the interim.

Comment 5. No compliance matrix was included with SAR 1300. This should be added, even though presumably it is the same table that was included with SAR 1200.

Comment 6. It would be helpful to have a requirement timetable matrix that lists all of the compliance requirements along with each one's respective periodicity.

Comment 7. 1301 - Under Compliance Monitoring Process Item (3) (v) it states that audit results and mitigation strategies be made available to the compliance monitor upon request. Is this just the results of internal reviews that are required under these standards or is this suggesting that a full audit be performed annually on standard compliance? If so, is the expectation that 3rd parties perform such audits? It would be helpful to clarify what is meant by audits.

Comment 8. 1301 - Under Requirements under Information Protection under Identification it says, 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. Question 2 under 1301 in the Frequently Asked Questions states that Some examples of critical information would be grid maps, network connectivity diagrams,... The 1300 list appears to be critical cyber asset related, while the FAQ list is bulk electric system related. Is 1300 intended to address the protection of bulk electric system information that is maintained completely separately from any critical cyber asset?

Comment 9. 1302 – Should the risk assessment consider collections of bulk electric system assets, all supported by the same cyber asset, which taken collectively could, by their destruction or compromise, 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 on the reliability or operability of the electric grid or would cause significant risk to public health and safety? Or is it allowable for the

risk assessment to consider only single bulk electric system assets in its identification of critical bulk electric system assets?

Comment 10. 1302 - Under Requirements under Critical Cyber Assets the first criteria is for cyber assets that support a critical bulk electric system asset. Some clarification of the word support would be helpful. Does support include control, configuration, monitoring or historic reporting? This should be clarified, because there are accounting-type systems and asset management systems that support critical assets, but would not be typically be considered critical since compromising such systems will not result in loss of load or system reliability. For example, would distribution capacitor control, transmission line monitoring or asset management/transformer maintenance prediction systems be considered critical cyber assets?

Comment 11. 1302 - Under Requirements under Critical Bulk Electric System Assets there is a list of examples of critical assets, but it would be helpful if you could be more specific. For example, would it be fair to say that critical bulk electric system assets are limited to those assets that if compromised could cause an outage of 300MW or more for 15 seconds or longer? Such a definition would provide the industry with a consistent yardstick for determining critical assets.

Comment 12. 1303 - Under Measures under Records it is stated that the responsible entity shall maintain documentation that it has reviewed its training program annually. Shouldn't this say review and update. It would seem that this mandate should also include the updating of cyber security training programs.

Comment 13. 1301, 1303, 1306 – There are multiple references to the time frame for implementing access changes. (See list of references below.) It would be helpful if the requirements were stated clearly and centralized in one place as suggested in Comment 6.

1301 (a) Requirements (5) Access Authorization (iv) Modification, suspension, and termination of user access to critical cyber assets is accomplished with 24 hours of a change in user access status.

1301 (e) Levels of Noncompliance (4) Level Four (xi) Access revocation/changes are not accomplished within 24 hours of any change in user access status.

1303 (l) Measures (4) Background Screening (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…

1303 (l) Measures (4) Background Screening (ii)…update the listing [of personnel with access to critical cyber assets] within two business days of any substantive change of personnel.

1303 (o) Levels of Noncompliance (1) Level One (ii)…instance of personnel termination (employee, contractor or service provider) in which the access control list was not updated within 2 business days…

1306 (b) Measures (2) Account and Password Management
…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.

Comment 14. 1304 - Question 5 in the Frequently Asked Questions defines strong authentication which is referenced in Standard 1304 as requiring at least two-factor identification. In a controlled

office environment that already has physical access controls in place, it would seem that single-factor identification such as a password would be adequate. Question 5 also states that strong authentication be implemented for interactive access to an electronic security perimeter. This raises a couple of questions:1) Is strong authentication only required for external interactive access? If so, please clarify external access. Is this referring to a remote access connection such as a VPN? 2) Is strong authentication required for interactive access from a network segment outside the electronic security perimeter, but within a controlled office environment that has physical access controls in place?

Comment 15. 1305 - Standard 1305 requires implementation of the necessary measures to control access points to the perimeter(s) and the critical assets within them. This appears to require utilities to put cameras or door alarms on every doorway through which people gain access to locations inside the physical security perimeter. It seems that monitoring a gate at a fenced facility such as a power plant would be sufficient.

Comment 16. 1305 - Under Measures under Logging Physical Access it is stated that physical access logs shall be retained for at least 90 days. It seems that 30 days should be adequate for videotapes.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Kenneth A. Goldsmith	
Organization:	Alliant Energy	
Telephone:	319-786-4167	
Email:	kengoldsmith@alliantenergy/com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT	☒	1 - Transmission Owners
☐ ECAR	☐	2 - RTOs, ISOs, Regional Reliability Councils
☐ FRCC	☐	3 - Load-serving Entities
☐ MAAC	☐	4 - Transmission-dependent Utilities
☒ MAIN	☐	5 - Electric Generators
☐ MAPP	☐	6 - Electricity Brokers, Aggregators, and Marketers
☐ NPCC	☐	7 - Large Electricity End Users
☐ SERC	☐	8 - Small Electricity End Users
☐ SPP	☐	9 - Federal, State, Provincial Regulatory or other Government Entities
☐ WECC		
☐ NA - Not Applicable		

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Bulk electric system facility and critical cyber assets included in this section are further defined in 1302. Suggest defining once and providing further explanation in the FAQ.

The definitions for critical bulk electric system facility and critical cyber asset are not clear. Establishing some additional criteria such as generation over 500 mw and transmission over 230 kv would be valuable.

Remove the separate definition of an Incident and have this standard include only Security Incident. The definition should remove 'could have resulted in' as this is too subjective.

Define Personnel and remove from 1302.

Include IROL definition and remove from 1302.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
See our comments in response to Question 3.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
General

The standard reflects good security practices companies follow for protecting cyber assets. However, the amount of specificity within the standard cannot be applied to all assets and may not need to be applied based on risk assessments and other mitigating controls. The standard should allow exceptions and other controls within levels of compliance.

The numbering and formatting is inconsistent throughout the entire document.

1301 Security Management Controls

Article a-5-iv, Access Revocation Changes should be within 24 hours for cause only. It should not attempt to define when it is removed for other reasons. This should be a documented procedure within the organization regarding review and revocation of access.

Article a-6, Authorization to Place Into Production does not seem to belong in this section and may fit better in 1306 where testing is addressed.

1302 Critical Cyber Assets

Article a-1 and 2 The definitions of bulk electric system facility, critical cyber asset and IROL should be moved to the Definitions section. Other clarification is needed regarding telemetry and common system under Generation

Article a-2-E Remove the statement: Any other cyber asset within the same electronic security perimeter as the critical cyber assets must be protected to ensure security of critical cyber assets. Having to comply with each section of this standard for a non-critical asset is too burdensome. Suggest a reference in Section 1306 to ensure non-critical cyber assets within the same electronic perimeter have appropriate controls to protect the critical asset.

1303 Personnel and Training

Within this section, personnel, employees and contractors are used interchangeably and it is not clear when contractors are included or not included.

Article l-1 Security awareness reinforcement is important but for the standard to dictate and measure quarterly seems excessive. Suggest it state periodic security awareness reinforcement with a focus on annual training of the NERC standard.

Article l-4-i, ii, and iii The first three paragraphs under background screening are covered elsewhere in the standard. Suggest removing from this section.

Article 1-4-v The standard should not address adverse employment.

Article 1-4-vi Requiring background investigations every 5 years for existing employees should occur for performance reasons only. Background investigations for existing employees should be dependent on corporate policy.

Article n-2-i Change Reviews to Security Awareness.

1304 Electronic Security

Article a-1 Stating non-critical cyber assets within the defined electronic security perimeter must comply with the requirements of this standard is excessive. There should be security controls in place to mitigate any impact to a critical cyber asset, but it should not be required to comply with this standard.

Article a-2 Electronic access control devices shall display an appropriate use banner upon interactive access attempts. . . . is good security but it does not seem appropriate for a NERC standard and it is not always technically feasibly. Request it be removed.
.

1305 Physical Security

Levels of non-compliance in this section are inconsistent with 1306.

Article b-4 Change Alarm Systems to be Access Control System.

Article b-5 If the only method used for logging physical access is video, unable to meet 90-day retention with digital video systems.

1306 Systems Security Management

This section has good security principles and appears to have been written for control centers and energy management systems. The same principles may not be applied to all critical cyber assets in generation and transmission. Proprietary software and vendor maintained software require a different set of controls. Test systems may not be an option, mal-ware may not be supported on each system, audit trails not available.
Because of the various types of systems, the levels of compliance are not feasible.

Suggest a reference to ensure non-critical cyber assets within the same electronic perimeter have appropriate controls to protect the critical asset.

Article a-3 Security patch management is a risk based decision and not all critical cyber assets have the same level of risk. If a patch is not installed, it should be documented and a compensating measure may not be required.

Article a-5 Remove “(controlled penetration testing)” as this could cause more risk to the asset.

Article b-2 Account and Password Management should be removed from this section as it is already addressed in 1301.

1307 Incident Response Planning

Only security incidents should be reported. Remove any language that differentiates between incident and security incident.

1308 Recovery Plans

Article a-3 Updating recovery plans within 30 days of system change is unreasonable. Should just state recovery plans are to be maintained.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Howard F. Rulf	
Organization:	We Energies	
Telephone:	262-574-6046	
Email:	Howard.Rulf@we-energies.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☒ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☒	3 - Load-serving Entities
	☒	4 - Transmission-dependent Utilities
	☒	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Recommend the following alternative definitions:

"Incident": Delete this definition.

"Security Incident": Any malicious act or suspicious event that compromises or was an attempt to compromise the electronic or physical security perimeter of a critical cyber asset; or, disrupts or was an attempt to disrupt the operation of a critical cyber asset.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
Cyber Security Standard 1300 should be dealing with Cyber Security Incidents only.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
Section 1302, Critical Cyber Assets item 2 (D). Please clarify what is meant here. Dos this statement mean a computer that is used to access a critical cyber asset via remote access (dial up) does not have to be included in the physical perimeter? Also, in the same section under measures, risk based assessment, the current NERC risk evaluation standard should be referenced as a guide.

Section 1303, Personnel and Training. We question the requirement to provide all individuals who have access to critical cyber assets to undergo the same levels of awareness and security training. Those individuals who have logical access to critical cyber assets should undergo more rigorous training around cyber security and awareness than those who only have access to the physical location where the cyber assets reside (example: janitorial staff). Strongly recommend that individuals with unescorted access to critical cyber assets on the day the revised requirements become effective should be granted continuing access (grandfathered) without the need for a background investigation. No periodic re-investigation should be required.

Standard 1305. Regarding "an in-depth defense strategy to protect the physical perimeter", what's considered "in-depth"?

Section 1306, Systems Security Management, item 5, Identification of vulnerabilities and responses. Can the annual vulnerability assessment be performed by internal staff? Will only an external, impartial auditor be accepted? Also, this section may not be applicable for power plant and substation control systems due to their proprietary nature and age. A different systems security management section may be warranted to address these instances.

Standard 1307, Sect. a4. Based the definition of an Incident, we would need to report all activities that disrupt functional operation of a cyber asset. This could include such operational items like server reboot after applying a patch. The ISAC would be flooded with these "incident" reports. Reporting should be limited to only security incidents. Strongly recommend that reporting only be required for incidents with malicious intent or of suspicious nature, whether physical or cyber. As written, the section requires reporting of incidents which may result from an equipment failure or software configuration error which have no genesis in an act against the entity. These are likely to be more numerous than actual attacks creating a reporting burden as well as yielding no value to the entity. Non-security related events should be outside the scope of the standard, in any case. Re-edit the section to embrace the amended definition of "security incident" above. The CIPC may have to amend the IAW SOP to recognize its reference by the 1300 standard to ensure harmony between these two documents.

General observations, comments and questions:
Compliance will have a financial impact for entities covered by the standard.
Identification of bulk electric system assets and performing a risk analysis with documentation will require resources and time to complete. Full compliance may not be achievable in the near term.
NERC should keep the scope of what's included as critical cyber assets the same as interim standard 1200 until we gain more experience with compliance and certification.
Who is going to determine whether an entity has defined their Critical Cyber Assets and Bulk Electric System Assets appropriately?

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Seiki Harada	
Organization:	BC Hydro	
Telephone:	604 623 3550	
Email:	seiki.harada@bchydro.com	
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT** ☐ **ECAR** ☐ **FRCC** ☐ **MAAC** ☐ **MAIN** ☐ **MAPP** ☐ **NPCC** ☐ **SERC** ☐ **SPP** ☒ **WECC** ☐ **NA - Not Applicable**	☐ ☐ ☐ ☐ ☒ ☐ ☐ ☐ ☐ ☐	1 - Transmission Owners 2 - RTOs, ISOs, Regional Reliability Councils 3 - Load-serving Entities 4 - Transmission-dependent Utilities 5 - Electric Generators 6 - Electricity Brokers, Aggregators, and Marketers 7 - Large Electricity End Users 8 - Small Electricity End Users 9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☒ Yes

☐ No

Comments

Some of these standards are dependent upon definitions or glossaries developed elsewhere by the NERC committees. For example, “bulk electric system” and “Interconnection Reliability Operating Limit” are defined outside CIPC (The NERC Critical Infrastructure Protection Committee). The NERC members must realize that any shift in the definitions outside CIPS may undermine the original intent of the Cyber Security Standards, with no wording changes to the Cyber Security Standards. Hence any shift in definitions should be cross-checked with interpretations in all standards in which the terms appear.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
I suggest we deal with the points raised in Question 3 next, before putting it to ballot.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

1) BC Hydro continues to support NERC's effort to represent the North American electricity industry in standard setting, and to help uphold the reliability of bulk electric systems via implementation of a set of cyber security standards.

2) The acceptance of the NERC functional model (that describes the roles and responsibilities of entities such as Reliability Authority, Balancing Authority, Buying/Selling Entity, etc.) is essential to the implementation of the compliance monitoring. If the model was not endorsed nor implemented by NERC, the NERC 1300 standards may become a voluntary compliance guide, rather than standards.

3) Regarding 1301 (a) (5) (iii), consider adding the condition to review access rights/privileges at least once a year.

4) Regarding 1302, (i) (1), change the wording to reflect that the compliance monitor may also use scheduled on-site visits of no more frequently than every three years.

5) Regarding 1303 Personnel & Training, Canadian law generally prohibits, and makes it an offence, to use or even communicate the Social Security Number (in Canada called Social Insurance Number) for any purposes other than as required or authorized by law in connection with the administration or enforcement of the Income Tax Act (Canada). Hence, the words "Social Security Number" should be replaced with "an appropriate identity".

6) 1306 System Security Management describes Security Patch Management. This section talks about tracking of all patches applied. These are necessary actions. However, in order to make this management process complete, there should be a log of ALL pertinent security patches published by respective software manufacturers, or all published vulnerabilities regardless of the availability of patches from the manufacturer, and their disposition. . An entity may accept some of these as a reasonable risk to take and do nothing except to log the decision, while others will take some defensive measures and require being logged. The evaluation results and the management decision/disposition should be logged in all cases.

7) Still on the same section, there is a requirement for "Backup and Recovery". These are again necessary functions. In addition, though, there must be a viable "disaster response plan" ready and maintained in case of a major catastrophe that may render mere backup and recovery irrelevant.

8) There are a number of structural inconsistencies in the draft. For example,

Regarding 1302 (a) (2) (i) (E), what is 1302.1.2.1 referring to? The paragraph designation format includes letters and numbers.

Regarding 1302, the first section is lettered (a) and the next section is lettered (g), instead of (b).

Regarding 1303, the first section is lettered (a) and the next section is lettered (l) instead of (b).

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Robert V. Snow P.E.	
Organization:	Robert Snow	
Telephone:	973 763 0832	
Email:	FamilySnow@aol.com	
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT** ☐ **ECAR** ☐ **FRCC** ☒ **MAAC** ☐ **MAIN** ☐ **MAPP** ☐ **NPCC** ☐ **SERC** ☐ **SPP** ☐ **WECC** ☐ **NA - Not Applicable**	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☒	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

The definition of the bulk electruc system should include a voltage definition similar to previous NERC definitions. The typical is to define systems equal to or greater than 100 kV. An additional descrioption are systems that are contained in a FERC tariff for jurisdictional entities or as defined in the applicable documents for others.

Add a new definition for intrusion Assessment. It is an analysis by an independent entity that attempts to defeat the security systems being defined. It is a standard practice in the cyber industry and other parte of the electric utility industry.

Question 2: Do you believe this standard is ready to go to ballot?

☒ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
This document is much better than the proor document. It could use to include some actual testing of the systems proposed. Suggest adding:

1. The requirement for an Intrusion Assessment by an independent agency once every three years with the requirement that any vulnerabilities be remedied within three months.
2. Adopting a "defence in depth" approach rather than what reads like one barrier around the system and nothing after an entity gets past the first barrier.
3. A network for information sharing about events and lessons learned between the cyber entities.

In the Roles and Responsibilities:

Senior Management of the respective entity must be responsible for providing sufficient resources (people and funding) to achieve the identified program and to provide additional resources to remedy any incidents or vulnerabilities that are identified.

These standards should apply to all control rooms that have a role in performing the functions in 1302 (a) (1) (i). They would include backup facilities and secondary control rooms.

In Electronic Security

Add denial of service protection as well as how to protect against transmisisons not originating from the authorized control centers. The first would stop a control center form taking actions and the second would protect against others from operating the systems independent from the authorized control center.

There should be some level of redundancy required to assure the systems function as required independent of cyber activity.

PHysical:

In locations that are not normally occupied, there should not be documents, prints, systems descriptions or other detailed information that would aid someone understand how the system operates or to bypass the intended safeguards in the system.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
The previous comments need to be integrated into the body of the standard in a number of locations.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:		
Organization:		
Telephone:		
Email:		
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT** ☐ **ECAR** ☐ **FRCC** ☐ **MAAC** ☐ **MAIN** ☐ **MAPP** ☐ **NPCC** ☐ **SERC** ☐ **SPP** ☐ **WECC** ☐ **NA - Not Applicable**	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name: Cinergy

Lead Contact: **Larry Conrad**

Contact Organization: **Cinergy**

Contact Segment: **3**

Contact Telephone: **+1 317-838-2022**

Contact Email: **Larry.Conrad@Cinergy.com**

Additional Member Name	Additional Member Organization	Region*	Segment*
Doug Hils	**Cinergy**	**ECAR**	**1**
Walt Yeager	**Cinergy**	**ECAR**	**6**

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
See additional comments

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
Cinergy Comments to NERC Regarding DRAFT of Standard 1300

Cinergy thanks NERC for initiating Standard 1300 language to address a permanent standard for cyber security. Cinergy also recognizes the need for cyber security controls and supports the industry wide effort which began with Standard 1200. While the Cinergy comments are extensive, they are submitted in the spirit of creating the best security standard possible. Each Section of Standard 1300 is addressed individually.

General Comments

Definitions need to be clear and consistent from one NERC document to the next if a true "consensus" throughout the industry is desired by NERC prior to balloting. Because documents such as Version 0 glossary, Standard 1300, and the Risk Assessment are all being developed simultaneously, it is difficult to get a consistent understanding of what participants are being asked to agree to. Examples include but are not limited to (1) Version 0 seems to have a different interpretation of Bulk Electric System than the way it is used in Standard 1300 (2) Risk Based assessment document, part of the criteria to identify the critical cyber assets, is not yet published (3) Version 0 defines a "Reportable Disturbance" as subject to regional interpretation. Cinergy believes such a regional interpretation will be problematic for Standard 1300 language.

By placing additional security restrictions/costs on routable (IP) technology, NERC will (in effect) slow the migration from older technologies to more flexible future technologies involving (IP).

During the Standard 1200 process, the NERC Responses to the Ballot Comments provided a different definition than the language contained in Standard 1200 in some cases. Example: Standard 1200 clearly stated an "isolated" test environment was required. NERC Responses clearly stated that an "isolated" test environment was NOT required. This led to mis-understandings about what the real requirements were. Although the Standard 1300 process is young, there appears to be too much reliance on the FAQ's to embellish the requirements. Documents, such as the FAQ's, should be used to provide examples. The intent of the requirements should be fully explained in the Standard 1300 language, not the FAQ's.

Cinergy is concerned that requirements, such as excessive documentation, will mean that resources are utilized to comply with requirements that do not truly enhance actual security.

Cinergy believes that some estimate of the costs vs. the benefit of the requirements must be understood before moving toward implementation.

Also, NERC needs to change the dicument style to be crisp, clear, and readable. See comments by Larry Conrad posted 10/22/04. Use the complete number reference in front of each clause.

General Question

If a company goes through the process and finds that it has NO critical cyber assets, does that company have any additional obligations under Standard 1300? If so, please explain.

Definitions Section

Page 1
The definition of "Cyber Assets" (on page 1 of the draft) is vague and leaves room for interpretation, and how it is interpreted could have drastic impact. The term "cyber" in the heading implies computerized equipment, particularly that which can be networked together via electronic communications, however the definition does not specifically state that. Cinergy seeks clarification from NERC regarding "non-computer" devices such as protective relays, solid-state transducers, etc. that are not networked nor communicated to in any way.

Definitions section needs to clearly define “routable protocol” in the definitions including what is a routable protocol and what is not a routable protocol. While the definition may be familiar to many, this concept is key to identifying the critical cyber assets, yet no definition is provided.

Definitions section also needs to define “dial up accessible” for same reasons noted above.

1301 Security Management Controls Section

Page 3: Several sections of 1301 will require coordination at executive level across business units throughout corporations. These types of sweeping administrative documentation requirements will prove extremely time consuming and, therefore, expensive to implement under the proposed 1300 language. Some are already inherent in the organization charts, operating procedures, and job descriptions of the corporation. Standard 1300, as proposed, will simply create redundant corporate documentation in these cases because (while documentation may exist) it may not be in a format readily available for Standard 1300 audit review. If no relevant threat information exists or the costs and benefits do not warrant implementation, Cinergy recommends section such as those listed below be eliminated or modified.

Governance section, which requires entities to document structure for decision making at executive level.

o The Cyber Security Policy section of 1301 requires that senior management acknowledge responsibility for cyber security. Therefore the ‘decision making’ at the executive level is covered in the Policy section, making the governance section un-necessary.

Roles & Responsibilities requiring participants to “maintain in its policy the defined roles & responsibilities…”

o If The Roles & Responsibilities section is not deleted entirely, then at least delete the second paragraph: ‘The responsible entity shall also define the roles and responsibilities of critical cyber asset owners, custodians, and users…identified and classified in section 1.2’. From the existing numbering system used, it is not clear what “1.2” refers to.

Page 4: “Authorization to Place into Production,” part of Section 1301, requires entities to “identify the controls for testing…and document that a system has passed testing criteria.” Cinergy agrees that a testing procedure is required. However 1301 language as proposed requires redundant documentation over and above requirements as spelled out on p. 26 and 28 in the “Test Procedures” part of Section 1306. Section 1306, “Test Procedures” (p. 28) states “…change control documentation shall include records of test procedures, results of acceptance of successful completion…documentation shall verify that all changes to critical cyber assets were successfully tested…prior to being rolled into production…” Recommendation: Section 1301 authorization to Place into Production section (for the most part) is redundant to Section 1306 Test Procedures. If

the following sentence was added to Section 1306, Test Procedures, then all of "Authorization to Place into Production" section could be eliminated. "Responsible entities shall designate approving authority that will formally authorize that a system has passed testing criteria." Appropriate references to associated non-compliance items would also have to be eliminated.

NERC's recently published FAQ's on Standard 1300 actually adds additional issues. Standard 1300 calls for "…entities to...identify controls…designate approving authorities that will formally authorize and document that a system has passed testing criteria….approving authority shall be responsible for verifying that a system meet minimum security configurations standards." There is nothing in the Standard 1300 which states the approving party cannot be an operator, programmer, or owner of the system. Yet in the FAQ for Standard 1300, NERC states " …assign accountability to someone other than the operator, programmer, or owner of the systems to ensure that …" testing has been completed. It appears that NERC is adding yet more requirements, ie., (separation of duties,) through the use of FAQ posting. Cinergy recommends that if requirements are not spelled out in the Standard language, additional requirements (such as this type of separation of duties) should not be introduced via the FAQ publications.

Page 4: Access Changes: By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 & 1306)
Need clarification & consistency from NERC on exactly WHAT the access change requirements are.

- 1301 states: "Responsible entities shall… ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."
- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)… and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.
- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who…are not allowed access…(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.
- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations…24 hours.

Further on the subject of Access requirements, commentors stated that the 24-hour access limitation for updating records was un-duly severe in the Standard 1200 comments. NERC Responses to Cyber Security Standard 1200 Ballot Comments 6-11-03 posted to the NERC website provided the following:

"NERC acknowledges the validity of these comments and will address them more fully in the final standard... we will expect that a system will be in place to periodically update access authorization lists on at least a quarterly basis. That protocol will also ensure that access be suspended as soon as possible and no later than 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems. Routine administrative changes resulting from retirements, resignations, leaves, etc. should be handled within the normal course of business but not in excess of three business days after occurrence…."

While Cinergy acknowledges that Standard 1300 is a different standard from 1200, we wish to remind NERC of the statement that they will address objections to the excessively stringent 24

hour access update requirement in the 'final standard." Since objections have not been addressed, NERC still needs to do this.

Regarding requirements for updating access records, Cinergy recommends:
(1) The requirement should be stated as recommended by NERC above 'Access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat…Routine administrative changes …should be handled within three business days after occurrence."
(2) The requirement should only be defined in one section of the document rather than currently proposed language which includes multiple conflicting requirements within the same Standard.
(3) If the item is used to identify non-compliance, all references throughout the document should reflect the revised requirements.

Page 3: (a) (2) (i) "The responsible entity shall identify "all" information, regardless of media type, related to critical cyber assets." It is impossible to certify that ALL information is identified and protected. Cinergy recommends that the word "all" should be deleted and language changed to: "The responsible entity shall identify information related to critical cyber assets."

Page 3: Cinergy seeks guidance from NERC regarding the minimum levels of 'protection' to be afforded this information.

Page 7: Levels of non-compliance, particularly for Level four are excessive. There are eleven (11) different items identified that can trigger a non-compliance item. This is far too many non-compliance triggers, and too burdensome. Recommendation: If the sections on Governance and Roles & Responsibilities are omitted as suggested above, then these items will also be omitted from Levels of Non-compliance, making the document manageable: Level 2 delete (iii); Level 3 delete (iv); Level 4 delete (iv), (v), (vi), (viii). If Governance and Roles & Responsibilities sections remain part of the document, then NERC should select 2 to 4 items from the list of 11 Level 4 triggers that will provide an indication of compliance and delete the remainder.

Page 7 (4) (xi) The item which seeks a violation if one access change is not accomplished within 24 hours needs to be either eliminated or else modified to reflect the above recommendation that a violation is only warranted if the access is not suspended in 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems.
1302 – Critical cyber assets
Page 10: Critical Cyber Assets: "…the cyber asset supports a critical bulk electric system asset." Examples: Environmental and performance software supports generation assets but is not critical to continuation of power. In the 10/18 Webcast, NERC used the word "control" rather than "supports". Cinergy recommends that the word "supports" be changed to reflect the intent that the cyber asset is essential to continued operation of the critical bulk electric system asset, i.e., loss of that cyber assets causes loss of the critical bulk electric system asset.
Page 10: "Critical Cyber Assets", as defined on page 10 of the draft, narrows the definition to cyber assets that "support critical bulk electric system assets" AND "uses a routable protocol" or "is dial-up accessible". Because a proper understanding of what constitutes a critical cyber asset, Cinergy has several questions and seeks clarification from NERC on protocols in use throughout the organization today as well as protocol proposed for the next generation of communication from remote locations to Cinergy's Energy Management System.

Cinergy interprets Standard 1300 to exclude devices such as remote terminal units that communicate over dedicated point to point communication circuits. An example of this would include RTU's communicating via Landis & Gyr 8979 RTU protocol over 4-wire dedicated Bell 3002 circuits.
Cinergy seeks clarification on the following:

Cinergy currently uses a "non-routable" protocol (e.g. Cinergy's current Landis & Gyr 8979 RTU protocol) that are communicated using PVCs (private virtual circuits) over a frame relay network. Cinergy seeks clarification on routable protocol reference and how NERC believes it applies here.

Cinergy needs clarification on 'routable protocol' reference and how requirements apply to proposed use of "DNP over IP" using frame relay.

Cinergy seeks clarification of the 'dial up accessible' reference regarding DNP.

Is an electronic relay interpreted by NERC to be a computerized cyber asset?

If a relay is constructed to allow remote data retrieval but prohibit any configuration changes, is it excluded from the requirements?

Page 9 Generation: Proposed Standard 1300 references other documents (Policy 1) that are open to interpretation by Regional Councils. Rather than spelling out the rules for generation that needs to be considered a Critical Bulk Electric System Assets, Standard 1300 refers to another document (Policy 1.B). ECAR has modified the definition of "Most severe single contingency".

Using the proposed Std 1300 language from the multiple documents and regional definitions mean that almost all Cinergy's generating facilities fall under the rules of Standard 1300.

Is it NERC's intent that all generating stations should be subject to the rules of Standard 1300? If this is not NERC's intent, then the proposed language needs to be changed.

Cinergy recommends that all of the rules for identifying the critical bulk electric system assets and the critical cyber assets should be identified in one document, rather than using multiple documents subject to regional interpretations as used in Std 1300 version 1. Recommendation: On page 9, eliminate reference to NERC Policy 1.B in (iii) (A) and replace with this language: "…greater than or equal to 80% of the most severe single contingency loss."

Cinergy seeks clarification from NERC of the term "Most severe single contingency". Please use the following example:

Utility owns approximately 600 MW of a total 1300 MW generation site all in ECAR
Same utility owns 100 % of a 635 MW generation site

Which of the above should be identified as the largest "single contingency"? If the 635 MW site is used, generating units, which Cinergy does not consider critical, will be included in the list of "critical cyber assets."

Cinergy recommends that a good use for the FAQ's would be to provide additional examples, including some examples using how the requirements apply to jointly owned units (JOU's).

Page 9: Either fully explain or eliminate (iii) Generation (B) "…generating resources that when summed meet the criteria…"

Page 10: Cinergy believes the level of documentation and administrative control required by proposed Standard 1300 is extensive and imposes a significant operating cost on participants. Once again, this section contains requirements without any documented evidence that the expense to implement will enhance security or that there is a relevant threat, which will be mitigated by this level of documentation. Parts of the section are redundant to other requirements. Cinergy has designated two company officers that are responsible for the Cyber Security Policy and implementation. "Critical Bulk Electric system Asset and Critical Cyber Asset List Approval section," requires a properly dated record of senior management officer's approval of the list of critical bulk electric system assets. Cinergy recommends that requirements such as this be deleted unless evidence is shown which indicates direct security benefit. Recommendation: Eliminate Requirement (a) (3) " …A sr. management officer must approve the list of…" and also eliminate corresponding "Compliance Monitoring Process" (i) (3) (iv) page 11. The senior officers are responsible for implementation of the program and should not be required to sign off on each section of the document as each section is updated.

In the October 18 Webcast, NERC slides indicated a "3 step" approach to identifying the critical cyber assets. Standard 1300 lists (#1) Identify the Critical Bulk Electric System Assets and (#2) Identify Critical Cyber Assets. Cinergy seeks clarification from NERC regarding the three (3) steps referred to in the Webcast.

1303 – Personnel & Training

Page 13 "Awareness Program": Once again, this section contains requirements without any documented evidence that such requirements will enhance security. Requiring both training program and awareness program seems redundant and burdensome. Cinergy recommends that the awareness in inherent in training and is part of the training requirements. We recommend that the separate "Awareness" section be deleted.

Page 14 Access Changes:
By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1301 & 1306)
Need clarification & consistency from NERC on exactly WHAT the access change requirements are.

- 1301 states: "Responsible entities shall… ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."
- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)… and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.
- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who…are not allowed access…(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.
- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations…24 hours.

Regarding requirements for updating access records, Cinergy recommends:
1. The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they

pose a threat…Routine administrative changes …should be handled within three business days after occurrence."
2. The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.
3. If the item is used to identify non-compliance, all references throughout the document should reflect the revised requirements.

Page 14: Background Screening. The entire section on background screening, as written in Standard 1300, is problematic. For example:
- "…A minimum of Social Security Number verification…" Language as written will deny access to anyone except U.S. citizens. Cinergy recommends that the language requiring a social security number be deleted unless it is NERC's intent that only U.S. citizens and no one else is granted electronic or physical access.

NERC showed insight when, in their Responses to comments submitted during the balloting of the Urgent Action Cyber Security Standard 1200, NERC wrote: "…organizations are NOT required to conduct background investigations of existing employees given the fact that they have had the opportunity to observe and evaluate the behavior and work performance of those employees after they have been employed for a period of time." Cinergy again recognizes that Standard 1300 is a different standard from Standard 1200; however, the logic that provided the foundation for the previous NERC comment is sound. If the company has had an opportunity to observe the long service employee, the background screen requirement should be relaxed.

Cinergy recommends one of the following to replace proposed Standard 1300 language:
A. The requirement should include background screening for all individuals (employees and vendors) who seek approval for new permanent access to critical cyber assets.
Background screening on existing employees, previously approved for access, is appropriate if there is cause to suspect the individual of suspicious behavior.
Requiring the screening of all personnel every 5 years should be deleted.
B. If the above proposed language is not acceptable as an alternative by NERC, then Cinergy recommends language be inserted indicating that background screening requirements will be evaluated by the company involved, and the policy toward such screenings will be documented by that company. Company will be free to document policies such as: At Company's discretion, long service employees, which the Company has observed, may be grandfathered and background checks will not be done on these employees. Company will not be found in non-compliance for such a policy.

Page 13: Language states that a "higher level of background screening" should be conducted on personnel with access. Cinergy's background screening for new hires complies with the NERC requirements and other legal requirements. Cinergy does not agree that multiple levels of background screening are required. Cinergy recommends that the reference to multiple levels of background screening be deleted.

Page 13: Records: " …background screening of all personnel having access to critical cyber assets shall be provided for authorized inspection upon request." Cinergy does not agree that the background screen information obtained on all its employees will be provided to NERC inspectors. In the 10/18 Webcast NERC stated that it is not their intent that the contents of the background screening be provided to the inspectors. Recommendation: Improve language so that it is clear that contents of background screen need not be divulged to inspectors.

Page 15 (i) Standard 1300 language implies that background check lists & verifications are kept by operations groups responsible for the cyber security implementation. Such records will continue to be maintained by the Human Resource Department at Cinergy.

Page 13: Background screening: Proposed language states: "…contractors and service vendors, shall be subject to background screen prior to being granted unrestricted access to critical assets." Is it NERC's intention that they be granted unrestricted access after completing a background screen as stated in 1300?
1304 – Electronic Perimeter
Page 17 (a) (1) Electronic Security perimeter: Proposed language states "Communication links …are NOT part of the secured perimeter…However, end points of the communication links… are considered access points to the perimeter. Where there are non critical assets within the defined perimeter these non-critical assets must comply with the requirements…" Language is contradictory and confusing. Proposed language makes the asset and the end point critical assets and within the perimeter, but language excludes the communication line between them. The next sentence implies the communication line needs to be treated as though it is part of the perimeter. Cinergy seeks clarification.
Page 18: (b) (1) Electronic Security Perimeter:
Cinergy seeks clarification regarding from NERC regarding Frame Relay Access Devices (FRAD's) and modems connected to cyber assets. Are these considered "access points to the electronic security perimeter"?

If the FRAD's are considered 'within the perimeter' with the resulting requirements extending to the FRAD's, this is an excessive and unnecessary level of detail and will prove costly and burdensome without proven corresponding benefit.

Page 18: Measures (3): Monitoring Electronic Access Controls: Wording of this section, particularly the last sentence, is very confusing and needs clarification regarding exact requirements for documentation and for implementation of monitoring the access controls.
P. 19 (e) (3) Electronic Access Controls: Page 19 identifies a non-compliance item if "…not all transactions documented have records." Cinergy seeks clarification. If a transaction is documented, by definition, doesn't that mean the transaction has a record?
Page 17 Electronic Access Controls: "…non critical cyber assets (within the perimeter) must comply with the requirements of this standard." Different departments within the organization will handle different functions. Current language implies one rigid process to apply to both critical assets and non-critical assets, which may exist within the perimeter. Recommend that this be changed to: non-critical cyber assets within the perimeter must utilize similar electronic access controls.
1305 – Physical Perimeter

While Cinergy acknowledges that controls may be required, it does not seem appropriate for NERC to dictate the controls to be implemented. Example: Implement CCTV or Alarm System.

Cinergy's interpretation of current draft language in Section 1302 will result in almost all Cinergy generating plants being subject to these rules. Section 1305 then seeks to name the controls, which must be implemented at each asset location. No mention to a review of costs associated with such sweeping changes is even mentioned in any of the language. Cinergy believes it is appropriate to address the costs and corresponding benefits before moving forward with such a sweeping and costly initiative. Cinergy recommends that participants and NERC develop an estimate of the proposed cost to the industry before finalizing these requirements.

Generating plants control rooms may be manned 24 hours a day seven days a week. Cinergy seeks clarification and evidence of the need for the many controls, such as CCTV, which are specified in the document in these cases where facilities are manned.

Page 24 (6) Maintenance and testing of security systems to be retained for 1 yr. This involves corp. wide – Equipment Maintenance area. This is one more example of the costs, which must be considered before moving forward. These types of requirements are very costly to large organization because they impose enterprise wide requirements. Maintenance records on the security installation equipment will not be kept in Electric Operations areas. Requirements will need to be coordinated across groups responsible for equipment maintenance.

1306 – System Security management

While the list of physical controls to be implemented in the proposed section 1305 language represents a huge, solid, and obvious cost burden, requirements in section 1306 represent a less obvious but huge cost burden as well.

Once again, there is no evidence presented that there is a relevant threat, which will be mitigated, if these types of controls/documentation requirements are implemented. Also, once again, there is no indication if the idea of associated costs was even contemplated prior to writing the language requiring the controls/documentation.

Cinergy requests that evidence needs to be presented showing (1) a relevant threat will be mitigated if the controls outlined in this section are implemented (2) costs and benefits associated with requirements have been identified.

Cinergy is concerned that if money and resources are required for documentation requirements that yield no real enhancement to security, then less money and resources will be available for security measures that could truly yield benefit. Recommendation: Either significantly lessen requirements or eliminate many of the following.

- Page 28: Archive backup information for a prolonged period of time and then test it annually to ensure it is recoverable. A definition of 'information' and 'archival information' should be provided. Archived information looses its value in time and may become irrelevant. Is NERC dictating records retention policy? What is the consequence if this does not occur? Requires extra work, but what is the point? Need better understanding of costs vs. benefits.

- Page 28: Create Operating Status Monitoring tools. This section indicates the tools gauge 'performance.' Standard 1300 language contains no statement as to what these performance-monitoring tools are trying to gauge nor are any performance goals indicated. This would be costly to implement with no defined benefit or even goals for the tools. Requires extra work, but what is the point?

- Page 28: Create Operating Status Monitoring tools: Language in the section implies that performance documentation is to be kept for every asset. This is not reasonable.

- Page 27: Retention of system Logs: "All critical cyber security assets must generate an audit trail for all security related system events." In the case of local RTU's this is probably not possible.

• Page 26: Test Procedure language as written is overly burdensome. Language implies that EVERYTHING needs to be tested. It is not realistic that EVERY minor change is documented in formal testing. FAQ's seem to conflict with Std. 1300 proposed language. Recommendation: Modify Standard 1300 language to imply levels similar to NERC's recent Standard 1300 FAQ posting.

• Page 27: Testing "…provide a controlled environment for modifying ALL hardware and software for critical cyber assets." Since the Energy Management System is by nature a critical cyber asset, the language implies that EVERYTHING must be modified in a separate controlled environment. Current language is burdensome and not practical. Recommendation: Indicate a reasonable level for testing within the controlled environment. Use levels similar to those identified in NERC's recent Standard 1300 FAQ posting.

• Page: 27 Test Procedure Measures: Language states, " …Critical cyber assets were tested for potential security vulnerabilities prior to be rolled into production…" It is unclear what 'potential vulnerabilities' are to be tested or how the tester is to know about them. Recommendation: Explain clearly or delete the reference.

• Page 29: Integrity software: Cinergy is pursuing a course of isolating the Energy Management System from the corporate network. This path of isolation reduces threat from email, Internet use, etc. The language requires anti-virus versions be kept immediately up to date. In practice, this conflicts with the work to isolate the EMS and presents un-necessary requirements since the EMS will be isolated from the source of the viruses.

• Page 27: Security Patch Management: Cinergy seeks clarification of " …upgrades to critical cyber assets." If this language includes every upgrade, it is costly and over-burdensome without resulting security benefit.

• Page 27: Created formalized change control & configuration management process: Entire section creates un-necessary and redundant requirements that are included in the Test Procedures requirements section of 1306.

Section 1306 Security Patch Management section presents additional problems for power plant control systems. For example,
• Security Patch Management language (page 27) requires timely installation of applicable security patches and operating system upgrades.
• Patches and upgrades (at the power plant) at Cinergy can only be applied during an outage of the control system.
Cinergy seeks clarification from NERC as to how all of Section 1306, including Security Patch Management, applies to power plant control systems. Will plants be expected to create more outages to keep up with requirements?

Page 28 (2) Account Management: "review access permissions within 5 working days. For involuntary terminations, …no more than 24 hours". By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 & 1301)
Need clarification & consistency from NERC on exactly WHAT the access change requirements are.
- 1301 states: "Responsible entities shall… ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."

- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)… and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.
- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who…are not allowed access…(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.
- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations…24 hours.

Cinergy recommends:
- The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat…Routine administrative changes …should be handled within three business days after occurrence."
- The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.
- If the requirement is used in the non-compliance section, then the non-compliance section should be consistent with revised requirements.

1307 & 1308- Response & Recovery Plans

Page 34:
1300 Language seems to imply NERC expects multiple plans to be created for Cyber Security. " …recovery plans associated with control centers will differ from those associated with power plants and substations." This level of detail may become too onerous. Cinergy seeks clarification from NERC if multiple plans are required. Once again, this will involve time, money and resources to create documentation at an un-precedented detail level with no indication that such a measure will increase real security.

If entities strictly follow the language proposed for 1307, they will be forced to create un-necessary documentation for very brief interruptions and for events, which were not malicious and did not create a disruption. NERC definitions provided the following:
- NERC defines an "incident" as ANY physical or cyber event that disrupts or could lead to a disruption of the critical cyber assets.
- Same section defines a "cyber security incident" as malicious or suspicious activities, which cause or may cause an incident.
- Definition section does NOT include a definition of a "reportable incident"

The language of the entire 1307 section is written to apply to both incidents and cyber security incidents.
Once again, as we have seen in other sections, companies that attempt to follow these requirements will create costly levels of detail and documentation (for every incident which either creates a slight disruption or could lead to a disruption) with no proven direct benefit to security. Here are some examples:

• Page 32 states, "…retain records of incidents and cyber security incidents for 3 calendar years." This includes but is not limited to:
o System and application log files
o Video and or physical access records
o Investigations and analysis performed
o Records of any action taken including recovery actions
o Records of all reportable incidents and subsequent reports
• …make all records and documentation available for inspection."
Recommendation: Re-work the language so that it is clear at what level this degree of detailed documentation needs to be retained.

Page 34 (a) (3) "…update the recovery plans within 30 days of a system or procedural change and post the recovery plan contact information." This language is problematic in 2 areas:
1. It is not realistic to expect that the plan will be updated within 30 days of each procedural or system change.
2. Cinergy does not "post" contact information. NERC does not specify what type of "posting" they require. Further this requirement is contradictory to other NERC cyber security requirements. Cinergy regards emergency plans and contact information as critical cyber asset information. Information is treated as such.
Cinergy recommends that plans be updated annually and that contact information should be treated consistent with other information related to critical cyber assets.

Additional Comments on Format
- The numbering sequence is not accurate throughout the document, making it difficult to follow in some sections. Recommendation: A different consistent numbering system should be used or, at the least, the entire document should be reviewed for appropriate numbering. Examples include but are not limited to:
o See Page 9 (a) Requirements then Page 10 (g) Measures. Where are items (b), (c), (d), (e), & (f)?
o Page 13: All of Section 1303 need review
- Typing mistakes need to be corrected. Example: Page 15 "…doesn't not cover one of the …"

FAQ's Recently Posted by NERC

In addition to inserting requirements regarding separation of duties noted above, question 3 on page 9 of the FAQ document seeks to limit the definition of RTU's, that use a non-routable protocol. Standard 1300 implies that non-routable protocols are excluded. However, the answer to question 3 tightens the definition of what is excluded by adding additional requirements that may not apply to all non-routable protocols: "…have a master/slave synchronous polling method that cannot be used to access anything on the EMS and they use SBO command…" As noted above, it is not appropriate to introduce additional restrictions to the Standard language via the FAQ posting process.

Cinergy Implementation Timeline

After the Standard 1300 language and requirements are finalized, Cinergy estimates:

o 1.5 to 2 years to evaluate standard impact and what is to be included in compliance.

- This is dependent upon how much guidance is given by NERC in regards to specifics for equipment and facilities to be included.

- 3.5 to 4 years to implement and become compliant.

- Total of 5 to 6 years from acceptance of the standard until compliance is reached.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Victor Limongelli	
Organization:	Guidance Software, Inc.	
Telephone:	626-229-9191	
Email:	Legal@GuidanceSoftware.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☒ WECC ☐ NA - Not Applicable	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☒ ☐	1 - Transmission Owners 2 - RTOs, ISOs, Regional Reliability Councils 3 - Load-serving Entities 4 - Transmission-dependent Utilities 5 - Electric Generators 6 - Electricity Brokers, Aggregators, and Marketers 7 - Large Electricity End Users 8 - Small Electricity End Users 9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☒ Yes

☐ No

Comments

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
In addition to the general statements regarding the need for incident response planning in 1307 (which focus only on "Incident Classification," unspecified "Response Actions," and Reporting), the Standard should detail the technical and procedural requirements for an effective cyber security incident response plan. As written, the Standard would allow each organization to define for itself the appropriate level of incident response actions and incident handling procedures. Unfortunately, this approach lowers the overall grid's reliability. The investigation of, and response to, a cyber security incident involving one or more entities or grids can run aground at the vulnerable organization that does not have an effective incident response capability. Thus, the failure of certain organizations can impact other entities, as well as the overall grid. In short, including within the Standard a baseline level of acceptable incident response capabilities will help ensure the integrity and reliability of the interconnected electric systems of North America.

Fortunately, the Standard need not attempt to develop the appropriate minimum standards. Earlier this year, the National Institute of Standards and Technology ("NIST"), pursuant to authority established by the Federal Information Security Management Act of 2002 ("FISMA"), issued Special Publication 800-61, entitled "Computer Security Incident Handling Guide" (the "NIST Guide," available at http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf). The NIST Guide sets forth detailed techincal, procedural, and policy guidelines for the implementation of a comprehensive incident response capability, consisting of four broad categories: (1) Preparation, (2) Detection and Analysis, (3) Containment, Eradication, and Recovery, and (4) Post-Incident Activity.

By way of example, within the category of Containment, Eradication, and Recovery, the NIST Guide calls for the following key technical processes and methodologies for effective incident response:

1. Immediate response capability. NIST comments: “It is generally desirable to acquire evidence from a system of interest as soon as one suspects that an incident may have occurred.”

2. Initial System Snapshot. In addressing this critical aspect of incident response, NIST correctly notes that: “Many incidents cause a dynamic chain of events to occur; an initial system snapshot may do more good in identifying the problem and its source than most other actions that can be taken at this stage.”

3. Analyze live systems with minimal invasiveness. The NIST Guide notes that without proper procedures, “risks are associated with acquiring information from the live system. Any action performed on the host will alter the state of the machine…”

4. Volatile data acquisition and analysis: The NIST Guide provides: “…it is often desirable to capture volatile information that may not be recorded in a file system or image backup, such as current network connections, processes, login sessions, open files, network interface

configurations, and the contents of memory. This data may hold clues as to the attacker's identity or the attack methods that were used."

5. Forensic hard drive data acquisition. The NIST Guide provides clear direction on this issue: "After acquiring volatile data, an incident handler with computer forensics training should immediately make a full disk image … (which) preserves all data on the disk, including deleted files and file fragments."

6. Computer forensic analysis. Section 3.3.2 of the NIST Guide states: "Computer forensics software is valuable not only for acquiring disk images, but also for automating much of the analysis process, such as:

- Identifying and recovering file fragments and hidden and deleted files and directories from any location (e.g., used space, free space, slack space)
- Examining file structures, headers, and other characteristics to determine what type of data each file contains, instead of relying on file extensions (e.g., .doc, .jpg, .mp3)
- Displaying the contents of all graphics files
- Performing complex searches
- Graphically displaying the acquired drive's directory structure
- Generating reports."

7. Establish a Proper Chain of Custody with a Message Digest Hash Algorithm.

8. Log file acquisition and analysis.

9. Ability to correlate multiple time zones of acquired media.

10. Validated computer forensics technology via courts and independent testing, as stated by NIST: "Evidence should be collected according to procedures that meet all applicable laws and regulations . . . so that it should be admissible in court."

These and the other detailed requirements set forth in the NIST Guide should be applied 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. The Standard can accomplish this by incorporating the NIST Guide by reference. In addition to the benefit of establishing a baseline for each entity's incident response capability, incorporating the NIST Guide has the following advantages: (1) increasing the coordination between entities in the event of a cyber security incident, since each entity's incident response plan will include similar technical processes and procedural steps; (2) providing evidence of due diligence in the event that there is ever a federal investigation of a cyber security failure within the bulk electric system, and (3) standardizing the industry on an approach already required of cetain entities (federal utilities).

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Jack Hobbick	
Organization:	Consumers Energy	
Telephone:	517-788-2427	
Email:	jwhobbick@cmsenergy.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☒	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☒	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☒ Yes

☐ No

Comments

Although we agree, the definitions are incomplete. Definition needs to be supplied for:

Critical Cyber Information

Large Quantities of Customers

Extended Period of Time

Critical Cyber Security Assets (sect 1306, para a.1)

Critical Infrastructure (section 1306, para a.10 and 11)

Question 2: Do you believe this standard is ready to go to ballot?

☒ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
1301 – Security Management Controls

2) Information Protection
The first sentence of section (i) identification should have the word "all" removed, it is impossible to certify that ALL information is identified and protected.
What is meant by maps? Is this maps of our electric system, maps of our buildings that contain the critical cyber assets, etc.

5) Access Authorization
The requirements in section IV Access Revocation / Changes needs to be made consistent with the other sections in the standard. The requirement should be 24 hours for cause, 5 days for other changes

6) Authorization to Place Into Production
Most of this section is redundant with 1306 Test Procedures and redundancy needs to be eliminated, in particular the requirements for redundant documentation.

Levels of non-compliance, there are far too many (11) different items that can trigger a non-compliance item. At a minimum, remove the following items;
(v) Executive management has not been engaged in the cyber security program
(vi) No corporate governance program exists
(viii) There is no authorizing authority to validate systems that are to be promoted to production

1302 – Critical Cyber Assets

1) Critical Bulk Electric System Assets

Our understanding is that the selection of critical facilities is based on each entities risk assessment. The list of facilities included in the standard is meant as a starting point in preparing the risk assessment and does not mean that those facilities have to be on your critical list.

The risk assessment process should allow for the extent in which cyber assets control a critical bulk electric facility (i.e. a large substation with a limited number of dial up accessible relays) while the substation may be critical, the cyber assets are not

iii)Clarification of the use of disturbance reporting NERC Policy 1B Section 2.4 as a selection criteria for generation:
a. Some Reliability Councils have added additional criteria to disturbance reporting
b. What is the impact of particiapating in a reserve sharing group

2) Critical Cyber Assets

A. Should be worded The cyber asset controls a critical bulk electric system asset

D For remote locations such as substations, in addition to dial up access only requiring an electronic perimeter, properly secured devices with a routable protocol should not require or have limited requirements for physical security. The ability to physically secure devices at an unmanned substation is limited and should be used in conjunction with electronic security. Also the ability to physically secure a substation control house or cage at the same level as a control center or computer room is not realistic. Background screening and logging all entrances would be expensive or difficult to enforce.

1303 – Personnel and Training
1) Awareness & 2) Training

Awareness on a quarterly basis will be very burdensome to accomplish. Annual training/refresher is all that is required and the Awareness section should be dropped.

1304 Electronic Security
3) Monitoring Electronic Access Control

An exception should be allowed for those locations that have only dial up access.

The measure for this section is confusing particularly the last sentence.

Section 1304, first paragraph, discusses the assignment of different security levels for the electronic perimeter(s), yet fails to note how these different levels might result in different security requirements. This seems to imply different requirements based on levels might be applied (and should be) yet there is no further discussion.

Section 1304, Subsection (a), Para (3), requires that access, authorized or unauthorized be monitored and detected. This is an unreasonable requirement for many substation equipment installations. Many dial-up-accessable pieces of equipment, such as relays, controllers, etc, that have a limited ability to effect overall system reliability, still might fall into the classification of Critical Cyber Assets. For these pieces of equipment, there is no reasonable solution to providing monitoring or detection. Efforts to attempt to satisfy this requirement, which might require a more network-type of connection, could even increase the susceptibility to unauthorized access. This requirement should either be deleted, or apply only to significant EMS-type or routable-protocol-types of installations.

1305 – Physical Security
It should be stated that this section only applies to locations that use routable protocols.

Section 1305, first paragraph (following the 3 bullets) discusses the assignment of different security levels for the physical perimeter(s), yet fails to note how these different levels might result in different security requirements.

2) Physical Security Perimeter
Need to differentiate between the differences of physical security of the computer/control rooms and the substations/plants.

1306 – Systems Security Management

3) requires that if the "installation of the patch is not possible, a compensating measure(s) must be taken and documented." This sentence is not consistent with the previous one, which recognizes reasons for not installing patches. It should be revised as follows, "installation of the patch is not possible, but necessary, a compensating measure(s) must be taken and documented." It is quite possible that not only might a patch not be installable, but it could be completely unnecessary, as the problem it is intended to fix, is not applicable to the configuration the software or hardware is connected in. In this case, compensating measure(s) are not necessary.

4) Integrity Software
Where available – there are platform availability issues

6) Retention of System Logs
Exportable format is not always possible, some of the legacy systems only have paper

10) Operating Status Monitoring Tools
Implementation plan for this item is new functionality and will need 3 years to implement. This is new requirement and time is needed to gather/implement the tools to accomplish.
This requirement should only apply to Control Room / EMS type applications, not substation and plant systems.

11) Back-up and recovery
What does storage of archival information have to do with security?

1307 – Incident Response Planning

4) This section is written to include both physical and cyber security incidents. This standard should focus on cyber incidents. Any physical incident that impacts cyber assets should be reported as a cyber incident, other physical incidents should be addressed in other standards

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Neil Shockey	
Organization:	Southern California Edison	
Telephone:	626-302-2669	
Email:	neil.shockey@sce.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☒ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☒	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☐ No

Comments

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☐ No

If No, what are the most significant issues the drafting team must reconsider?

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
The "Applicability" section on page 2 should be revised to explicitly exclude nuclear units from the standard as they fall under NRC jurisdiction. In addition, the timelines throughout the standard need to be reconciled as there are variations in the time alloted to cancel electronic/physical access following termination, suspension, transfer, etc.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Everett Ernst	
Organization:	OG&E Energy Corp	
Telephone:	405-553-8102	
Email:	ernstee@oge.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☒ SPP ☐ WECC ☐ NA - Not Applicable	☒ ☐ ☒ ☐ ☒ ☐ ☐ ☐ ☐ ☐	1 - Transmission Owners 2 - RTOs, ISOs, Regional Reliability Councils 3 - Load-serving Entities 4 - Transmission-dependent Utilities 5 - Electric Generators 6 - Electricity Brokers, Aggregators, and Marketers 7 - Large Electricity End Users 8 - Small Electricity End Users 9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

The definition of Security Incident should agree with NIPC-IAW-SOP as known or suspected to be of malicious origin and it should be clarified that Standard 1300 incident reporting applies only to Security Incidents as defined.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
The standard as it is written is too prescriptive, does not make provisions for legacy equipment capability, and requires too much documentation and logging.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
Section 1303 - Need to do away with background screening on a five year interval and require updates for cause only. Only the latest background investigation results need be kept.

Section 1305 - Access control needs are different at attended and unattended facilities. Attended facilities do not need alarms in addition to access controls. Some substations may not need access monitoring in addition to access controls, only a policy to report in to a central location.(Possibly substations w/o breakers or SCADA on a blackstart route) Leeway needs to be given to match the controls/monitoring to the needs.

Section 1305 - Observed log in is not practical at unattended substations. A logbook along with check in to a central location should be sufficient.

Section 1306 - The requirements in this area are excessive. There should be different requirements for the master station equipment and equipment at remote locations. Even on the master, the documentation and logging requirements are excessive. It should recognize not all legacy equipment will have the capabilities described. Note these are desired goals to work toward, with it being a requirement if the equipment has the capability.

Section 1306 - Security Patch Management It may not always be practical to take a compensating measure. The situation should be assessed and documented as to steps taken and why or why not.

Section 1306 - Identification of Vulnerabilities Penetration testing is probably not required or worth the cost. Perhaps a requirement for an annual internal assessment with an outside vendor assessment every three years might be more appropriate.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:		
Organization:		
Telephone:		
Email:		
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT**	☐	1 - Transmission Owners
☐ **ECAR**	☐	2 - RTOs, ISOs, Regional Reliability Councils
☐ **FRCC**	☐	3 - Load-serving Entities
☐ **MAAC**	☐	4 - Transmission-dependent Utilities
☐ **MAIN**	☐	5 - Electric Generators
☐ **MAPP**	☐	6 - Electricity Brokers, Aggregators, and Marketers
☐ **NPCC**	☐	7 - Large Electricity End Users
☐ **SERC**	☐	8 - Small Electricity End Users
☐ **SPP**	☐	9 - Federal, State, Provincial Regulatory or other Government Entities
☐ **WECC**		
☐ **NA - Not Applicable**		

Group Comments (Complete this page if comments are from a group.)

Group Name: Public Service Commission of South Carolina

Lead Contact: **Philip D. Riley**

Contact Organization: **Public Service Commission of South Carolina**

Contact Segment: **9**

Contact Telephone: **803-896-5154**

Contact Email: **philip.riley@psc.state.sc.us**

Additional Member Name	Additional Member Organization	Region*	Segment*
John E. Howard	**Public Service Commission of SC**	**NA**	**9**
David A. Wright	**Public Service Commission of SC**	**NA**	**9**
Randy Mitchell	**Public Service Commission of SC**	**NA**	**9**
Elizabeth B. Fleming	**Public Service Commission of SC**	**NA**	**9**
G. O'Neal Hamilton	**Public Service Commission of SC**	**NA**	**9**
Mignon L. Clyburn	**Public Service Commission of SC**	**NA**	**9**
C. Robert Moseley	**Public Service Commission of SC**	**NA**	**9**

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☒ Yes

☐ No

Comments

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
The Public Service Commission of South Carolina believes that both electronic and physical access to critical cyber assets should be withdrawn coincident with notification to the employee of his/her involuntary termination.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	R. Scott McCoy	
Organization:	Xcel Energy	
Telephone:	612-330-7666	
Email:	richard.s.mccoy@xcelenergy.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☒ MAIN ☒ MAPP ☐ NPCC ☐ SERC ☒ SPP ☒ WECC ☐ NA - Not Applicable	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☒	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☒	5 - Electric Generators
	☒	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*
Doug Jeager	**Xcel Energy**	**MAPP**	**1**

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Critical Cyber Assets definition. The later part of the first sentence "such as…at a minimum" implies that all these assets perform critical bulk electric system functions, which is not consistent with criteria in 1302 (for example, small generators). Removing it is recommended since specifics are addressed in 1302.

The definition of Critical Bulk Electric System assets in 1302 should also be modified, by eliminating item ii), item B) under iv), and item vi. Including substation equipment in this standard is not workable for numerous reasons. NERC should establish a cyber security standard that will advance the cause of security AND be workable to implement. Substation equipment should be captured by utilities under item vii (risk-based assesment) as needed.

Need to include definitions of the terms: Owners, Custodians, and Users. It would be a good idea to include a definition of "Sensitive Information" or something similar that refers to "information pertaining to critical cyber assets…". The idea is to be more definitive about what information should be protected pursuant to 1301 (a)(2).

For the definition of Incident, recommend the phrase "or could have lead to a disruption of" be removed. How would one measure/determine if it "could have" lead to a disruption? It would be interpretted differently by each entity.

For the definition of Incident, the phrase "or was an attempt to compromise" should be eliminated. This will be interpretted by each individual entity and may result in thousands of reports daily.

For the definition of Security Incident, recommend the phrases "are known to" and "or could have resulted in" be removed. They are vague, and would be interpretted differently by each entity.

Responsible Entity. Since definitions are to be included in a separate glossary, rewording the last part of the sentence "as identified in the Reliability Function table of the Standard Authorization Request for this standard" is suggested.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?

1302 Critical Cyber Assets, (a) (1). The standard is not clear whether the Largest Single Contingency for a Reportable Disturbance is specifically for the Entity or the Reserve Sharing Group (as an Entity may belong to a Reserve Sharing Group).

Question: The FAQ defines the MOST SEVERE SINGLE CONTINGENCY as the largest single generator in the system. Does this mean only a single generating unit and not a generating station? What about greater single contingency losses as represented by the transmission facilities (subs, high voltage lines) that carry aggregated power from multiple units in a single station, and therefore carry more power than any individual generators in a Reserve Sharing Group? Wouldn't those facilities then represent the most severe single contingency?

1302 Critical Cyber Assets, (a) (2). The logistics for Items A-E should be clarified; it is confusing.

1302 Critical Cyber Assets, (a) (2). There should be more clarification/restatement of requirements for dial-up cyber assets that do and do not support routable protocols (what requires a physical perimeter and what does not, and what requires an electronic perimeter, and what does not) - is there a typo in 1302 (a) (2) (i) (D): it reads "which do use a routable protocol" - should is say "which do NOT use a routable protocol"?

All required minimum review periods should be a standard period of one year. Having so many review periods and having numerous periodicities is not practicable.

NERC should lean on existing standards including National Institute of Standards and Technology (NIST) Cyber Security standards (See series 800, Computer Security) that are already well-developed and tested, instead of having electric utility people create a whole new set of such standards. Also, as a general comment, the NERC standard seems to have redundancy with other security compliance requirements such as Sarbanes-Oxley, etc, but seems not to be well coordinated with these other standards. Would the NERC standard be served more efficiently if based on existing Cyber Security standards?

Under 1301 (a) (3), the sentence that says "This person must authorize any deviation or exception from the requirements of this standard." should be changed to read "The person that must authorize any deviation or exception from the requirements of this standard must be specified in the responsible entity’s governance documentation."

In several places in the standard, the issue of authorized access and tracking that access is discussed. It is usually unclear if this is meant to include only those that have access with administrative privileges, or if it extends to those that utilize the assets as users (Dispatchers using an EMS, for example). One example of such a gray area can be found in 1301 (a) (5) (ii), for example - but there are many such areas. NERC should not focus on access by those that only

have rights to use the system, and should clarify in all such contexts that the reference is only to those with administrative access.

Section 1303, under Measures (4) (iv) has minimum criteria for types of checks, but this is worthless without requiring some form of denial criteria. While (4) (v) does mention adverse actions, it is not intuitive that this is a criterion for denial of employment based on a set criterion. This should not be prescriptive either, but spelling out that the company should have a written denial criteria that us uniformly enforced should be added for both clarification and to ensure that the purpose of conducting background screenings is accomplished.

Section 1303, Requirement (4) the phrase "prior to being granted unrestricted access to critical assets" should be removed since it conflicts with Section 1305, "When physical perimeters are defined, different security levels shall be assigned to these perimeters depending on the assets within these perimeter(s).

Section 1303, Requirement (4) (vi) is unnecessary and an unreasonable administrative and costly requirement. For cause is justified, but renewing a background check every five years serves no point, especially when this standard does not require a company to take action based on derogatory information.

Section 1303, Requirement (4) (iii) Access revocation within 24 hours is not a practical requirement. Even assuming that a company has these processes automated, it is an unrealistic target, especially considering that contract workers are included and it is more difficult to even interpret when they have technically left.

Section 1305, Requirement (1) Documentation section assumes that there is one central security plan for the whole company vs. a security program. If this standard requires a 1300 security plan, then that is what it should say. Otherwise, it should just state that "the company shall have a documented implementation plan approved by the a senior manager responsible for the implementation of NERC 1300.

Section 1305, Measures (3) Physical Access Controls. Security cage does not belong in this list it is not interchangeable with the other 5 options. it is the same a walls or a perimeter fence around a sub station, just a smaller application and is covered under "four wall boundary". Also, Specialty Locks are from magnetic locks, which require some type of activation, which is covered under Other Authentication Devices. Mag locks, electric strikes and/or electrified mortise (to name a few) are implied when using a Card Key or Device. If not electric specialized locks are an option, and then it should only state, "Lock sets with restricted key system.

Section 1305, Measures (4) Alarm System. The first sentence is not consistent with the rest of the paragraph. "Ana alarm system based on the contact status that indicated a door or gate has been opened". This is consistent with a programmable alarm system which will report the state of a contact, open or shut and hold programming which will initiate an alarm based on a given state. The examples that follow (excluding door contact) are part of an intrusion detection system not related to an open or closed state of a door or gate. What is the goal? Do you want a system capable of reporting the state of a door or gate on the physical perimeter? Do you want to require an additional physical intrusion detection system? I recommend adding a section dealing with intrusion detection from alarm systems to clarify the measure. One or more of the following is not applicable in this measure, the two stated options are not interchangeable, they accomplish things. Either requires a minimum (recommend door state monitoring/reporting) and then one or more of the following (CCTV, Intrusion Detection etc.)

Under 1301 (d) (3) (ii), remove the word "and" at the end of the sentence.

Under 1301 (e) (1). What is the difference between (iv) and (v)?

Under 1306 (a) (2), please rephrase the 2nd sentence (The responsible entity must establish…) to make it clear.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

Generally agree with the thought and principles behind the new standard; however, are concerned about the considerable expansion in the number and types of critical cyber assets, as well as the increased specificity throughout the standard. Will there be an expanded implementation timeframe in which to address the standard (beyond the first quarter of 2006)? Also a general comment that the standard requires a significant amount of diligence (especially in the tracking, authorization and management of sensitive information) and will undoubtedly lead to staffing increases.

Standard 1300 refers to certain sections (1302.1.1,1302.1.2, etc.) but no such section exists since the document appears to use a different section numbering scheme.

1302 Critical Cyber Assets. Section headings are out of sequence (a..g).

1300 Cyber Security, Page 2. The items in the text box aren't consistent with this standard (refers to Purchasing/Selling Entity which is not applicable, but omits Transmission Operator, etc).

Section 1303, under Requirements (1). It appears like the phase "Responsible entity shall comply with the following requirements of this standard" should preceed items 1 through 4, not be part of item 1.

1307 Incident Response Planning. The meaning of the acrynom ESISAC should be stated. It would also be helpful to state how to access ESISAC.

The formatting requirments to translate this data (for submission to NERC for this Standard review) into a database are unreasonable. This commenting process must be designed to work effectvely for the industry, and not hindered by special NERC formatting requirements. NERC indicates in the first paragraph of this form to submit comments with Version 0 in the subject line. That looks to be an error.

Here is some alternative language for 1305

(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 KeyElectronic Access Control A means of electronic access where the access rights of the cardtoken
holder are pre-defined in a computer database. Access rights may

differ from one perimeter to another. (e.g., proximity card, biometric reader, weigand wire, or any one of unique token that can control access through personal authentication.)
Special Locks These may include pad locks or door locks with non-reproducible or restricted keysways., 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 oneall or more of the following monitoring methods.
CCTV Video surveillance that captures and records images of activity in
or around the secure perimeter and to assess alarm events as they occur..
Alarm Systems An alarm system based on contactboth reflects the current status that indicated aof a door or
gate has been opened (e.g., open or closed), but also can be programmed to generate an alarm under certain conditions (e.g., at certain times or if a door/gate is forced open or left open for too long). 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.
Intrusion Detection System a system that can detect intrusion into a given perimeter. This can be accomplished in a variety of ways(e.g., seismic sensors, glass breaks, passive or active infrared sensors, camera in conjunction with pixel analysis, cameras in conjunction with motion algorithm software, etc.)
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.on or off site second party verification.
Computerized Logging Electronic logs produced by the selected access control and monitoring method.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Tom Flowers	
Organization:	CenterPoint Energy	
Telephone:	(713) 207-2122	
Email:	tom.flowers@centerpointenergy.com	
NERC Region		**Registered Ballot Body Segment**
☒ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

see CenterPoint Energy comments

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
The number, gravity, and structural nature of the CenterPoint Energy comments are to great to consider a ballot at this time.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
CenterPoint Energy is attaching a Word file with this form as instructed.

CenterPoint Energy Comments
to the September 15, 2004 version of the Draft NERC Standard 1300 – Cyber Security

October 29, 2004

Page 1, 1300 Definitions

Replace the current definition of "Critical Cyber Assets**" with … "**Those [Cyber] 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. For the purposes of this Standard, the following critical Cyber assets are not addressed: (1) critical telecommunication infrastructure, (2) critical RTUs, PLCs, or Meters other than where specifically included, (3) critical Cyber support infrastructure, (state other exceptions and exclusions here)"

Delete the definition of "Incident"

Replace the definition of "Security Incident**" with…** "Any malicious or suspicious activity that has or could disrupt or compromise critical Cyber assets or its support infrastructure."

Insert definitions for: common systems, authorized access, unauthorized access, contractors or vendors, employees or staff, compliance audit, large quantity of customers (ESISAC website #s), (a thorough search and review of needed definition is needed)

Page 3, 1301 Security Management Controls

General comment:

This section uses the term "responsible entities" while most other sections use "the responsible entity". Choose one and be consistent.

Specific Comments:

Page 3, Introduction

Insert this as the third sentence. "Each entity will have to modify or adjust the requirements below to deal with environmental, technical, logistic, personnel, and access differences between attended facilities such as Control Centers and Power Plants and critical Substations which are typically unattended."

Page 3, (a)(1) Requirements – Cyber Security Policy

Replace the paragraph with…"The responsible entity shall create and maintain a role based Cyber security policy that addresses the requirements of this standard as well as the unique roles and responsibilities at each entity. "

Page 3, (a)(3) Roles and Responsibilities

Replace "member**" with…**"member(s) "

Replace "the Cyber security standard" **with…** "this Cyber security standard and all related policies, procedures, and practices unique to the entity."

Replace "person**" with…**"person(s) "

Replace "section 1.2" **with…** "subsection (a)(2) above."

Page 4, (a)(5)(iv) Access Revocation/Changes

Replace the first sentence with… "The responsible entity shall define procedures to ensure that modifications, suspension, and termination of user access to critical Cyber assets are accomplished in a timely manner. Revocation/changes of access due to termination for cause or suspension shall be accomplished within 24 hours while normal termination, transfer, or change of responsibilities shall be accomplished within 5 days "

Page 4, (a)(6) Authorization to Place into Production

Delete this subsection. This subsection should be moved to section 1306**.**

Page 9, 1302 Critical Cyber Assets

General comment:

This section is ambiguous in several areas:

(1) The language in 1302 and the FAQs associated with it seem to exclude the support systems and infrastructure at the control center, power plant, and substation such as UPS, batteries, computer room cooling systems, air handling systems, and switchgear for example. While these systems may not be critical infrastructure in another environment, the critical Cyber assets at the Control Center, Power Plant, and Substation are dependent on these systems to function normally."
(2) Along these same lines, 1300 at this stage does not recognize the Remote Telemetry Unit (RTU) or other sensory/alarm devices at a critical substation as inherently being a critical Cyber asset even though the RTU may be the only source of situational awareness at that station for the Control Center critical Cyber assets. The standard, as written, defines the criticality of an RTU solely on its vulnerability instead of its role in the reliable operation of the bulk electric system. The RTU in the entity's most critical substation must also be the entities most critical RTU .
(3) Nuclear Generation needs to be clearly excluded from this section.
(4) There is no provision or discussion about one responsible entity declaring the assets of another responsible entity critical. What about one way dependencies?
(5) There are several references to "common system" in this section. What does it mean (i.e. Region, Control Center, Plant Control System, etc.)?

Specific Comments:

Page 9, Introduction

Replace the paragraph with… "The responsible entity shall identify and protect all critical Cyber assets related to the reliable operation of the bulk electric system."

Page 9, (a) Requirements

Replace the paragraph with…. " The responsible entity shall identify and inventory their critical bulk electric system assets using their preferred risk assessment methodology. All critical Cyber assets must be an identified subset of this inventory and protected in accordance with this Cyber security standard."

Page 9, (a)(1) Critical Bulk Electric System Assets

Replace the first two sentences with…. "The responsible entity shall identify its critical bulk electric system assets in accordance with the definition approved by the NERC Critical Infrastructure Protection Committee (see definitions)."

Page 9, (a) (1)(ii) Critical Bulk Electric System Assets

This subsection is ambiguous. Does this mean that any substation connected electrically to an element monitored for IROL purposes? If so, what substation doesn't?

Page 9, (a) (1)(iii) Critical Bulk Electric System Assets

Define "common system**" or replace it.**

Page 9, (a) (1)(iv) Critical Bulk Electric System Assets

Replace "initial**" with "**required for**".**

Page 10, (a) (1)(v) Critical Bulk Electric System Assets

Define "common system**" or replace it.**

Page 10, (a) (2) Critical Cyber Assets

This entire subsection needs to be reconsidered for technical content and scope. Here are several points that need to be addressed and clarified:

1. Serial point-to-point (PTP) communication is not dial-up even though it may be over telephone lines
2. RTUs (including PLS, smart meters, EIDs, etc) that supply critical situational awareness information to critical Cyber assets at the Control Center for critical Substations are inherently critical Cyber assets themselves regardless of their vulnerability.
3. The support equipment (i.e. AC power, batteries, cooling, protective structure, etc.) that critical Cyber assets depend on to function are inherently critical Cyber assets because of this dependency.

Pages 10 -12, (b) – (f)

CenterPoint Energy will defer comments on these subsections based on the gravity and structural nature of comments on the Introduction and Requirements Subsections.

Page 13, <u>1303 Personnel & Training</u>

General comment:

This section needs to clearly identify the types of access:

Physical :

1. Unescorted Access
2. Escorted Access
3. Unauthorized/Illegal

Cyber:

1. Authorized
2. Unauthorized

Specific Comments:

Page 13, (a)(4) Requirements

Delete "unrestricted**" from the second sentence.**

Page 17, <u>1304 Electronic Security</u>

General comment:

The Levels of Noncompliance should refer to "insufficient evidence to support" or " there is evidence to indicate".

Specific Comments:

Page 17, Introduction

Replace the paragraph with…. "The responsible entity must create/identify all electronic security perimeters, implement necessary access controls through these perimeters, monitor access into and usage within the perimeter, and have an appropriate level of documentation to support a compliance audit."

Page17, (a)(2) Requirements – Electronic Access Controls

Replace the second paragraph with …."Where technically feasible, all computer monitors through which electronic access is controlled shall display an appropriate use banner upon interactive access attempts."

Page 17, <u>1305 Physical Security</u>

General comment:

In the Measures subsection, some discussion needs to occur about exit controls. This is not anti-pass back because it doesn't matter how an individual got into the physical security area. Rather it is a form of failure management. For example, if an individual gets into a secure area by accident, tail gating, or malicious means they will not be allowed to exit without a trace that the unauthorized entry ever occurred. This should be discussed in subsection (b)(3).

Specific Comments:

Page 22, Introduction

Replace the paragraph with…. "The responsible entity must create/identify all physical security perimeters, implement necessary access controls through these perimeters, monitor access into and usage within the perimeter, and have an appropriate level of documentation to support a compliance audit."

Page 22, (a) Requirements

Replace the first paragraph with…"(1) Physical Security Plan: The responsible entity shall develop and maintain a Physical Security Plan for use and application at all of its physical sites containing critical Cyber assets."

Insert after the last requirement… "(7) Documentation: The responsible entity shall maintain sufficient documentation concerning its implementation of its Physical Security Plan to support a compliance audit."

Page 23, (b)(3) Physical Access Controls

Replace "Security Cage**" with "**Additional Physical Perimeters**" in the table.** Use the cage as an example.

Replace "de-authorization**" with "**revocation**" in the second paragraph.**

Page 23, (b)(4) Monitoring Physical access Control

Replace "Alarm System**" with "**Access Control System**" in the table.** Use the open door alarm as an example.

Page 24, (b)(5) Logging Physical Access

Replace "human observation" **with** "human observation or remote verification"

Page 24, (b)(6) Maintenance and Testing of Physical Security Systems:

Replace the Paragraph with… "The responsible entity shall maintain documentation of all testing for an appropriate period of time to support a compliance audit."

Page 26, 1306 <u>Systems Security Management</u>
General comment:

This section should be broken into two sections. One section should discuss security management at the Control Center and Power Plant (attended) and the Substation (unattended). While there are generic commonalities between the two Cyber environmental, the technical, logistic, personnel, and access differences are sufficient to warrant different management solutions. In addition, the Substation Cyber environment is much more restricted by legacy systems technical limitations than Control Centers and Power Plants.

This section is too prescriptive when specifying measurements as in the case of "Retention of System Logs". The specifics of "how" an entity complies with a requirement should be left to the entity to determine and defend. There should be more use of the term "or other mitigating controls" throughout this section in order the address the reality that critical Cyber systems that are less than three years old may have components that exhibit legacy type restrictions when dealing with Patch Management for example. In lieu of restructuring this section, the following specific comments are necessary.

Specific Comments:
Page 26, Introduction

Insert after first sentence….."Many of the requirements in this section will not be applicable in the critical Substation environment since they are typically unmanned and the legacy technology is much more restrictive. Each entity will have to modify or adjust the requirements below to deal with environmental, technical, logistic, personnel, and access differences between attended facilities such as Control Centers and Power Plants and critical Substations which are typically unattended."

Page 26, (a)(1) Requirements – Test procedures

Insert at the end of second sentence…."or other mitigating controls"

Page 26, (a)(2) Account and Password management:

Insert into the first sentence after "establish"…"a system and user"

Replace the last sentence with…."The responsible entity must establish and implement password management practices, review systems, and documentation that includes but is not limited to :"

Page 26, (a)(2)(i) Strong Passwords:

Replace the paragraph with…"Passwords shall be changed periodically using a combination of alpha, numeric, and special characters whereever possible, to reduce the risk of password cracking."

Page 26, (a)(2)(ii) Generic Account Management:

Replace the last two sentences with…."Where technically and operationally feasible, individual accounts must be used, as opposed to group accounts. Where individual accounts are not feasible, other mitigating controls must be put in place and documented."

Page 27, (a)(2)(iv) Acceptable Use

Replace the last sentence with…"The policy must support a compliance audit of all account usage."

Page 27, (a)(3) Security Patch Management

Replace the last sentence with…"In the event that immediate installation is not possible, other mitigating controls must be implemented."

Page 27, (a)(4) Integrity Software

Replace sentence with…. "A formally documented process governing the application of anti-malware system integrity tools must be employed to prevent, limit, and/or mitigate their introduction or exposure to critical Cyber assets at and within the electronic security perimeter."

Page 27, (a)(5) Identification of Vulnerabilities and Responses

Replace the first sentence with…"Where technically and operationally feasible, an industry standard vulnerability assessment or scan shall be performed periodically that includes a diagnostic review of the access points, open ports/services, modems, default accounts, and patch management."

Page 27, (a)(6) Retention of System Logs

Replace the paragraph with…"Where technically and operationally feasible, all critical Cyber assets must generate logs/reports of related system events. The responsible Entity must retain these logs/reports for a reasonable period of time as necessary for a compliance audit and incident response purposes."

Page 27, (a)(7) Change Control and Configuration Management

Replace the paragraph with…"The responsible Entity shall establish a Change Control Process for modifying hardware and software for critical Cyber assets. The process should include change management procedures for testing, modification, compliance auditing, failure management, and overall integration integrity, where technically and operationally feasible."

Page 28, (a)(8) Disabling Unused network Ports/Services

Delete this element…Redundant. Covered in (a)(5)

Page 28, (a)(9) Dial-up Modems

Delete this element…Redundant. Covered in (a)(5)

Page 28, (a)(10) Operating Status Monitoring Tools

Insert before the word "Computer"…"Where technically feasible, …"

Page 28, (a)(11) Back-up and Recovery

Replace the first sentence with…."Information and data that is resident or required by computer systems used to manage critical electric infrastructure must be backed-up on a regular basis, where technically feasible. The back-up must be stored in a remote or hardened site some distance away from the critical Cyber assets."

Pages 28 -31, (b) – (f)

CenterPoint Energy will defer comments on these subsections based on the gravity and structural nature of comments on the Introduction and Requirements Subsections.

Page 32, <u>1307 Incident Response Planning</u>

General comment:

This section should focus on security incidents only and avoid discussion of other forms of incidents.

Specific Comments:

Page 32, Introduction:

Replace the paragraph with this…"Security measures designed to protect critical Cyber assets from intrusion, disruption or other forms of compromise must be monitored on a continuous basis and all detected security incidents must be dealt with, when possible, with a preplanned response. Incident Response Planning defines the procedures that must be in place and effectively executed when Cyber security incidents occur."

Page 32, (a)(1) Requirements

Delete…"(1)" **and replace the second sentence with**…"The plan shall provide specific procedures that are to be implemented in the event a Cyber security incident occurs in order to assess, mitigate, contain, or prevent negative impacts to any critical Cyber infrastructure."

Page 32, (a)(2) Incident Classification

Delete this subsection. If this section focuses on Cyber security incidents and the definition of such an incident is provided in the Definition section, as suggested, this subsection is redundant.

Page 32, (a)(3) Electronic and Physical Incident Response Actions:

Replace title with…"Incident Response Actions"

Replace the paragraph with…"(1) The responsible entity shall define the roles and responsibilities of individuals and incident response teams. In addition, procedures, evidence retention, and communication/contact practices must be unambiguous. "

Page 32, (a)(4) Incident and Cyber Security Incident Reporting:

Replace title with…"Incident Response Reporting"

Replace paragraph with… "(2) The responsible entity shall report all security incidents to the ESISAC as appropriate"

Pages 32 -33, (b) – (e)

CenterPoint Energy will defer comments on these subsections based on the gravity and structural nature of comments on the Introduction and Requirements Subsections.

Page 34, <u>1308 Recovery Plans</u>

Specific Comments:

Page 34, Introduction:

Replace the first sentence with this…"The responsible entity must establish recovery plans and put in place the physical and Cyber assets necessary to put these recovery plans into effect once triggered."

Delete the third paragraph. Create a Frequently Asked Question. (FAQ) out of this paragraph.

Page 34, (a)(1) Requirements

Replace (1) with…"The responsible entity shall create Recovery Plans for critical Cyber assets and exercise its Recovery Plans at an appropriate periodicity."

Page 34, (a)(3)

Replace (3) with…"The responsible entity shall update its Recovery plans as soon as possible after a significant system or procedural change and redistribute the revised plans appropriately."

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Peter Burke [on behalf of ATC's Dave Mueller]	
Organization:	American Transmission Company (ATC)	
Telephone:	262-506-6863	
Email:	PBurke@atcllc.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☒ Yes

☐ No

Comments

Question 2: Do you believe this standard is ready to go to ballot?

☒ Yes

☐ No

If No, what are the most significant issues the drafting team must reconsider?

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
On page 10 under the section Critical Cyber Assets item (B) which currently reads:

"the cyber asset uses a routable protocol, or"

should be changed to:

"the cyber asset uses a non secure routable protocol, or"

With this change the standard can achieve the desired goal of insuring that critical assets are secure without imposing a severe burden on those companies that installed modern equipment in their substations while rewarding those companies that have continued to use old legacy equipment. The implication in the current draft of the standard that non routable protocols are more secure than routable protocols when used for communications with substation equipment is not correct. While routable protocols are typically attacked by hackers the non routable legacy protocols are very easy for someone to exploit with readily available technology. These protocols while proprietary have been in use in many cases for over thirty years worldwide. Before security concerns changed documentation on these protocols was readily disseminated. When they were developed most of these legacy protocols required special hardware to implement. With today's PCs the protocols can be emulated easily using only software. Various methods can be used to impose malicious traffic on a circuit causing major problems on the electric system. A properly secured routable protocol connection to the substation using at a minimum encryption and certificates is significantly more secure than the legacy protocols. The standard should be written to encourage companies to install new systems that improve security, not encourage them to leave vulnerable legacy equipment in place. Since most of the cyber equipment installed in substations are embedded equipment applying the cyber standards have little effect. The equipment cannot be upgraded for security issues and was not designed with security concerns in mind. The proper way to protect these assets is to secure the communications path, not to attempt to impose control center security controls on the substation equipment.

If the goal of the standard is to improve security then the standard should apply equally to all substation sites irrespective of protocol or the standard should simply address the point of vulnerability, the communications interface, and insure that it is secured.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Tony Eddleman	
Organization:	Nebraska Public Power District	
Telephone:	402-845-5253	
Email:	tdeddle@nppd.com	
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT** ☐ **ECAR** ☐ **FRCC** ☐ **MAAC** ☐ **MAIN** ☒ **MAPP** ☐ **NPCC** ☐ **SERC** ☐ **SPP** ☐ **WECC** ☐ **NA - Not Applicable**	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Vague wording is used throughout the standard. How do we know if we are compliant with the standard? The openness of the standard is good from the perspective that it allows each entity to apply the standard to their situation, but will make compliance difficult. An individual entity may consider they are compliant, but actually not be compliant with the standard. Some examples are:

1302(a) - preferred risk-based assessment - what is this - a general, broad assessment or is it a specific format?

1302(a)(1) - "significant impact on the ability to serve large quantities of customers for an extended period of time" What is considered "significant impact"? How many are "large quantities" - 10 or 10,000,000? How long is an "extended period of time" - 10 minutes or 10 months?

1302(a)(1) - Define "a detrimental impact on the reliability or operability of the electric grid". Who determines a detrimental impact?

1302(a)(1) - Define a "significant risk to public health and safety". Does this include every feeder that serves a traffic light, police station, hospital, senior care facility, jail, etc.? An agrument could be made that this includes every line and substation in our system.

1302(a)(1)(iv)(B) - Define "initial" system restoration. Are you referring to cranking paths for blackstart units to critical generation or enough of the system to get units stabilized or maybe something else?

1304(a)(2) Electronic Access Controls: Define "strong" procedural or technical measures.

These examples should give a general overview of my comment and aren't meant as all the vague wordings in the standard.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?

A major issue is the new requirement to classify information and will significantly drive up costs to customers as currently written. This will require additional resources (labor, background checks, etc.) to implement. Our business is to generate and transmit energy. This new requirement could require a classification on a large portion of the documents that we use daily. This will affect a significant number (virtually all) of the employees in a utility, vendors, individuals in public office, such as our Power Review Board, etc. Then, for a person to have access to that information will require a background check that is renewed every five years. This standard requires significant "paperwork" and "red tape". How do you mark electronic files? More specifics are needed on how to classify information and a cost / benefit analysis should be performed on this requirement.

Recommend paragraph 1302(a)(2) Critical Cyber Assets be modified to specifically exclude all nuclear plants. These are covered under the Nuclear Regulatory Commission (NRC) standards.

Paragraph numbers and references are incorrect. One example is 1302(a)(2)(i)E) lists a reference to 1302.1.2.1. which doesn't exist in this document. The same section jumps from (a) directly to (g) without (b), (c), (d), (e), or (f). Section 1303 jumps from (a) to (l) without any in between.

Section 1304(a)(3) needs clarification. What are the expectations for a response to an unauthorized access attempt? Do we need a 24 hour - seven days a week desk watching for events? This will be very expensive for a minimal benefit. Can we use an intrusion detection system (IDS) that sends a page and alerts us? An IDS for all critical cyber assets will be expensive to install and maintain. Is a review of logs every business day sufficient to meet the standard? What is the incident review response time frame?

Section 1308 Recovery Plans requires physically and cyber assets not currently required by NERC Template P6T3, Emergency Operations / Loss of primary Controlling Facility. The two should be consistent.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
I support cyber security for critical assets and feel this is an important standard to implement. As currently written, this standard will be very resource intensive to implement.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Charlie Salamone	
Organization:	NSTAR	
Telephone:	781-441-8552	
Email:	Charles_Salamone@nstaronline.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☒ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Incident: The following definition is from SANS

The term "incident' refers to an adverse event in an information system and/or network or the treat of the occurrence of such an event. Incident implies harm or the attempt to harm.

Examples:

• Unauthorized use of another user's account

• Unauthorized use of system privileges

• Execution of malicious code that destroys data

Event:

An "event" is any observable occurrence in a system and/or network

Examples

• A system crash

• Packet flooding within a network

• The system boot sequence.

Critical Cyber Assets - Use definition from CIPC

Bulk Electric System Assets - define large quanitiy of customers

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
Needs to be more specific around RTUs. This is provided in the FAQs; why not bring into the standard.

Format of how standard is written; inconsistent (i.e. numbering throughout the standards document)

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
1301.a.5.iii - Need to identify frequency of access reviews.

1301.a.6 - Should be 24 business hours (1 business day) v. 24 hours. This is referenced throughout the document. Make this consistent throughout the document.

1301.b.6 - Should be 48 business hours (2 business days) v. 48 hours. This is referenced throughout the document. Make this consistent throughout the document.

1302.a.1.i.A - Define Telemetry

1302.a.2.i - Items B and C should be sub-bullets of requirement 1302.a

1303a.4 - Unrestricted access needs clarification. Should this be unescorted?

1304.a.2 - Clarify that this screen is intended for the user to see, saying essentially that they should "follow policy". Insert language similar to "where technically feasible" to recognize that some older equipment cannot be made to display such screens.

1305.a.1 - Change "above" to "following"

1305.a.6 - Further clarification around "Comprehensive Testing Program"

1306.a.2.i - First sentence should read "Where practicable, strong passwords for account must be used in the absence of more sophisticated methods such as multi-factor access controls"

1306.a.3 - Remove "and upgrades to" at the end of the 1st sentence.

1306.a.3 - Change last sentence to include "business justification must be documented". A compensating measure may not always be an option.

1306.a.6 - The standard needs to be more specific on what logs needs to be maintained.

1306.e.3.vii - Need to identify what is meant by operator (system administrator or control system operator)

1307 - Change title of requirement to "Incident Reporting and Response Plan"

1307.a.2 - Requirement should be applicable to malicious and or suspicious security incidents; need to clarify.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Deborah Linke	
Organization:	U.S. Bureau of Reclamation	
Telephone:	303-445-2922	
Email:	dlinke@do.usbr.gov	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☒ WECC ☐ NA - Not Applicable	☐ ☐ ☐ ☐ ☒ ☐ ☐ ☐ ☐ ☒	1 - Transmission Owners 2 - RTOs, ISOs, Regional Reliability Councils 3 - Load-serving Entities 4 - Transmission-dependent Utilities 5 - Electric Generators 6 - Electricity Brokers, Aggregators, and Marketers 7 - Large Electricity End Users 8 - Small Electricity End Users 9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Critical Cyber Assets definition. The later part of the first sentence, "such as…at a minimum," implies that all these assets perform critical bulk electric system functions which is not consistent with criteria in 1302 (for example, small generators). Removing it is recommended since specifics are addressed in 1302.

Need to include definitions of the terms: Owners, Custodians, and Users. It would be a good idea to include a definition of "Sensitive Information" or something similar that refers to "information pertaining to critical cyber assets…." The idea is to be more definitive about what information should be protected pursuant to 1301(a)(2).

Responsible Entity. Since definitions are to be included in a separate glossary, rewording the last part of the sentence, "as identified in the Reliability Function table of the Standard Authorization Request for this standard," is suggested.

The definition of critical asset in 1302(a)(2) should be clarified. For example, one of the key determinants to whether a device is considered a critical asset is whether it uses a routable protocol. At the very least, what is considered a routable protocol should be defined in the glossary. Also, the and-or boolean logic of this section is confusing. Possibly a decision tree chart would help clarify the logic.

Critical Cyber Assets – The term “adversely impact” needs to be defined more clearly.

Bulk Electric System Asset – Should be retitled as “Critical Bulk Electric System Asset” and the definition should be defined by the NERC Operating Committee.

Bulk Electric System Asset – The terms “significant impact”, “large quantities of customers’, “extended period of time”, “detrimental impact”, and “significant risk” all need to be clearly defined.

Incident – This definition should be consistant with existing operation reporting requirements, which are already in existence.

Security Incident – This definition should read; “Any malicious or suspicious activity which is known to have caused or would have resulted in an outage or loss of control of a Critical Cyber and/or Critical Bulk Electric Asset.”

For purposes of this cyber standard, that the physical perimeter under consideration be that associated only with the cyber assets (e.g., the control room), not that associated with the physical (facility) asset. Physical asset breaches should be addressed under other guidance.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
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. Suggest this be changed to read "… the governance of the cyber security controls." It is the controls that require governing, not the 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. Suggest this be changed to read "… cyber-based information pertaining to or used for critical business and / or operational functions. Protection controls shall address information in storage, in transit, and while being processed." Please reconsider the scope of information covered by this statement. Is it adequate?
(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. The authors may wish to consider using the term "categorize" in lieu of "classify" to ensure there is not confusion with "classified" information guidance and standards. Suggest this be "unauthorized" to address a broader audience. "Authenticated" personnel could be construed to only include those with proper log-in credentials.
(5) Access Authorization
The following should read:
(i) The responsible entity shall institute and document a process for the management of access to information pertaining to or used by critical cyber assets where the compromise of such access 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 all personnel who are responsible for authorizing access to critical cyber assets. Logical and 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. How often? Unless this review is covered elsewhere, the authors may want to consider including the review period here. Certainly every 6 months is not out of the question. Sooner if practicle.

(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. Is this time period practical? Suggest that a longer time be considered, perhaps one business week?

1302 Critical Cyber Assets
(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. Doesn't NERC provide guidance to help define critical bulk electric system assets? This would seem to be fundamental to this process. This would seem necessary in order to ensure that entities address assets at their boundaries such that their interconnection partners designate the same boundary assets. Aren't the assets to be protected by the responsible entity's cyber security policy and its attendant procedures and practices? This standard only sets the requirements for the entity's actions. It is unclear why the authors appear to be including non-cyber bulk electric system assets in this standard. In general, such critical assets would appear to be outside the scope of this standard and should be addressed in other appropriate plans and assessments, including those for continuity of operations. Once such critical asset identification is complete, and where it identifies critical cyber assets, then the protection of those cyber assets is covered by this standard. As prepared, this section is confusing.

(ii) Transmission substations associated with elements monitored as
Interconnection Reliability Operating Limits (IROL) - It is unclear how this is a critical cyber asset.
(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) Perhaps this could be clearer if worded as "Cyber systems providing centralized control of generating resources meeting the criteria for a Reportable Disturbance…" It appears that what is being attempted here is the identification of Critical Cyber Assets in terms of the power system and impact, but it is being attempted in a way that appears backwards. This is common to other material under this subparagraph and makes the application of this standard difficult.

B) the cyber asset uses a routable protocol, or - Although a routable protocol is significant from the perspective of a cyber system exposed to other interconnected systems, this may not be a good indicator for a critical cyber asset. A critical cyber asset should be identified based on its impact on the power system or the business functions of the responsible entity. Based upon this assessment, the risks faced by the entity (and the industry should the system be compromised) can be established. The vulnerabilities presented by the use of a particular protocol can then be examined in the context of exposure (e.g., the use of a routable protocol on an isolated minor system whose compromise would have little business impact, does not qualify it for categorization as critical.)
C) the cyber asset is dial-up accessible. Similar comment to that above. Exposure is assumed, however. Nevertheless, the impact of the system and its compromise through the exposure

mechanism must be considered before the system should be categorized as critical. In addition, mitigating controls, such as dial-up through a private branch exchange or the employment of dial-back technology must be considered.
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.

(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 the protection of sensitive information about or within these critical assets. - The authors may want to consider specifically addressing incident response and contingency operations training for appropriate individuals

(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.- The authors may want to consider escort requirements for service vendors and visitors who do not have appropriate background investigations. Obviously, it is impractical for all access to be unrestricted. This requirement could impact costs associated with janitorial/custodial services as well as that provided by some vendors.

(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.). - This time should probably be shorter than this if the termination or suspension is an adverse action and the critical cyber system allows access from outside the organization.

(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. - What actions are suggested for incumbents who may be found to not meet background screening minimum critieria, but whose employment has been satisfactory?

(a) Requirements - Although this may be addressed in other NERC guidance, there appears to be no identification of data types or attributes (numeric/alphanumeric, range checks, maximum deviation allowances, etc.) associated with information crossing perimeter boundaries. This, along with appropriate security MOAs/MOUs executed with communication partners would promote security by providing guidelines for the acceptance of data and criteria/procedures for addressing potential security incidents between partners. It should be considered that the “bad guy” does not have to perform direct attacks against the entity’s system, he may have broken into a partner’s system and be sending bad data, out-of-bounds commands, or contaminated files to the entity through a “trusted” channel.

(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). - Unless covered elsewhere, this perimeter may need to be expanded to cover support equipment, such as engine/generator sets, UPS equipment, fire protection equipment and controls, security and card-key controllers, telephone and communication systems, and HVAC systems. Breaching these systems may prove easier for an adversary and yield results as severe as a direct attack upon the cyber asset (or facilitate a more direct attack).

(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. - This should also include changes (not patches) that may be made by the responsible entity, the entity's contractors, or the product vendors. Patches are assumed to be those modifications made to S/W, F/W to address coding errors. Changes are those modifications made to address new or different functionality requirements. Both change and patch management processes should be a part of the security controls required on critical cyber assets covered under this standard. Testing is required under both scenarios, but the testing is different in each case.

(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. - The acceptable use policy should address all users, not just those who have administrator or generic access accounts. It should address types of activities allowed (e.g., controlling a power system in accordance with appropriate SOPs through Operator accounts) and types of activities disallowed (e.g., loading unauthorized applications or games, or surfing inappropriate sites – where web access is permitted).

(8) Disabling Unused Network Ports/Services
The responsible entity shall disable inherent (unnecessary default) and unused services.
(9) Dial-up modems
The responsible entity shall secure dial-up modem connections. - Security mechanisms could include dial-back technologies, disconnection except when specifically required, and monitoring of activity when the modem is in service.
(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. - It is assumed that the function of such tools is to look for and alarm on "abnormal" conditions after tools have had an adequate time to "learn" normal operating conditions. This is not clear as written.
(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. - It may be necessary to define what constitutes a remote facility (one located more than one mile from the primary facility and in a direction that is likely to be accessible under adverse conditions – such as floods) Also consider indicating physical and access protection requirements to the storage location to be a stringent as those required for the primary site. Finally, there does not appear to be any requirement listed for marking/identifying backup media.

(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 - Physical incident response, if confined to the cyber assets, is within scope of this policy. Each entity probably has a physical security incident reporting and response process that addressed site access, vandalism, theft, and other activities. This may be distinctly different than the cyber security incident response process and may be covered by other policy. Wording changes may clarify the boundaries between these two processes and not be mistaken to indicate that an integrated plan is necessary.

(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. The plans shall include communication with partner entities, as appropriate - These actions can be documented in the MOUs/MOAs suggested earlier.

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. - Some of the issues discussed in this section relate to continuity of business or continuity of operations. It would appear that these discussions are outside the scope of this standard. It is recommended that this standard only address recovery or contingency plans associated with the cyber asset(s) under consideration. A business or operations continuity plan would identify whether or not the cyber assets require recovery under various general scenarios. That business or operations plan should also address the priority associated with cyber system restoration and the allowable outage and recovery times. Attempting to address business or operations issues within this cyber standard appears out of place and is probably redundant with other NERC guidance or policy.

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. - It is unclear whether this is to be read as a requirement for backup control centers. Such centers present considerable investments and bring with them attendant risks (related to attacks mounted on the backup centers rather than the active sites – they are libel to be not as effectively defended.) Additional hardening of a single site may be more cost-effective than a backup center. Additional “hardening” is also provided by the elasticity and inertia of the system. An analysis such as that above, coupled with power stability studies would be necessary to determine the true need for a backup control center.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
NERC should consider following the NIST guidance for security controls, plans, and reviews. This wouldn't cover the penalties component of the NERC materials, but it would standardize the front-end security program controls. Specific NIST guidance that would be reasonable to cite would be Special Publications 800-18 (Security Plans), 800-30 (Risk Assessments), 800-37 (Certification and Accreditation), and 800-53 (Recommended Security Controls).

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 subnetworks
(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.[LM1]

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[LM2].

(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[LM3].

(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[LM4] information related to critical cyber assets to aid personnel with access to this information in determining what information can be disclosed to unauthenticated[LM5] 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[LM6] 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[LM7] in section 1.2.

(4) Governance

Responsible entities shall define and document a structure of relationships and decision-making processes that identify and represent[LM8] 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 the management of access ~~management~~ to information pertaining to or used by critical cyber assets where the~~hose~~ compromise of such access 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 all personnel who are responsible for~~to~~ authorizing~~e~~ access to critical cyber assets. Logical and~~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[LM9] 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~~ elevated from a test to~~operate in a~~ 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.[LM10]

(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.[LM11] 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[LM12].

(1) Critical Bulk Electric System Asset[LM13]s

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)[LM14]

(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)

[LM15]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[LM16], or
C) the cyber asset is dial-up accessib[LM17]le.
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.[LM18]
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 [LM19]governing access to, the use of, and the protection of sensitive information about or within~~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[LM20], 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 through~~in~~ the application of the entity's cyber security policy~~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 web pages/banners??, 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[LM21], 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.[LM22]
(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[LM23]

(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).[LM24]

(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[LM25].

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 nonproduction 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 semiannually. 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.[LM26]

(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 (unnecessary default) and unused services.

(9) Dial-up modems

The responsible entity shall secure dial-up modem connections.[LM27]

(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.[LM28]

(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.[LM29] 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[LM30] 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. The plans shall include communication with partner entities, as appropriate.[LM31]

(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.[LM32]

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. [LM33]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.

[LM1]Would suggest, for purposes of this cyber standard, that the physical perimeter under consideration be that associated only with the cyber assets (e.g., the control room), not that associated with the physical (facility) asset. Physical asset breaches should be addressed under other guidance.
[LM2]Suggest this be changed to read "… the governance of the cyber security controls." It is the controls that require governing, not the policy.
[LM3]Suggest this be changed to read "… cyber-based information pertaining to or used for critical business and / or operational functions. Protection controls shall address information in storage, in transit, and while being processed." Please reconsider the scope of information covered by this statement. Is it adequate?
[LM4]The authors may wish to consider using the term "categorize" in lieu of "classify" to ensure there is not confusion with "classified" information guidance and standards.
[LM5]Suggest this be "unauthorized" to address a broader audience. "Authenticated" personnel could be construed to only include those with proper log-in credentials.
[LM6]Categorization ?
[LM7]Categorized ?
[LM8]Characterize ?
[LM9]How often? Unless this review is covered elsewhere, the authors may want to consider including the review period here. Certainly every 6 months is not out of the question. Sooner if practicle.
[LM10]Is this time period practical? Suggest that a longer time be considered, perhaps one business week?
[LM11]Doesn't NERC provide guidance to help define critical bulk electric system assets? This would seem to be fundamental to this process. This would seem necessary in order to ensure that entities address assets at their boundaries such that their interconnection partners designate the same boundary assets.
[LM12]Aren't the assets to be protected by the responsible entity's cyber security policy and its attendant procedures and practices? This standard only sets the requirements for the entity's actions.
[LM13]It is unclear why the authors appear to be including non-cyber bulk electric system assets in this standard. In general, such critical assets would appear to be outside the scope of this standard and should be addressed in other appropriate plans and assessments, including those for continuity of operations. Once such critical asset identification is complete, and where it identifies critical cyber assets, then the protection of those cyber assets is covered by this standard. As prepared, this section is confusing.
[LM14]It is unclear how this is a critical cyber asset.
[LM15]Perhaps this could be clearer if worded as "Cyber systems providing centralized control of generating resources meeting the criteria for a Reportable Disturbance…" It appears that what is being attempted here is the identification of Critical Cyber Assets in terms of the power system and impact, but it is being attempted in a way that appears backwards. This is common to other material under this subparagraph and makes the application of this standard difficult.
[LM16]Although a routable protocol is significant from the perspective of a cyber system exposed to other interconnected systems, this may not be a good indicator for a critical cyber asset. A critical cyber asset should be identified based on its impact on the power system or the business functions of the responsible entity. Based upon this assessment, the risks faced by the entity (and the industry should the system be compromised) can be established. The vulnerabilities presented by the use of a particular protocol can then be examined in the context of exposure (e.g., the use of a routable protocol on an isolated minor system whose compromise would have little business impact, does not qualify it for categorization as critical.)
[LM17]Similar comment to that above. Exposure is assumed, however. Nevertheless, the impact of the system and its compromise through the exposure mechanism must be considered before the system should be categorized as critical. In addition, mitigating controls, such as dial-up through a private branch exchange or the employment of dial-back technology must be considered.
[LM18]Unclear.
[LM19]The authors may want to consider specifically addressing incident response and contingency operations training for appropriate individuals.
[LM20]The authors may want to consider escort requirements for service vendors and visitors who do not have appropriate background investigations. Obviously, it is impractical for all access to be unrestricted. This requirement could impact costs associated with janitorial/custodial services as well as that provided by some vendors.
[LM21]This time should probably be shorter than this if the termination or suspension is an adverse action and the critical cyber system allows access from outside the organization.
[LM22]What actions are suggested for incumbents who may be found to not meet background screening minimum critieria, but whose employment has been satisfactory?

[LM23]Although this may be addressed in other NERC guidance, there appears to be no identification of data types or attributes (numeric/alphanumeric, range checks, maximum deviation allowances, etc.) associated with information crossing perimeter boundaries. This, along with appropriate security MOAs/MOUs executed with communication partners would promote security by providing guidelines for the acceptance of data and criteria/procedures for addressing potential security incidents between partners. It should be considered that the "bad guy" does not have to perform direct attacks against the entity's system, he may have broken into a partner's system and be sending bad data, out-of-bounds commands, or contaminated files to the entity through a "trusted" channel.
[LM24]Unless covered elsewhere, this perimeter may need to be expanded to cover support equipment, such as engine/generator sets, UPS equipment, fire protection equipment and controls, security and card-key controllers, telephone and communication systems, and HVAC systems. Breaching these systems may prove easier for an adversary and yield results as severe as a direct attack upon the cyber asset (or facilitate a more direct attack).
[LM25]This should also include changes (not patches) that may be made by the responsible entity, the entity's contractors, or the product vendors. Patches are assumed to be those modifications made to S/W, F/W to address coding errors. Changes are those modifications made to address new or different functionality requirements. Both change and patch management processes should be a part of the security controls required on critical cyber assets covered under this standard. Testing is required under both scenarios, but the testing is different in each case.
[LM26]The acceptable use policy should address all users, not just those who have administrator or generic access accounts. It should address types of activities allowed (e.g., controlling a power system in accordance with appropriate SOPs through Operator accounts) and types of activities disallowed (e.g., loading unauthorized applications or games, or surfing inappropriate sites – where web access is permitted).
[LM27]Security mechanisms could include dial-back technologies, disconnection except when specifically required, and monitoring of activity when the modem is in service.
[LM28]It is assumed that the function of such tools is to look for and alarm on "abnormal" conditions after tools have had an adequate time to "learn" normal operating conditions. This is not clear as written.
[LM29]It may be necessary to define what constitutes a remote facility (one located more than one mile from the primary facility and in a direction that is likely to be accessible under adverse conditions – such as floods) Also consider indicating physical and access protection requirements to the storage location to be a stringent as those required for the primary site. Finally, there does not appear to be any requirement listed for marking/identifying backup media.
[LM30]Physical incident response, if confined to the cyber assets, is within scope of this policy. Each entity probably has a physical security incident reporting and response process that addressed site access, vandalism, theft, and other activities. This may be distinctly different than the cyber security incident response process and may be covered by other policy. Wording changes may clarify the boundaries between these two processes and not be mistaken to indicate that an integrated plan is necessary.
[LM31]These actions can be documented in the MOUs/MOAs suggested earlier.
[LM32]Some of the issues discussed in this section relate to continuity of business or continuity of operations. It would appear that these discussions are outside the scope of this standard. It is recommended that this standard only address recovery or contingency plans associated with the cyber asset(s) under consideration. A business or operations continuity plan would identify whether or not the cyber assets require recovery under various general scenarios. That business or operations plan should also address the priority associated with cyber system restoration and the allowable outage and recovery times. Attempting to address business or operations issues within this cyber standard appears out of place and is probably redundant with other NERC guidance or policy.
[LM33]It is unclear whether this is to be read as a requirement for backup control centers. Such centers present considerable investments and bring with them attendant risks (related to attacks mounted on the backup centers rather than the active sites – they are libel to be not as effectively defended.) Additional hardening of a single site may be more cost-effective than a backup center. Additional "hardening" is also provided by the elasticity and inertia of the system. An analysis such as that above, coupled with power stability studies would be necessary to determine the true need for a backup control center.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Ed Riley & James Sample	
Organization:	California ISO	
Telephone:	916-351-4463	
Email:	eriley@caiso.com	
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT**	☐	1 - Transmission Owners
☐ **ECAR**	☒	2 - RTOs, ISOs, Regional Reliability Councils
☐ **FRCC**	☐	3 - Load-serving Entities
☐ **MAAC**	☐	4 - Transmission-dependent Utilities
☐ **MAIN**	☐	5 - Electric Generators
☐ **MAPP**	☐	6 - Electricity Brokers, Aggregators, and Marketers
☐ **NPCC**	☐	7 - Large Electricity End Users
☐ **SERC**	☐	8 - Small Electricity End Users
☐ **SPP**	☐	9 - Federal, State, Provincial Regulatory or other Government Entities
☒ **WECC**		
☐ **NA - Not Applicable**		

Group Comments (Complete this page if comments are from a group.)
Group Name:

Lead Contact:			
Contact Organization:			
Contact Segment:			
Contact Telephone:			
Contact Email:			
Additional Member Name	**Additional Member Organization**	**Region***	**Segment***

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable

entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☒ Yes

☐ No

Comments

We agree with the definitions in general, but would recommend the following changes:

1. Critical Cyber Assets – The term "adversely impact" needs to be defined more clearly.
2. Bulk Electric System Asset – Should be retitled as "Critical Bulk Electric System Asset" and the definition should be defined by the NERC Operating Committee.
3. Bulk Electric System Asset – The terms "significant impact", "large quantities of customers', "extended period of time", "detrimental impact", and "significant risk" all need to be clearly defined.
4. Incident – This definition should be removed based on existing operation reporting requirements, which are already in existence. If the definition cannot be removed completely at least remove the second bullet as the first bullet sufficiently covers any incident. The reference to attempts in the second bullet dilutes the definition and could result in excessive reporting.
5. Security Incident – This definition should read; "Any malicious or suspicious activity which is known to have caused or would have resulted in an outage or loss of control of a Critical Cyber and/or Critical Bulk Electric Asset."

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?

1. Format inconsistencies exist throughout the document between each section. These inconsistencies results in difficulty in determining what the true requirements are. In several instances, more than one section calls for the same requirement with different time periods. The document needs a professional tech writer to review and make each section consistent and homogenous. It is understandable that the drafting team cannot provide this level of review and consideration must strongly be given to hiring a professional tech writer prior to the next publication.

2. In addition to the format inconsistencies, there seems to be a lot of typos and incomplete sentences.

3. For consistency, the work reliability should be used on it's own and operability should be excluded. Both terms seem to be used synonymous within the standard.

4. Due to the formatting inconsistency mentioned above in several sections it is difficult to differentiate between the section introduction paragraph, requirements, and measurements sections. In many cases they each seem to define requirements.

5. In all sections, compliance monitoring doesn't appear to synchronize with the section introduction paragraph, requirements, and measurements sections.

6. Identification of the compliance administration/monitoring is not clear. Believed to be the RRO's. Who is responsible for overseeing compliance should be made clearer in the standard.

7. The compliance section is very difficult to understand. Multiple compliance levels are complex and should just be that you are compliant or non-compliant.

8. It is difficult to comment on the compliance section without understanding how the sanctions and fines are going to be imposed.

9. Consider removing all timeframe references (e.g. quarterly, annually, etc.) and replace with "to ensure compliance with the entities document processes." This would achieve the goal of ensuring that the entity documents their processes and procedures and would provide them the flexibility to define their own auditable/measurable business rules.

10. The standard makes heavy use and references to industry groups, committees, and other acronyms and it would be helpful to have these defined and/or described.

11. Due to the fact that many entities that will be required to be compliant with this standard is also subject to other regulations such as Sarbanes-Oxly (SOX). To comply with SOX many organizations are undergoing SAS 70 audits. It is highly suggested that the NERC 1300 Drafting Team try to align of control objectives within the standard with the SAS 70, both from a wording standpoint as well as an activity standpoint, to enable entities to optimize their activities as it relates to compliance and oversight.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
In addition to the comments listed in Question 1 and 2, the following comments are provided. Also note, based on comments in Question 2 about the measurements and compliance, little to no comments about these sections will be documented below. The focus was on the introduction paragraph and requirements sections.

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.	**The term Reliability Authority was recently removed in the creation of the NERC Standard 0. Should be reflected here.**
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.	**Change Information Protection to Information Protection Program to be aligned with the references within the measurement section.** **Remove "used by", the pertaining to is defined below.**
(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.	**Remove "all", minimum requirements is defined. Disaster Recovery plans should be specifically identified as a minimum requirement.**

(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.	**The use of unauthenticated personnel is anomalous to the rest of the document. Unauthorized is a better term. Even some authenticated personnel may not necessarily be authorized.**
(iii) Protection Responsible entities must identify the information access limitations related to critical cyber assets based on classification level.	**"as defined by the individual entity" should be included after classification level to read "…classification level as defined by the individual entity."**
(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.	**Where is 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.	**Remove "or used by".** **Access Revocation/Changes: Should be reworded to read: Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished in a time frame that ensures critical cyber assets are not compromised.**
(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.	**Policies are supposed to be broad with a life cycle of 3-5 years. This should be changed to "reviewed as needed with a minimum review of every 5 years".**
(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.	**To be consistent, change title to Information Protection Program.**
(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.	**(i) Seems to be speaking about critical cyber "information" but the last work refers to "assets." The last word in the sentence should be "information." This sentence could be reworded to make a clearer statement.** **Remove "within five days" from section (i). The effort required to make this an auditable function only creates unnecessary administrative overhead and distracts from the intent of the control.** **The review periods seem to be to often and don't seem to synchronize with each other in this section.**
(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.	**Remove the last line. The effort required to make this an auditable function only creates unnecessary administrative overhead and distracts from the intent of the control.**
(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.	**This section should provide more clarification to identify the meaning of audit result which refers to compliance with the NERC 1300 Standard and not any other audit.**
(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.	**This paragraph should be rephrased to provide clearer meaning. By commencing with the first sentence, it could be interpreted that the standard may be intending to speak to protection methods around bulk electric systems when it is only the cyber systems. If the second sentence were stated first, this may be clearer.**
(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:	**Replace "electric grid" with "critical bulk electric system" for consistency.**
(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.	**FORMATTING/NUMBERING ISSUE** **(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** **i) the cyber asset uses a routable protocol, or** **ii) the cyber asset is dial-up accessible.** **B) 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.**
(3) A senior management officer must approve the list of critical bulk electric system assets and the list of critical cyber assets.	**The term "senior management" and "officer" have legal meaning in many companies, it should be clarified further of what is level of authority is necessary.** **Should be worded in a way that would enable identification by category, not just individual asset. Example would be that any device placed within the Energy Management System environment would automatically be covered and would not have to go to senior management.**
(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 riskbased 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.	**Replace "personnel subject to the standard " to "personnel having access to critical cyber assets".**
(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.	**Where background screening may be a deterrent, it can cause a false sense of security. By only performing "common" corporate background screenings, someone the is fraudulently acting as someone else is normally not detected. Only more through background screening like fingerprinting can provide the necessary assurance that someone is who they say they are.** **Also, this does not account for non-US citizens. A lot of our workforce is working with green cards and background screening would not provide any value for this scenario.** **Using "escorted access" and "unescorted access" is better terminology than "unrestricted access".**
(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.	**Access revocation is covered within other sections of this standard. Should be reconciled to ensure consistency.** **In Canada, the equivalent is the Social Insurance Number (SIN) and should be added.**
(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.	**Strong is a subjective term and needs to be clearly defined.** **Add "where equipment supports banners" to the end of the last sentence to read "…use banner upon interactive access attempts, where equipment supports banners."**
(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 orprevents 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 nonproduction environment. All testing must be performed in a manner that precludes adversely affecting the production system and operation.	**Remove "Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment. The last sentence is an adequate statement.**
(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 semiannually. 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.	**Should qualify "strong password" as to where it is technically supported. Not all technology allows for this.** **Access Reviews is covered within other sections of this standard. Should be reconciled to ensure consistency.**
(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.	**The word 'timely' does not adequately reflect the risk management approach that should be used in applying patches.**
(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.	**Needs to state that it will exist "where applicable as defined by the entity".**
(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 of three (3) years in an exportable format, for possible use in further event analysis.	**The first sentence needs to be changed to reflect that audit trails need to be generated, but not necessarily by the asset as described within the first sentence. Not all devices have this capability. Additionally, should state "where technically feasible".** **What is the definition of "security related system events"?**
(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.	**This section sound very much like section 1301, authorization to place into production. Should be reconciled to ensure consistency.** **What is the definition of a "controlled environment"? Could be interrupted as a separate test environment, is this what is intended?**
(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.	**This section is not about archival, it is about back-up and recovery, so the last sentence should be removed.**
(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.	**The responsible entity must identify in its policy a minimum retention period satisfactory to reconstruct a 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.	**These specific logs have not been referred to previously in this section of the standard, yet the standard is requiring compliance.**
(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.	**The introduction paragraphs read more like requirements and should be in the appropriate section. Goes back to the formatting inconsistencies.** **Annual testing of low probability events is to frequent, focus on training our operators on higher probability events has more value and allows them to focus on the job at hand.** **The last paragraph is very wordy and could be reworded to be clearer.**
(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.	**Post is misleading and suggest posting to a broad audience. It should be modified to reflect its real nature which is publishing to documents that only individual with a need-to-know would use in an event of a crisis.**
(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.	

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard 1300, Draft 1" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	TERRY DOERN	
Organization:	Bonneville Power Administration	
Telephone:	360-418-2341	
Email:	tldoern@bpa.gov	
NERC Region		**Registered Ballot Body Segment**
ERCOT **ECAR** **FRCC** **MAAC** **MAIN** **MAPP** **NPCC** **SERC** **SPP** **WECC** **NA - Not Applicable**	X	1 - Transmission Owners
		2 - RTOs, ISOs, Regional Reliability Councils
		3 - Load-serving Entities
		4 - Transmission-dependent Utilities
		5 - Electric Generators
		6 - Electricity Brokers, Aggregators, and Marketers
		7 - Large Electricity End Users
		8 - Small Electricity End Users
		9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)	
Group Name:	**BONNEVILLE POWER ADMINISTRATION**

Lead Contact:	**TERRY DOERN**
Contact Organization:	**–Transmission Business Line SYSTEM OPERATIONS - TOT**
Contact Segment:	**TRANSMISSION OPERATOR**
Contact Telephone:	**360-418-2341**
Contact Email:	**tldoern@bpa.gov**

Additional Member Name	Additional Member Organization	Region*	Segment*
Jon Stanford	**BPA – Cyber Security**	**WECC**	**1-Transmission Operator**
Kevin Dorning	**BPA – Cyber Security**	**WECC**	**1-Transmission Operator**
Tracy Edwards	**BPA – System Operations - TOT**	**WECC**	**1-Transmission Operator**
Randi Thomas	**BPA – Control Center Software**	**WECC**	**1-Transmission Operator**
Curt Wilkins	**BPA –Data Hardware & Telecommunications**	**WECC**	**1-Transmission Operator**
Bob Windus	**BPA Security Manager**	**WECC**	
Randy Suhrbier	**BPA SCADA Software**	**WECC**	**1-Transmission Operator**
Ron Rodewald	**BPA Power Business Line - Scheduling**	**WECC**	**3-Load Serving Entity 5-Electric Generator 6-Electric Marketer**
Cliff Carpenter	**BPA Power Business Line Software**	**WECC**	**3-Load Serving Entity 5-Electric Generator 6-Electric Marketer**
Ross Pies	**BPA Power Business Line Software**	**WECC**	**3-Load Serving Entity 5-Electric Generator 6-Electric Marketer**

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable

entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

Yes

No X

Comments

1. The first page of the standard must include a statement of scope developed by NERC CIPC. The scope must be absolutely clear as to the standard's purpose and to what it applies. The definitions of terms should follow. The definitions should define terminology used within the standard, but not be used to define the scope of the standard. A standard must be prescriptive in it's use of terms in order to establish a uniform baseline for compliance.

Definitions:

2. **Bulk Electric System Asset** – The term "if unavailable" narrows the applicability of the standard to that portion of "Bulk Electric System Assets" that are somehow made unavailable AND have "a significant impact on the ability to serve large quantities of customers for an extended period of time" etc. If the definition applies to a loss of "availability", then "Incidents" must correlate to such loss. This is standard cyber security practice. Also, the terms "significant impact", "large quantities", "detrimental impact" and "significant risk" are not defined.
3. **Electronic Security Perimeter** – The statement "and for which access is controlled" narrows the definition of the perimeter to networks that have access control in place. If no access control is in place, then they would be outside the security perimeter. If the intent of the standard is to bring uncontrolled networks into best practice compliance, then this definition is counterproductive. This statement should be changed to "and for which access should be controlled".
4. **Physical Security Perimeter** – As with the comment for the definition of Electronic Security Perimeter, the statement "and for which access is controlled" should be changed to "and for which access should be controlled".
5. **Incident** – The terms Physical and cyber event" should be dealt with separately. With reference to these events, the terms "could have" and "an attempt to" are counter to cyber security industry practice. These terms are impossible to correlate to any criteria and are not reportable. An incident should be a concrete benchmark related to actual activity and not intentions.

   The terms "disruption" and "compromise" are not defined...They should be clearly defined as an impact, such as a disruption which led to a loss of availability of a critical bulk electrical system asset or a compromise which sent out confidential data. As a federal agency, BPA has been given criteria for reportable security incidents.
6. **Security Incident** – The terms "malicious" and "suspicious" are nebulous and not defined. Delete them from this definition.
7. Definitions need to be provided for the terms: **Bulk Electric System Asset** and **Critical Bulk Electrical System Assets.**

BPA Transmission is in agreement with the following WECC EMS WG's comments:

8. Critical Cyber Assets – The term "adversely impact" needs to be defined more clearly.
9. Bulk Electric System Asset – Should be retiled as "Critical Bulk Electric System Asset" and the definition should be defined by the NERC Operating Committee.

10. Bulk Electric System Asset – The terms “significant impact”, “large quantities of customers’, “extended period of time”, “detrimental impact”, and “significant risk” all need to be clearly defined.
11. Incident – This definition should be removed based on existing operation reporting requirements, which are already in existence.
12. Security Incident – This definition should read; “Any malicious or suspicious activity which is known to have caused or would have resulted in an outage or loss of control of a Critical Cyber and/or Critical Bulk Electric Asset.”

Question 2: Do you believe this standard is ready to go to ballot?

Yes

No X

If No, what are the most significant issues the drafting team must reconsider?

1. BPA and other utilities may have conflicts between NERC 1300 and aplicapable cyber security related laws, guidelines, policies and regulations (e.g., U.S. Federal, State, Canadian, etc.). A process to resolve these conflicts will need to be developed by NERC and the affected utilities.
2. Technical issues at the systems level may limit the ability to follow this standard. Exceptions may be needed, therefore a process to resolve these issues will need to be developed by NERC and the affected utilities.
3. This Standard contains policy statements and should be acknowledged as such in order to be in alignment with the CYBER SECURITY industry.
4. Consider removing selected timeframe references (e.g., quarterly, annually, etc.) and replace with "to ensure compliance with the entities documented processes." This would ensure that the entity documents their processes and procedures, while providing them the flexibility to define their own auditable/measurable business rules.

BPA Transmission is in agreement with WECC EMS WG's comments below:

5. Format inconsistencies exist throughout the document between each section. These inconsistencies results in difficulty in determining what the true requirements are. In several instances, more than one section calls for the same requirement with different time periods. The document needs a professional tech writer to review and make each section consistent and homogenous. It is understandable that the drafting team cannot provide this level of review and consideration must strongly be given to hiring a professional tech writer prior to the next publication.

6. In addition to the format inconsistencies, there seems to be a lot of typos and incomplete sentences.

7. Due to the formatting inconsistency mentioned above in several sections it is difficult to differentiate between the section introduction paragraph, requirements, and measurements sections. In many cases they each seem to define requirements.

8. In all sections, compliance monitoring doesn't appear to synchronize with the section introduction paragraph, requirements, and measurements sections.

9. The compliance section is very difficult to understand. Multiple compliance levels are complex and should just be that you are compliant or non-compliant.

10. It is difficult to comment on the compliance section without understanding how the sanctions and fines are going to be imposed.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

In addition to the comments listed in Question 1 and 2, the following comments are provided. Also note, based on comments in Question 2 about the measurements and compliance, little to no comments about these sections will be documented below. The focus was on the introduction paragraph and requirements sections.

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.	BPA Transmission is in agreement with the WECC EMS WG's comment: The term Reliability Authority was recently removed in the creation of the NERC Standard 0. Should be reflected here.
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.	Is "cyber assets affecting" the same as "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.	BPA is bound by DOE Order 457.3 in how it protects information that is categorized as OUO (Official Use Only) and CII (Critical Infrastructure Information) BPA Transmission is in agreement with the WECC EMS WG's comment: Change Information Protection to Information Protection Program to be aligned with the references within the measurement section.

(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.	This is very, very broad. Example, "equipment layouts" could include every document related to substation equipment in the field. BPA Transmission is in agreement with the WECC EMS WG's comment: Remove "all", minimum requirements is defined.
(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.	Change the term "classify" to "categorize". As a federal agency the term "classify" has a different meaning than what is implied here (e.g., classify = TOP SECRET). This comment applies to all sections herein that use the term "classified" or "classify." See NIST cyber standards. BPA Transmission is in agreement with the WECC EMS WG's comment: The use of unauthenticated personnel is anomalous to the rest of the document. Unauthorized is a better term. Even some authenticated personnel may not necessarily be authorized.
(iii) Protection Responsible entities must identify the information access limitations related to critical cyber assets based on classification level.	BPA Transmission is in agreement with the WECC EMS WG's comment: "as defined by the individual entity" should be included after classification level to read "…classification level as defined by the individual entity." It would even be better to use standard language here. FIPS 199 give a method of defining security levels which may be more appropriate The phrase "identify the information access limitations" is unclear. Change to "prescribe protection measures based on categorization for critical cyber asset information."
(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.	Separate the assignment of roles from the definition of roles.
(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.	The term "access management to information" is unclear. BPA Transmission is in agreement with the WECC EMS WG's comment: Remove "or used by". Access Revocation/Changes: Should be reworded to read: Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished in a time frame that ensures critical cyber assets are not compromised.
(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.	If a scope statement addressing critical cyber assets is defined - this section OK.
(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.	Change "its written cyber security policy" to " a written cyber security policy(s)." This comment applies to all sections herein that use "its policy". BPA Transmission is in agreement with the WECC EMS WG's comment: Policies are supposed to be broad with a life cycle of 3-5 years. This should be changed to "reviewed as needed with a minimum review of every 5 years".

(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.	Define Information Protection and Cyber Security. BPA treats these as one program. In the phrase "to the classification level assigned to that information.", change "classification" to "sensitivity". BPA Transmission is in agreement with the WECC EMS WG's comment: To be consistent, change title to Information Protection Program.
(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.	BPA Transmission is in agreement with the WECC EMS WG's comment: Remove "within five days" from section (i). The effort required to make this an auditable function only creates unnecessary administrative overhead and distracts from the intent of the control. The review periods seem to be too often and don't seem to synchronize with each other in this section.

(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.	In federal terms this is the Accreditation portion of a certification and accreditation process. I don't see any mention of an Interim Authority to operate, which recognizes significant risks, and accepts them for a given period of time, while providing (within the organization) a corrective action for those risks. BPA Transmission is in agreement with the WECC EMS WG's comment: Remove the last line. The effort required to make this an auditable function only creates unnecessary administrative overhead and distracts from the intent of the control.
(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.	Change "investigations" to "inquiry". In Federal perspective investigation means criminal. Clarify who can file Complaints.
(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.	Refer to Audit records section.
(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.	"Written cyber security policy" needs to be redefined as "Any written cyber security policy(s) which incorporates the requirements of this standard." As a federal agency, public entities such as NERC compliance monitors may not have access to all BPA's policies or procedures under applicable regulation or law. There is no provision here for non-disclosure agreements with the compliance monitor. This will limit the scope to what others has access to.
(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.	The term "critical bulk electric system asset" is first defined here, but not in the definitions section. The phrase "preferred risk-based assessment" should add the word "methodology" to the end.
(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.	This is an alternate definition of critical cyber asset. A clearer definition is needed. Protocol and dial up are not measures of criticality, they are risks to the security of the asset.
(3) A senior management officer must approve the list of critical bulk electric system assets and the list of critical cyber assets.	BPA Transmission is in agreement with the WECC EMS WG's comment: Should be worded in a way that would enable identification by category, not just individual asset. Example would be that any device placed within the Energy Management System environment would automatically be covered and would not have to go to senior management.
(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	As a federal agency, FISMA requires BPA to follow FIPS-199 as the standard by which to categorize the criticality all information and information systems.
(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.	BPA Transmission is in agreement with the WECC EMS WG's comment: Replace "personnel subject to the standard " to "personnel having access to critical cyber assets". BPA comment - We are looking to ensure that persons who have been identified by the utility/agency as being of a certain risk level, should have the appropriate training.

(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.	Section (iv): Each utility/Agency should define the level of check required. In our case, those who are identified as being Level 2 security positions by OPM's (U.S Office of Personnel Management) definition, will require a level of background check and possibly federal clearance that will be defined by the agency. Also note that SSN or SIN checks are not good enough to detect problems, even when coupled with Criminal checks. We find that doing a credit history, job history and education check often provides information that would not have been revealed by the SSN and Criminal checks. There is also no mention of verification of citizenship or association with terrorist sponsoring countries here. The minimum SSN & 7 yr criminal checks they prescribe may be in conflict with "federal, state, provincial, and local laws." Add a clause "where allowed by federal, state, provincial, and local laws.".. BPA Transmission is in agreement with the WECC EMS WG's comment: Access revocation is covered within other sections of this standard. Should be reconciled to ensure consistency. In Canada, the equivalent is the Social Insurance Number (SIN) and should be added.
(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.	Item 2. It may be legally problematic to keep certain documents. Some flexibility needs to be built into this section. Records may, for example, be maintained by a contracted background checking organization rather than the agency. This would relieve the agency of legal liability for the sensitive documents while still allowing them access when required.
(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.	Reword "critical cyber assets reside and all access points to these perimeter(s)" to "critical cyber assets and all access points to the perimeter(s) reside." Change "implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical assets within them" to "implementation of access control to critical assets within the logical security perimeter."
(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.	The phrase "access is controlled" should read "access should be controlled" (See the comments for Electronic Security Perimeter. The description of communication links and end points is ambiguous and seems to assume only hard wired infrastructure. Do microwave towers and communications equipment, and fall under this definition if they are the end points?
(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.	The statement "implement the organizational, technical, and procedural controls to manage logical access" is very nebulous. There are three types of controls: Management (sometimes known as Administrative), Operational (sometimes known as Physical), and Technical. Procedural controls are a form of management control, as is organizational control. But technical controls are not management controls. This section is mixing these, and the section heading is "Electronic Access Controls" which are a form of Technical control. What is "external interactive logical access"? If the standard wishes to be prescriptive about procedural controls or technical controls in order to ensure authenticity, then it should be clear about which applies and place them in the proper section accordingly. BPA Transmission is in agreement with the WECC EMS WG's

	comment: Strong is a subjective term and needs to be clearly defined. Suggest simply removing the subjective word “strong”. Add “where equipment supports banners” to the end of the last sentence to read “…use banner upon interactive access attempts, where equipment supports banners.” Or reword as follows: "Where technically possible, 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).	How do you define and gauge an “in-depth defense strategy”? The statement “When physical perimeters are defined” implies that they may not be defined. However it is earlier stated that defining a “physical security perimeter” is a requirement. This should be resolved. The “different security levels” are vague, and should be tied to an assessment of the residual risk to the critical cyber assets and the impact of their loss or compromise. Suggested text: Physical perimeters shall be defined and where possible, layers of physical security shall be implemented with different security levels to these perimeters depending on the level of criticality of 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 orprevents 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 nonproduction environment. All testing must be performed	BPA Transmission is in agreement with the WECC EMS WG's comment: Remove "Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment." The last sentence is an adequate statement.

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 semiannually. 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.	It has been our experience that having "Strong" passwords is not a measure of protection. Protecting the password files themselves is more valuable that having strong passwords. Strong passwords merely slow down unauthorized access a bit. BPA Transmission is in agreement with the WECC EMS WG's comment: Should qualify "strong password" as to where it is technically supported. Not all technology allows for this. Access Reviews is covered within other sections of this standard. Should be reconciled to ensure consistency.
(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.	"In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented." This is too restrictive. It conflicts with "applicable" in 1st sentence. BPA Transmission is in agreement with the WECC EMS WG's comment: The word 'timely' does not adequately reflect the risk management approach that should be used in applying patches.
(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.	BPA Transmission is in agreement with the WECC EMS WG's comment: Needs to state that it will exist "where applicable as defined by the entity".
(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 of three (3) years in an exportable format, for possible use in further event analysis.	BPA Transmission is in agreement with the WECC EMS WG's comment: The first sentence needs to be changed to reflect that audit trails need to be generated, but not necessarily by the asset as described within the first sentence. Not all devices have this capability. Additionally, should state "where technically feasible". What is the definition of "security related system events"?
(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.	BPA Transmission is in agreement with the WECC EMS WG's comment: This section sound very much like section 1301, authorization to place into production. Should be reconciled to ensure consistency. What is the definition of a "controlled environment"? Could be interrupted as a separate test environment, is this what is intended?
(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.	Suggested text - "System backup information should be tested at least annually." Define prolonged period. BPA Transmission is in agreement with the WECC EMS WG's comment: This section is not about archival, it is about back-up and recovery, so the last sentence should be removed.
(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).	As a Federal entity, BPA must report to CIAC, who then reports to ESISAC.
(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.	An alternative wording for this section is: Entities must perform business impact analysis that results in emergency response, disaster recovery, and continuity of operations plans as appropriate to the entity. BPA Transmission is in agreement with the WECC EMS WG's comment: The introduction paragraphs read more like requirements and should be in the appropriate section. Goes back to the formatting inconsistencies. Annual testing of low probability events is to frequent, focus on training our operators on higher probability events has more value and allows them to focus on the job at hand. The last paragraph is very wordy and could be reworded to be clearer.
(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.	

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Raymond A'Brial	
Organization:	Central Hudson Gas & Electric Corp.	
Telephone:	845-486-5677	
Email:	rabrial@cenhud.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☒ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name: Central Hudson Gas & Electric Corp (CHGE)

Lead Contact: **Raymond A'Brial**

Contact Organization: **Central Hudson Gas & Electric**

Contact Segment: **1**

Contact Telephone: **845-486-5677**

Contact Email: **rabrial@cenhud.com**

Additional Member Name	Additional Member Organization	Region*	Segment*
Gary Wright	**CHGE**	**NPCC**	**1**
William Ziegler	**CHGE**	**NPCC**	**1**
			0
			0
			0
			0
			0
			0
			0
			0
			0
			0
			0
			0
			0
			0
			0
			0
			0
			0
			0
			0

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

CHGE's participating members recommend that the definition of Critical Cyber Assets be;

Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).

Under Bulk Electric System Asset what is meant by large quanities of customers. tandard needs to have one single industry definition.

Incident and Security Incident - Inadequate for usage in subsect. 1307

CHGE's participating members recommend changing the Incident definition from

Additional terms may need to be added - Even if terms are not defined, they need to be used with greater consistency, and consistent terms need to be chosemn. For example: there are intentional differences amoung key staff, employee and personnel.

CHGE's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?

CHGE's participating members feel there is much redrafting to be done to the standard.

Standard 1300 is based on what the critical BES assets are, which is defined in 1302.a.1. Per question 1, CHGE's participating members do not agree with that definition and have made suggestions as to what the Drafting Team may do to address the issue.

CHGE's participating members also believe the need to change the Incident definition.

As previously discussed and commented on in various forums, CHGE supports the NERC decision to move away from monetary sanctions.

CHGE's participating members have also expressed concern over the incremental administrative tasks and documentation requirements to be compliant with this standard and hopes the Standard Drafting Team will consider this during the development of the associated Implementation Plan.

Throughout the document, the compliance levels should be updated to measure the proposed revisions suggested below. CHGE has made some recommendations in this regard.

There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected and recognized with consideration of this Standard.

The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to gauge the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. It is CHGE's hope that this will be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.

CHGE's participating members agrees with the intent of Section 1303. The term background screening however has too many issues for CHGE participating members and recommend that this section's title become Personnel Risk Assessment. Portions of 1303 are too prescriptive and CHGE's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk and have made recommendations later in the form that will make this Section acceptable.

The references within the standard made to other portions of Standard 1300 are not correct. Without clear references, CHGE cannot determine if the document is acceptable or not. For example, 1301.a.3 says as identified and classified in section 1.2. Where is this section? Each one of these incorrect references must be corrected.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

Correct references as covered in question 2.

Request clarification on what information is protected in 1301.a.2.

Change 1301.a.2 from;

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

to

The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets. (CHGE's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)

Change 1301.a.2.i from;

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.

to

The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well. (CHGE's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)

1301.a.3 Needs clarification.

Change 1301.a.3 from; ….entity's implementation of… to …entity's implementation and adherence of…(CHGE's participating members believe it is important to stress that not only is it important to implement this Standard but to adhere to it as well.

1301.a.3 - shall assign a member of senior management. needs clarification to address major operating subdivisions.

1301.a.5.iv The 24 hours rule for change.termination of access may be too short - inconsistent with other limits in 1300. Should onlu apply to dimissals for cause - routine transfers should allow 3-5 days(even NRC allows 7 days for a favorable termination, and FERC allows 7 days regarding market access.)

1301.a.6 Move to 1306

1301.d.1 on-site reviews every three years What does this mean? Period is acceptable if review is part of a NERC audit, but too frequent if conducted by a hired auditor.

1301.d.2 (and throughout the document) make the reference three calendar years for clarity and consistency in the reference for retention of audit records.

1301.d.3.ii, change from address and phone number to business contact information. Also on page 5, 1301.b.5.iii to ensure the protection of the identity/personal information of the affected individuals

1301.d.3.iv, request clarification that this audit applies to only audits on RS 1300, carried out by the compliance monitor

Recommend that under Regional Differences, it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor

1301.e.1.iii, request clarification on 30 days of the deviation. Also please explain the difference between deviation and exception. This does not match the FAQ 1301 Question 4.

1301.e.2.iii, change from;

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

to

An authorizing authority has been designated but a formal process does not exist to
test, validate and deploy systems into production, or (CHGE believes it was the drafting team's itent to deploy the system rather than promote which has a different connotation associated with it,)

Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change Executive Management to Senior Management for consistency and clarity.

1301.e.4.xi, repeat of the earlier 24 hours if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).

CHGE Participating Members believe that the concept of the Bulk Electric System and association definitions may not be appropriate to capture the intent of the standard. CHGE suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.

Replace the 1302 preamble and 1302.a.1 and 1302.a.2 as shown below, with;

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 which support the reliable operation of the bulk electric system.

The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.

(a) Requirements
Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.

(1) Critical Bulk Electric System Operating Functions and Tasks

The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:

- monitoring and control
- load and frequency control
- emergency actions
- contingency analysis
- arming of special protection systems
- power plant control
- substation control
- real-time information exchange

1302.a.1.i.A Clarify that telemtry does not include telecomm equipment.

1302.a.1.ii move to definitions

1302a.1.ii Does generating resources include physical and market resources? If it includes market resources, how is a determination by the buyer that a resource is critical to be communicated to the seller and/or generator? How is this performance to be evaluated, and by whom? This applies to voltage support.
Define common system

1302.a.1.iv.B What is meant by initial?

1302.a.1.v - Define common system

1302a.1.vii.A - Needs to clearly exclude nuclear assets.

(2) Critical Cyber Assets

(i) In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:

(a)(2)(i)(A) – Underline and to emphasize it.

A) The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.

B) The consequences of the Operating Function or Task being compromised (i.e. highjacked) for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.

C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.

D) Known risks associated with particular technologies

(a)(2)(i)(D) – if kept appears to have dropped a not: should read "which do not use a routable protocol"…

Change 1302.g.1 from;

(a)(2)(i)(E) – Unmatched reference to 1302.1.2.1.

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.

to

1 Critical Bulk Electric System Operating Functions and Tasks
(i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1.

Change 1302.g.2.i from;

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.

to

The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure

(g)(3)(i) – Unmatched reference to 1302.1.2.1.

Change 1302.g.5 from;

Critical Bulk Electric System Asset and Critical Cyber Asset List Approval

to

Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval (CHGE believes that it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations of operations is lost.)

Change 1302.g.5.i from;

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

to

A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained.

Change 1302;
critical bulk electric system assets

to

critical bulk electric system operating functions and tasks

1303, CHGE's participating members agrees with the intent of Section 1303. The term background screening however has too many issues for the CHGE participating members and recommend that this section's title become Personnel Risk Assessment. Portions of 1303 are too prescriptive and CHGE's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk.

(a)(4) – Term unrestricted access does not appear anywhere else – delete, or (even better) clarify and use consistently (i.e., some access may be restricted and thus may not require as high a level of employee/contractor clearance).

The FAQ describes supervised access, 1303 does not touch upon this topic.

Change 1303.a.4 title to Personnel Risk Assessment.

Change 1303.a.4 to A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks.

Change 1303.a.2 from;

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.

to

The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets

1303.a.4 from;

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.

to

Personnel Risk Assessment: There must be a documented company personnel risk assessment process.

Add to 1303 Measures.2, a training measures for disaster recovery (1308) and incident response planning (1307).

The numbering of 1303 starting with Measures needs correction.

1303 Measures 4.i, request clarification. Does this include third party personnel?

Change 1303.Measures.4.i from;

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).

to

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 respective security perimeter(s). (CHGE believes there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)

Change 1303.Measures.4.ii from;

two business days

to

seven calendar days, per earlier comments and to keep consistent with FERC Order.

1303.Measure.4.iii, change 24 hours to 24 hours if terminated with cause or disciplinary action, or seven days, per earlier comments

1303.Measure.4., remove;

Subsections iv, v and vi.

and replace with

There must be a documented company personnel risk assessment process. these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities

1303.Compliance Monitoring Process.2,

(i)(4th bullet) What is meant by reviews?

CHGE's participating members do not agree with background screening documents for the duration of employee employment. and suggest changing the last bullet in (i) to Verification that Personnel Risk Assessment is conducted.

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of Background investigation program exists, but consistent selection criteria
is not applied, or" to Personnel risk assement program is practiced, but not properly documented, or

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to Personnel risk assement program exists, but is not consistently applied, or

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to Personnel risk assement program does not exist, or

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to 24 hours with cause or seven days (as mentioned earlier). Change personnel termination to personnel change in access status.

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to Access control list exists, but is incomplete.

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from two days to 24 hours with cause or seven days (as mentioned earlier). Change personnel termination to personnel change in access status.

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from cover two of the specified items to cover two or more of the specified items.

Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii

From 1304.a.2, remove Electronic access control devices shall display an appropriate use banner upon interactive access attempts. because it does improve security. This banner assists in legal matters.

Change 1304 a.2 Electronic Access Controls:
to
The responsible entity shall implement a combination of organizational, and/or echnical, and/or 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).

Change 1304 a.3 Monitoring Electronic Access Control:
to
The responsible entity shall implement a combination of organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."

Change 1304 a.4 from;

The responsible entity shall ensure that all documentation reflect current configurations and processes.

to

The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.

1304.a.4 Remove -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. (This is a measure and should be removed here)

Compliance Monitoring Process;
Change 1304.d.3 from;

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

to

The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:

Level of non compliance
Level three-Supporting documents exist, but not all transactions documented have records - this part is ambiguous and should be clarified.

(e)(2)(2nd parag.) – The phrase for less than one day is unclear in context – substitute Access to any critical cyber asset remains unmonitored for some period that does not exceed 24 hours.
1305 Physical Security;

Eliminate the bulleted items in the Preamble to Section 1305-they appear in the Requirement section.

Replace 1305 a.1 with;
Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.
• The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),
• The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and
• The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."

Change the following - (a) Requirements;
"(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."

to

(3) Physical Access Controls: The responsible entity shall implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.
(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.
(5) (We recommend deleting this bullet as the intent is captured in bullet 4).
(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."

Change Measures;

(b)(3)(table)(4th item) – Too restrictive a definition: consider changing name from Security Cage to Additional Perimeter or Internal Perimeter – in any event, change the definition to read: An Additional, internal secured perimeter within a secured area that permits additional control of physical access to a cyber asset within a larger (usually secured) perimeter, such as by means of a cage or cabinet.

(b)(3)(text)(2nd parag.) – documentation [re implementation] for each physical access point: Far too much paperwork for numerous, identical physical access points. Where there are several identical or substantially equivalent access points for one or a group of security perimeters, this language should be interpreted as requiring only records indicating the controls implemented for the type of access point, and the location of each such individual point. Better to change the language to read: for all physical access points.

(b)(4)(table)(2nd item) – Wording implies that an audible or visual alarm must go off at every access. This would lead users to turn off or ignore the alarm. Only unauthorized or forced access events should be alarmed. This item should be revised to read as follows:
Access Control System – A system that logs and record each access event, including those of unauthorized or forced entry (which must give rise to an alarm. When an alarm is appropriate, the alarm system must be based on" [REMAINDER OF TEXT AS IN ORIGINALLY PROPOSED DRAFT]

(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.

to

The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility.

(b)(5)(table)(1st item) – Manual logging will be difficult or impossible at unmanned locations, and is not even required by the NRC at all locations. Moreover, for safety reasons, access to unmanned substations must be reported by phone, etc., in almost all circumstances. The supporting text should be modified to read: "A log book or sign-in sheet or other record of physical access accompanied by remote verification."

In 1306.a.1, last paragraph, modify the second sentence to read as follows;

Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."

(a)(2) – The last sentence should have a phrase inserted to clarify the intent, so that the operative reads: "must establish end-user (e.g., administration, system, and guest) account management practices."

(a)(2)(i) – Implementation of strong passwords may not be possible on legacy equipment. The sentence should read "Where practicable, strong passwords for accounts must be used in the absence of more sophisticated methods such as multi-factor access controls."

1306.a.2.ii change pooding and puffing to putting (it appears a pdf translation problem as some documents the group printed have it and others did not)

1306.a.2.ii remove Generic from the title

1306.a.2.iii, use at least annually instead of at least semi-annually

Change 1306.a.3 – As proposed, this is impossible to implement for all legacy equipment. In addition, the last sentence is overly prescriptive – compensating measures are not necessary or possible in every instance. The last sentence should be revised: Where installation of a patch is not practicable or possible, alternative compensating measures must be evaluated, and that evaluation, as well as any such measures actually taken, must be document.

Remove the last sentence in 1306.a.3, In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented.

Change 1306.a.4 – The listed malicious software is not complete – use a broader term to cover it, such as mal-ware.

(a)(5) – Controlled penetration testing is almost always done by third parties, and is very expensive – certainly far too expensive and intrusive to require on a yearly basis. Reference to such testing should be removed from the standard and placed – only as an example – in the FAQ.

1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).

Change 1306.a.6 to

Legacy equipment may not be able to generate audit trails. The first sentence should begin with the phrase Where practicable, critical cyber security assets must generate…

1306.a.7 Remove Configuration Management from the title

1303.a.8 Remove the word inherent it is not clear what is meant by it.

1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.

1306, remove 1306.a.11 since 1308 addresses back-up and recovery.

1306.b.1, remove Test procedures must also include full detail of the environment used on which the test was performed. Also replace potential with known in the last sentence. Also in the last sentence insert the words if possible at the end of the sentence.

1306.b..2. – Move the entire subsection to 1303, and reword to bring it into conformity with that section.

1306.b.3, remove;

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.

and change

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.

to
The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability.

1306 b.3 first sentence-eliminate the word management.

1306.b.4, remove anti-virus, anti-Trojan, and other" from the first sentence.

1306.b.4 third sentence Change
..so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware.

to

..mitigate risk of malicious software.

1306.b.4 Remove the second sentence.

1306.b.4 Replace the fourth sentence with;

Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented.

1306.b.5 remove the first sentence.
Based on the common use of third parties for outsourcing of this associated work of vulnerabilty assessment, it is not reasonable to maintain the information called for in sentence one.

Change 1306.b.6 from;

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.

to

Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis.

1306.b.7 In the final sentence remove the word all and change the heading by deleting and Configuration Management

Remove 1306.b.11, since 1306.a.11 was removed.

1306.d.2, change from The compliance monitor shall keep audit records for three years. to The compliance monitor shall keep audit records for three calendar years.

1306.d.3.iii, change system log files to audit trails

1306.e.2, change the monthly/quarterly reviews to the reviews

1306.e.2.ii.C, change anti-virus to malicious

1306, the Compliance levels should be updated to match the above measures.

1307 Retitle this section to be more specific and clear: Incident Reporting and Response Plan.

1307, spell out and provide clarification on the acronyms throughout.

Change 1307, from;

Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified.

to

Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified.

(a)(2) delete this entire subsection, consistent with the revision in the Definitions to remove reference to “Incident.” The standard should only be applicable to malicious and/or suspicious (security) incidents.

1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;

"Incident and Cyber Security Incident Reporting"

to

Security Incident Reporting.

and also Change from;

The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP).

to

The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)." or perhaps even be to the CIPIS, rather than the IAW-SOP.

Refer to our definition of a security incident, change 1307.b.5 from;

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

to

The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements.

Change 1307.b.6 from The responsible entity shall retain records of incidents and cyber security incidents for three calendar years.

to

"The responsible entity shall retain records of security incidents for three calendar years."

Change 1307.b.7 from The responsible entity shall retain records of incidents reported to ESISAC for three calendar years.

to

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

1307.d.1 there is a 90 day reference that does not appear in the measures.

In 1308, to remain consistent with the scope of critical cyber assets, it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.

Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Allen Klassen	
Organization:	Westar Energy	
Telephone:	785 575-6073	
Email:	Allen_Klassen@wr.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☒ SPP ☐ WECC ☐ NA - Not Applicable	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☒ Yes

☐ No

Comments

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
Clarification of requirements of the increased scope of 1300 vs 1200.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
Please do NOT use an existing NERC Policy i.e. Policy 1.B as a reference to define a requirements.

Pick a value, such as 800 Mws, or define the requirement directly in this standard. Reference to a document that is planned to be obsolete and does not address cyber security only adds confusion to the interpretation of this standard.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:		
Organization:		
Telephone:		
Email:		
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT** ☐ **ECAR** ☐ **FRCC** ☐ **MAAC** ☐ **MAIN** ☐ **MAPP** ☐ **NPCC** ☐ **SERC** ☐ **SPP** ☐ **WECC** ☐ **NA - Not Applicable**	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name: Pepco Holdings, Inc. - Affiliates

Lead Contact: **Richard Kafka**

Contact Organization: **Potomac Electric Power Company**

Contact Segment: **3**

Contact Telephone: **(301) 469-5274**

Contact Email: **rjkafka@pepco.com**

Additional Member Name	Additional Member Organization	Region*	Segment*
Ken West	Conectiv Power Delivery	MAAC	1
Mike O'Grady	Potomac Electric Power Company	MAAC	1
Dennis Leonard	Potomac Electric Power Company	MAAC	1
Brian Carroll	Conectiv Power Delivery	MAAC	1
Carl Kinsley	Conectiv Power Delivery	MAAC	1
Alvin Depew	Potomac Electric Power Company	MAAC	1
George Muller	Conectiv Energy	MAAC	5
Glenn Hein	Potomac Electric Power Company	MAAC	1
Paul Miller	Conectiv Power Delivery	MAAC	1
Bill Griffin	Conectiv Power Delivery	MAAC	1
Vic Davis	Conectiv Power Delivery	MAAC	1
David Thorne	Potomac Electric Power Company	MAAC	1
Jim Lasher	Potomac Electric Power Company	MAAC	1
Ted Bower	Conectiv Power Delivery	MAAC	1
Mark Godfrey	PHI Power Delivery	MAAC	1

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

While the definition section offers some clarity, it is not entirely clear what is in scope and out of scope for this standard. Clarification with some of the existing definitions is needed (e.g. Bulk Electric System Asset and Critical Cyber Assets) to help with the understanding of what is in scope. Additional definitions are required for terminology utilized in the standard which are not presently defined under the definitions (e.g. Under Control of a Common System, Compliance Monitor, Routable Protocol, differentiation between Special Protection Scheme and a standard Protection System,). In some cases the definition is provided within the standard or FAQ rather then in the definition section (e.g. Section 1302.a.1.ii). In some cases there are inconsistencies in the standard (e.g. Section 1306.b.2 and Section 1301.a.5.iv.) where a definition might offer consistency. Specific details supporting the comments above are provided under Question 3, Additional Comments.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
The first draft of Standard 1300 is a good start in helping to focus cyber security beyond EMS/SCADA systems. Certainly a standard is needed across the industry. However we believe that there are significant issues that need to be resolved prior to this standard being ready for vote. The most significant issues include clarification on what is in scope and out of scope for the standard. Clear definitions will help in this effort. In addition, listing what is out of scope for the standard (similar to what was done in the Urgent Action Standard 1200) would be helpful. For example based on the NERC webcast, it is our understanding that communication systems are out of scope (as well as nuclear). Inconsistencies between sections in the draft and other NERC or industry standards need to be addressed as well. It is our understanding that this standard will be reliant on or impacted by other NERC standards or policies that either exist, are being revised, or are under development (e.g. Standard 200, a telecommunication standard, a risk assessment guide or standard). It would be helpful to reference these standards within Standard 1300 when there is an overlap or touch point. Security efforts and requirements for EMS/SCADA systems, substation equipment/systems, and generator control systems can and should not always be the same (e.g. Section 1306 applies mainly to EMS/SCADA systems). These differences are further complicated if these systems are networked and utilizing routable protocol. Having separate sections/requirements in the standard for EMS/SCADA systems, substation equipment/systems, and generator control systems would help clarify these differences and the security expectations (e.g. splitting Section 1306 into 3 sub-sections). We believe that the incident reporting requirements should only focus on security incidents. Equipment and system failures are common (e.g. modem problems or telephone equipment problems). These general incidents may not only be burdensome but may mask actual security incidents because of their volume. In the FAQs (Section 1304, question 3) different solutions are listed as a means of providing an electronic security perimeter. This is very helpful and could be expanded. Please note that one method listed does not necessarily meet the requirements of Section 1304.a.3 and has a known security weakness (i.e. dial-back modems do not usually provide logging capabilities and have proven to be an insecure means of user authentication because of dial-back spoofing). There is no implementation plan included in this draft. We appreciate that the drafting team on page 3 of this Comment Form acknowledges this and states that an implementation plan will need to take into account the time needed to attain compliance. Page 3 also states that a plan will be developed at a later date for posting with a subsequent draft of this standard. An implementation plan will be needed at the same time of a revised standard in order to determine if the standard is ready to go to ballot. Specific details supporting several of the comments above are provided under Question 3, Additional Comments.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
General: Should or will the FAQs be part of standard? The FAQ provided a great deal of clarification of the intent of the standard. It is preferred that the standard be reworked to avoid the need for a separate document to assist in its interpretation. At the very least, the FAQ's need to be made consistent with Standard 1300 and referenced by the standard.
General: The standard does not specifically address whether protective relays connected via non-routable protocols are in scope or not. The original urgent action item 1200 specifically excluded electronic relays installed in generating stations, switching stations, and substations. The only reference to protection systems is special protection systems in the new standard. Standard relaying systems (used to isolate faulted elements) are not specifically included or excluded from the new NERC 1300 standard. Clarification should be provided.
General: If standard protective relay systems are included, because of remote communication access, more detailed requirements need to be provided for the physical and electronic security perimeters of the dial-up access point. It appears the thrust of the standard is to address access to those cyber assets which could affect multiple facilities or components from a single access point. Using the example provided in the FAQ section 1304, question 3, access to a single RTU controlling a critical bulk asset in a substation, which doesn't use a routable protocol, does not require an electronic security perimeter at the RTU. It continues to say if a dial-up modem is used, an electric security perimeter is required just around the dial-up access point. Is the access point the location in the substation, or the remote terminal calling into the substation? It appears obvious that the access point mentioned above should be located inside the electronic security perimeter in the substation, but the standard does not specifically outline this concept. A similar analogy needs to be drawn for protective relay access. If protective relays in a substation do not use a routable protocol, do they only require a security perimeter around the dial-up access point in the substation? When addressing dial-up access, the discussion of security perimeters should be specific as to what requirements are for the local and remote access point.
General: An inconsistent timeframe for removal of access after an employee's change in status is used in the standard. In section 1301.a.5.iv, access to a critical cyber access should be accomplished within 24 hours of a change in user access status. Again in section 1303.l.4.iii (1303.b.4.iii), a 24 hour timeframe is mentioned. Section 1306.b.2 says Upon normal movement of personnel out of the organization, management must review access permissions within 5 working days. A 5 day timeframe for normal movement (transfers, etc) is more reasonable.
General: Unmatched references appear through out the standard (e.g. Section 1302.a.2.i.E refers to Section 1302.1.2.1 which does not exist). Apparently the nomenclature changed from all numeric to alternating numeric and alpha characters. All references need to be reviewed and corrected.
General: At the end of each of the eight sections of the standard it states, Sanctions shall be applied consistent with the NERC compliance and enforcement matrix. Will the matrix be included in the standard or should there be a specific reference where this is located/maintained (e.g. separate document or standard)?
Definition: The definition of Responsible Entity needs clarification (e.g. Is all generation included? Excluded?). Section 1301.a.3 (Page 3) uses Responsible Entity and the present definition does not assist in understanding this section.
Definition: Other terms used in the standard should also be defined. Such terms include Routable Protocol, Dial-up access point (local vs. remote), differentiation between a Special Protection System and a Standard Protection System.
Definition: A clearer definition to understand what assets are considered is needed for Critical Assets as it applies to Generation. Section 1302 specifies a range of assets that are considered critical. It is not clear enough. For example, the implication of Section 1302.a.1.iii.a in

combination with the referenced NERC reportable incident definition is that ANY entity with even a single small generator would have that generator a critical asset since it would be the largest single generator under that entities control.
Definition: Recommend utilizing the CIPC definition of Critical Cyber Assets.
Definition: There is a need for a single industry definition for Bulk Electric System Assets and Critical Bulk Electric System Assets. What is meant by large quantities of customers or significant impact or risk? Perhaps the IAW-SOP definition in the FAQs should be utilized or referenced.
Definition: Clarity is needed between the definitions of Incident and Security Incident. Recommend removing the definition of Incident and clarify the definition for Security Incident. (e.g. Security Incident: Any malicious act or suspicious event that compromises or was an attempt to compromise the electronic or physical security perimeter of a critical cyber asset; or, disrupts or was an attempt to disrupt the operation of a critical cyber asset.)
Definition: The standard refers to a Compliance Monitor (e.g. Section 1301.d.1) but provides no additional detail. Can this be a company's internal auditors? Must it be an outside party? Recommend adding Compliance Monitor to the definitions.
Definition and Section 1302.a.1.iii.a: Define Under Control of a Common System and give examples; clarify how this applies with examples.
Definition (Section 1302.a.1.iii.b): Define Generation Control Centers.
Definition (Section 1302.a.1.iv.B): What is meant by Initial system restoration (e.g. one bus away)?
Definition: Define Having Access for the purpose of Section 1303? [Is this only for physical access?]
Definition (Section 1303.a.4): The term Unrestricted Access does not appear anywhere else. Please clarify meaning and use (i.e. some access may be restricted and thus may require different levels of employee/contractor clearance).
Definition (Section 1303.n.2.i.4th bullet): What is meant by Reviews?
Definition (Section 1304.a.2): What is meant by External interactive logical access?
Definition: Clarify Four-wall Boundary in Section 1305.a.2.
Definition (Section 1306.a.8): What is meant by Inherent services?
Definition: Clarity is needed on the dial-up perimeter definition. Does it only include the modem or does it also include the device providing password security? If a device dials a critical cyber asset is the device in scope?
Definition: Even if terms are not defined, there is a need for terms to be used consistently (e.g. Are there intentional differences among "key staff," "employee," and "personnel"?).
Section 1301.a.3: This section states the responsible entity shall assign a member of senior management in order to ensure compliance with the standard. Does this mean there should be only one responsible/accountable member of senior management? Most large utilities have major operating subdivisions (e.g. regulated T&D, unregulated Generation, and Corporate IT)? Does one individual have to be designated or can this be a shared designation/responsibility?
Section 1301.a.5.iv (Page 4): Recommend having different requirements for revocation/changes for users terminated/dismissed with cause (i.e. potential hostile employee or contractor) versus other more routine user changes (e.g. employee changing positions). Timeline for terminated/dismissed with cause should be more stringent. (Section 1306.b.2 of the draft standard does in fact make this distinction and appears to be in conflict with Section 1301.a.5.iv.) There are inconsistencies with other standards or guidelines on the timeliness needed to make the change (e.g. FERC Code of Conduct: 7 days regarding market access, NRC: 3 business days for normal changes; and inconsistencies within the draft 1300 Standard (e.g. 1306.b.2)).
While EMS/SCADA systems and network devices may be able to meet a more stringent time criteria, this may be not be possible to meet for dial-up substation equipment.
Each in-scope dial-up substation device would need to be manually called up and/or visited to change access passwords. This is not practical within a 24 hour period. In addition the password

change would need to be communicated to all potential support staff in the same period. The effort involved will be dependent on the clarity on what is in scope for the electronic perimeter for dial-up devices that are serially connected. If the perimeter includes the serial devices the challenge will be even greater. The security risk for dial-up devices should be less than devices using routable protocol (i.e. on a network). Can and/or should dial-up have a less stringent timeline than devices using routable protocol or EMS/SCADA systems?
Section 1301.a.6: Recommend moving to Section 1306.
Section 1301.d.1: This section states outside reviews should be done every three years. What does this mean? Period is acceptable if review is part of NERC audit – too frequent if conducted by hired independent auditor. Suggest longer cycle times between certification and external reviews.
Section 1302.a.1.vi (Page 10) and Definitions: How does a Generator Owner know if their assets are deemed a critical electric bulk system asset? What if a Transmission Owner believes a Generator Owner is a critical electric bulk system asset (e.g. voltage support for system) but the Generator Owner does not agree? Who has responsibility of the electronic or physical perimeter if the perimeter includes assets from both a Transmission Owner and a Generator Owner?
Section 1302.a.2.i.C - Suggest clarifying the wording to read, The cyber asset is dial-up accessible and connected. [Further discussion suggests that this WILL apply to cyber-assets with modems if those modems are periodically connected, since for the period in which they are connected they will meet the criteria. The implication of this is that those assets will be subject to the standard and the associated access lists, controls, monitoring etc, and that the modem requires security measures such as call-back or other authentication. Does a procedure and log requiring physical disconnection of a modem telecom connection meet the security control requirements?
Section 1302.a.2.i.D: The text should read, Dial-up accessible critical cyber assets, which do not use a routable… (The word Not appears to have been omitted from the original text).
Section 1304.a.2.2nd paragraph: Clarify that this display is intended for the user to see, saying essentially that they should Follow Policy. Insert language similar to Where technically feasible in order to recognize that some equipment cannot be made to display such screens (e.g. substation electronic equipment).
Section 1304.a.3: This section discusses the controls for monitoring authorized access and detecting unauthorized access. How does this apply for dial-up access? In the FAQ section 1304, question 3, the use of SCADA controlled, or dial-back modems, was listed as a means of electronic security perimeter. Dial-back modems would not necessary meet the requirements of Section 1304.a.3, as they do not usually provide logging capabilities. Additionally, dial-back modems have proven to be an insecure means of user authentication. From Schweitzer Engineering Laboratories paper, Attack and defend tools for remotely accessible control and protection equipment in electric power systems, available at http://www.selinc.com/techpprs/6132.pdf, pg. 16. Dial-back security was once common in the electric power industry, but is no longer adequate because of dial-back spoofing. Hackers have learned to fake the hang-up tone and remain on the line while the called modem attempts to dial its predefined dial-back number. Hackers just ignore the incoming dial tones and issue an answer tone that reestablishes connection to the dial-back modem. Thus, the dial-back has been spoofed or fooled into an unauthorized connection.
Section 1305: Regarding self-certification, will there be a standard form to complete?
Section 1306.a.2.i: Existing hardware is grandfathered for password strength by the phrase, …to the extent allowed by the existing environment. To what extent is other equipment grandfathered, such as logging capability of dial-up equipment and the ability to display an appropriate use banner?
Section 1307: As written, it appears that this the section requires reporting of all incidents including equipment failures or software configuration errors. If this assessment is correct, would all hung-up or failed modems need to be reported? Should non-security related incidents be outside the scope of this standard? We believe the standard should focus only on security incidents. If not the ESISAC may be inundated with repetitive and ultimately useless information

possibly masking the security incidents due to the volume of non-security incidents. Are ESISAC reported events available to the public?
Section 1308: The first sentence in the first paragraph does not list transmission owner or generator owner. Were these omitted on purpose? The last two sentences of second paragraph conflict with 1308.a.1 requirement (i.e. a higher probability event with a short duration may not require a recovery plan at all versus the requirement of annually tested recovery plan). The third paragraph states that this will require a redundant or backup facility regarding a control center. Is this a requirement for a redundant EMS/SCADA system? If yes, it is not listed in the requirements or measures. This should be clarified.
Section 1308.a.3: This section states that a responsible entity shall update its recovery plans within 30 days of system or procedural change as necessary and post its recovery plan contact information. What is meant by post (e.g. external internet, internal)?
FAQ Section 1304, question 1: The addition of dial-up connection to relays and RTUs using both routable and non-routable protocols should be added to the diagram. The diagram would be a useful addition to the actual standard..

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:		
Organization:		
Telephone:		
Email:		
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT**	☐	1 - Transmission Owners
☐ **ECAR**	☐	2 - RTOs, ISOs, Regional Reliability Councils
☐ **FRCC**	☐	3 - Load-serving Entities
☐ **MAAC**	☐	4 - Transmission-dependent Utilities
☐ **MAIN**	☐	5 - Electric Generators
☐ **MAPP**	☐	6 - Electricity Brokers, Aggregators, and Marketers
☐ **NPCC**	☐	7 - Large Electricity End Users
☐ **SERC**	☐	8 - Small Electricity End Users
☐ **SPP**	☐	9 - Federal, State, Provincial Regulatory or other Government Entities
☐ **WECC**		
☐ **NA - Not Applicable**		

Group Comments (Complete this page if comments are from a group.)

Group Name: Duke Energy Corporation

Lead Contact: **Tom Pruitt**

Contact Organization: **Duke Power Company**

Contact Segment: **1**

Contact Telephone: **(704) 382-4676**

Contact Email: **tvpruitt@duke-energy.com**

Additional Member Name	Additional Member Organization	Region*	Segment*
Regie Bryant	**Duke Energy Corporation**	**SERC**	**5**
Vicky Bannon	**Duke Power Company**	**SERC**	**1**
Mike Butler	**Duke Power Company**	**SERC**	**5**
Jon Decoste	**Duke Power Company**	**SERC**	**5**
Glen Frix	**Duke Power Company**	**SERC**	**5**
Mike Hagee	**Duke Energy Corporation**	**SERC**	**3**
Ernie Scronce	**Duke Power Company**	**SERC**	**1**
Greg Stone	**Duke Power Company**	**SERC**	**1**
Mark Tully	**Duke Energy Corporation**	**SERC**	**6**
Phyllis Withers	**Duke Power Company**	**SERC**	**1**

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

There is some confusion and need for clarity on some of the terms. See comments in the details section of the accompanying document.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
Scope of the standard; consistency between sections, narratives, measures, and requirements; and certainly organization and editing.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
There are too many to itemize here. Please see the accompanying document.

The efforts of the Drafting Team in posting this initial version of the permanent standard are appreciated.

Comments are provided in two forms – high level and detailed. The high level comments summarize the major themes identified in the detailed comments. The detailed comments provide specific examples of the questions, concerns, and confusion noted in the document and its accompanying FAQ. Wherever possible, constructive suggestions have been offered to improve the document.

High Level NERC 1300 Comments

Scope

Given the critical role played in today's environment, why is the PSE excluded from meeting this standard? The LSE IS included, though the FAQ indicate that loss of load, in and of itself, is not a NERC reliability concern. This is, at best, inconsistent application of this standard. Given the critical role of the PSE in today's environment, the PSE should be included.

Explicitly state that nuclear facilities are excluded from this standard as is stated in the SAR. Since the Drafting Team has structured the standard so that individual entities are charged with defining the scope of assets subject to this standard, this limitation needs to be spelled out.

The draft states that risk assessment of bulk electric assets and all cyber support assets is part of the standard. The standard should also identify another risk assessment of cyber assets to determine their scope. More clarity is needed on the number and types of assessments. How many steps are there – 1, 2, or 3? How is this communicated across ISO and other third party arrangements for conducting operations on the grid?

Administrative Costs

Overall the required processes and frequency of execution are a major concern and likely cost prohibitive to implementation at Duke Energy Corporation.

While Duke Energy agrees with the intent and general nature of the proposed 1300 standard, many of the specific requirements imply significant administrative costs to develop and maintain a significant number of new processes. (A simple change would be to reduce implementation costs by reducing the frequency of executing the processes.)

This is a common concern across a number of operational units at Duke Energy.

One example is the definition of “incident” and the further inclusion of this term in several requirements that would mean the logging and reporting of thousands of discrete events per day. Limiting incident processing to the term defined as “security incident” significantly reduces the administrative burden, but continues to focus on the cyber security health of the bulk power systems that should be monitored.

As well, a large burden is placed on executive senior management to review and approve what could be large number of NERC 1300 related items. This manager should be allowed to delegate this administrative overhead, but maintain the overall responsibility of providing governance to the NERC 1300 regulated company entities.

A majority of the burden is through record keeping and reporting – which have their place, but are dominant in this standard. The cost benefit for such administrative burden is simply not apparent.

Personnel Related Concerns

Another high-level concern is the cost of implementing the personnel-oriented processes described in this draft of 1300. Like many other energy companies, much of the work force at Duke has become contracted or third-party based.

Background checks, training, and other regulations that are not particularly burdensome when addressed over time with full-time employees, become quite problematic with transient, contracted, part-time labor forces, affecting direct and administrative costs.

Costs

Many of the technical requirements of the proposed 1300 standard are either not technically possible with legacy systems or very expensive to implement. Examples include such things as strong passwords, system logging, and procuring and developing complete test systems. This includes physical security implementation (fossil control rooms), site access (cameras at sub-stations) and building physical rooms to isolate equipment.

Narratives /Requirements/Measures/FAQs are Inconsistent

Measures don't match the actual requirements. For example, background checks are more strictly defined in the measures than they are in the requirements.

Answers provided in the FAQ's in some cases do not match wording in the standard. In other places, narratives, measures, and requirements do not match. Wording should be consistent throughout each section.

There should also be some consistency in the timeframes required to remove user-ids and permissions. It is confusing trying to remember what is 24 hours, 48 hours, etc.

Organization and Editing

Although misspellings are relatively few, other organizational and editing errors are substantial. Consistent and sequential numbering/lettering is a must. Inconsistent use of terms in differing sections also contributes to confusion. These problems must be cleaned up prior to ballot.

Compliance planning will need adequate time to put into place.

What is the anticipated timeline for implementation? It would take an extended period of time to get initial 5 year background checks completed for larger entities. Will the plan be phased in over time?

Detailed comments on Cyber Security Standard 1300

Section	Comment for NERC
Definitions	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. – The use of the terms “Incident” and “security incident” must be reviewed and clarified. The definitions are acceptable, where “incident” are common events that could include the thousands of daily pings against secured systems, but “security incident” is one that is anomalous, uncommon, suspicious, or a known malicious event. However, a search on the word “incident” in the document reveals the definitions are misused. Of the 40 occurrences of “incident”, many are confusing; these are included in the next comments below. (In some cases, “incident” is used when it may have been intended to by a “physical security incident”.)
Definitions	Critical Cyber Assets: …power plant control… – Please clarify what is meant. There are numerous power plant control systems that are “indirectly” vs. “directly” related to the production of electricity. Also, please clarify what is meant by substation automation control. Does this include protective relaying and disturbance monitoring equipment?
Definitions	Critical Bulk Electric System Asset – Please define “significant”, “large quantities” and “extended.”
1301	Does this require a data "classification" system and a personnel "clearance" system to be created? Do we have to stamp/mark any potential critical info? The “Separation of Duties” referenced in FAQ#8 should be explicitly stated in the standard.
1301(2)(i) & (v), pg 4	Suggest that these reviews be at least every two years to reduce administrative costs of policy implementation.
1301(a)(1)(ii)	Please define “unauthenticated personnel.”
1301(a)(3), pg 3	Duke agrees whole-heartedly with the need for senior management leadership and management of the implementation of the NERC 1300 standard. However, the detailed tasks listed in these two sections seem to be particularly onerous and time-consuming for a senior manager to personally conduct. We would suggest that for “authorization of any deviation or exception” and for approval of lists of assets, that these tasks be something that could be delegated by the senior manager (particularly the approval of exceptions).
1301(a)(5)(i) & 1301(a)(5)(ii)	The burden of applying such controls on systems at generation and transmission stations is great. The incremental benefit of doing so, taking into account the amount of controls already in place, is minimal.
1301(a)(5)(iii)	What is the frequency of review?

Section	Comment for NERC
1301(a)(5)(iv)	Evaluate changing 24 hours to 2 weeks. For example, physical access to a nuclear station is revoked within the stated 24 hours. Other than that, 24 hours is overly restrictive for revoking access to a single component or system (i.e. turbine control system). In some cases our equipment is not capable of such change. In this case, we are relying on revoking the security badge (i.e. physical access). Network accounts are also disabled within 24 hours. This prevents one from accessing through the corporate network for network connected control systems. The "within 24 hours" should only apply to terminations or required transfer. Other changes due to normal reassignments should be longer and the 10 business day period suggested by others is reasonable. For consistency, all changes to all types of access lists should be changed within 24 hours and normal work reassignments within 10 business days. Suggested re-wording: "Responsible entities shall define procedures to ensure that a modification, due to required transfers or terminations, of user access to critical cyber assets is accomplished within 24 hours of the change having taken place. Other modifications, due to normal transfers, of user access to critical cyber assets is accomplished within 10 business days of the change having taken place. All access revocations/changes must be authorized and documented." Consistency is needed for delegation of approval. Suggested re-wording: "The responsible entity shall maintain documentation of any deviations or exemptions authorized by the current senior management official or designee responsible for the cyber security program."
1301(b)(2)(i)	Request that these reviews be at least every two years to reduce administrative costs of policy implementation.
1301(b)(2)(ii)	This section on controls has six other areas associated with control issues and many of them also have an annual review cycle. There should be some consistency since all six areas are of importance.
1301(b)(5)(i)	Consider changing five (5) days to 2 weeks. See comment for section 1301(a)(5)(iv) above.
1301(b)(5)(ii)	Why wouldn't the entity audit this annually, like all the other items? This should be evaluated for combination with 1301(b)(4).
1301(b)(5)(iii)	This is quite a burden for a generation station with little benefit. The list would be small, and the list of systems/applications would be "all."
1301(b)(5)(v)	Quarterly is too often, but should be done at least annually. Suggested re-wording: "The responsible entity shall review user access rights periodically and at least annually to confirm access is still required.
1301(b)(6)	Authorization to place into production when? After maintenance? After modification? New devices? Define production environment? Is that "physically mounted" or "operational"? Why 48 hours? Standardize on 2 weeks. Too many frequencies (i.e. 24 hours for one thing, 48 for another, 2 weeks, quarterly, annually) is going to be very confusing and is likely to be missed. Standardize on time periods for different type of activities. Elsewhere 5 days is used to complete a change to a list identifying authorizing individuals. Suggested re-wording: "Changes to the designated approving authority shall be documented within 5 business days of the effective change. If a person's title, phone or address changes mid-year, is this required to be documented within 48 hours of the change?
1301(d)(2)	Please define performance-reset period.
1301(iv), pg 5	Request that this time period be extended to 10 business days for current employees with status change that no longer requires access to critical cyber assets, 1 business day for terminated employees.

Section	Comment for NERC
1302	There is confusion about which cyber assets are included in this section. Please clarify. This section seems to be more inclusive than that described in 1304. Why? Policy deviation documentation language is **not** left out of the standard as FAQ#4 indicates. What is the correct answer? What are the implications for dial-up language? References to section 1302.1.xxxxx in 1302 are confusing.
1302(a)(2)(i)	Are the protective relays which have dial in capability on an individual component level considered a critical cyber asset? Duke does not agree with the inclusion of individual protective relays. Please define use of the term “routable protocol.” Specifically, is this limited to transport protocols (e.g., TCP/IP, UDP, etc.) or does it include application layer protocols such as DNP 3.0 serial or vendor proprietary protocols? Are cyber assets that are only accessible via point-to-point communications included or excluded with respect to this standard?
1302(a)(2)(iii)	What is the definition of "common system" as it is used here?
1302(a)(3), pg 10	The term “officer” is used here and “official” is used other places. There is no reason to require an officer of the company to perform this role. Suggested re-wording: “This person, or his delegate (an approving authority), must authorize any deviation or exception from the requirements of this standard.” Should be able to delegate approval. Suggested re-wording: “A senior management official, or their delegate (an approving authority), shall approve the list of critical bulk electric system assets and the list of critical cyber assets.”
1302(b)	Should be labeled as “(b)” instead of “(g).” 1302 (a) is the requirements section. This is the next section.
1302(b)(4)(i)	Isn’t this timeframe a little tight? For comparison, standard nuclear policies are much longer than 30 days for updating documentation.
1302(b)(5), (i), & (ii), pg 11	Contains duplicate text, please delete duplication. The term “officer” is used here and “official” is used other places. There is no reason to require an officer of the company to perform this role.
1302(c)	Should be “(c)” instead of “(h)”
1302(d)	Should be “(d)” instead of “(i)”
1303	Administrators should have a higher level of security awareness on a particular system, but not necessarily a higher level of training or screening than an operator.
1303	Background checks are not defined by the requirements, but are defined by the measure. The measure should not be more restrictive than the requirement.
1303(4)(vi)	Requiring re-screening every 5 years is unreasonable and would have a significant administrative cost not to mention an employee relations impact. It is reasonable to perform re-screening for cause.
1303(a)(4)	Does this apply to current employees as well as new employees?
1303(b)	This should be labeled as “(b)”

Section	Comment for NERC
1303(b)(1), pg 13	Suggest that this reinforcement be done on an annual basis to reduce administrative overhead of implementing this standard. It is not clear whether the reinforcement is to be the only training (I don't think that's what is intended but it is not clear how often the training should be conducted and quarterly reinforcement is too often). How is this to be measured?
1303(b)(2)	Suggest that the training be annually with reinforcement between training cycles.
1303(b)(2)(ii)	Does this mean operators (users), administrators, or both?
1303(b)(4)(i)	What type of access? User access? There are NUMEROUS users w/ USER access to systems in a power plant. Administrative rights? This is much more manageable.
1303(b)(4)(ii)	2 business days is unreasonable for a large generation station, especially for USER access. 2 weeks would be a more manageable timeframe. This is assuming that "any substantive" means any 1 person?
1303(b)(4)(iii)	If a person is terminated, they are no longer allowed unescorted access to a generation station. Two business days is unreasonable for other changes, such as a transfer. Two weeks would be a more manageable timeframe. The "within 24 hours" should only apply to terminations or required transfer. Other changes due to normal reassignments should be longer and the 10 business day period suggested by others is reasonable. For consistency, all changes to all types of access lists should be changed within 24 hours and normal work reassignments within 10 business days. Suggested re-wording: "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, due to required transfers or terminations. Access revocation must be completed within 10 business days for any personnel who have a change in status where they are not allowed access to critical cyber assets due to normal transfer."
1303(l)	Should have been (b) - cross references between sections is messed up. Sections are labeled xxxx (a) (bb) but referenced xxxx.a.bb. Suggested change: (b) Measures
1304	What is the significance of the answer to FAQ#3? There is confusion over how this applies – see comment to section 1302 above.
1304(a)(2)	"READ ONLY" access should require less control than "USER" or "ADMINISTRATOR" access. Such read only access would be used by maintenance or engineering for troubleshooting, trending, etc. Older systems do not have this ability. For systems that are accessed only through a "client" connection, does the LAN banner displayed at logon to the LAN suffice?
1304(b)(3)	90 days is more realistic than previous timeframes.
1304, pg 17	Suggestion: please clarify that "control access" can be generic, such as access by anyone via TCP/IP port 25, and that this access control is not only meant to be access by specified users.
1305	This standard could require significant physical security upgrades and tremendous cost depending on types and numbers of facilities to which it would apply. The answer to FAQ#6 is not consistent with measures 3, 4, and 5.
1305, pg 24	Using the terms defined in the definitions, suggest that this sentence reads: "The responsible entity shall have a process for creating unauthorized incident access security incident reports."
1306	Consider deleting references for backup and recovery (section 11) from 1306 and move as applicable to 1308 "Recovery Plans."

Section	Comment for NERC
1306(2), pg 28	It is expensive and time consuming to audit all accounts quarterly. Suggest this be at most annually.
1306(5), pg 27	Annual reviews of this nature are expensive and can be dangerous if improperly done in a real-time operation environment, in fact potentially impacting the critical cyber systems themselves. Duke does not agree with this requirement.
1306(6), pg 27	Retaining all system logs for 90 days is problematic do to the significant sizes. Large amounts of storage media and/or operational costs are required. Suggest a 30 day requirement for retaining these logs.
1306(a)(1)	In many cases, there is no "controlled, non-production environment" available for existing, sometimes "legacy," equipment.
1306(a)(2) & (i)	Many "legacy" systems are not capable of modern "strong" passwords, etc. The definition of strong passwords is different between this draft and the FAQ document. The definition of strong passwords needs to be clarified.
1306(a)(2)(ii)	Management of individual passwords for a particular application is quite burdensome for a system with potentially thousands of users. Legacy systems do not necessarily incorporate domain type technology. In these cases, passwords have to be managed for each individual system. Thus, some power plants use generic passwords for some less critical applications. Does this apply to all Operating Systems?
1306(a)(5)	If the network is properly isolated (logical and/or physical), this type vulnerability assessment lends little value in an "annual" frequency.
1306(a)(8)	Legacy systems or vendor developed systems cannot support this without voiding the warranty in some cases.
1306(10), pg 28	Many SCADA systems do not have or are not going to support operating status tools. Also, in many cases bandwidth is not going to support the added network traffic and actually critical SCADA traffic may be delayed. Duke does not agree with this requirement in its current form. This is a very large burden for a stand alone system. In some cases, the notification is only a status alarm in the control room of a power plant. In some cases, introducing a monitoring function to a particular system **increases** its vulnerability – particularly to stand alone systems.
1306(a)(10)	Regarding "on a regular basis" – a "backup" of real time data (i.e. tape backup) is virtually useless in a power plant. There are a wide variety of data historian tools that are much more suited to analyzing transients, etc. Backups should only be performed prior to and after a change is made to the system – to ensure that you can return to the original state if a problem is encountered in implementing the change. Is a full system restore required for the test?
1306(a)(10) & (11)	What do these requirements mean?
1306(b)(1)	In some cases, non-production equipment is not available. "Potential security vulnerabilities"… this is very open-ended leaves a lot to local interpretation. Please clarify. In some cases, non-production equipment is not available.

Section	Comment for NERC
1306(b)(2)	Timelines are inconsistent with other requirements in the document – in this case, 5 working days and 24 hours. A quarterly audit is too often. Suggest the audit be completed at most annually. The time to complete access review for normal movement of personnel should be 10 business days. Suggested wording: "The responsible entity shall maintain a documented password policy and record of annual audit of this policy against all accounts on critical cyber assets. The documentation shall verify that all accounts comply with the password policy and that obsolete accounts are promptly disabled. Upon normal movement of personnel out of the organization, management must review access permissions within 10 working days. For terminations for cause, management (or designee) must review access permissions within no more than 24 hours." Again, legacy systems do not support password interrogation.
1306(b)(3)	A monthly review of all vendor security patches and Operating system upgrades is too frequent. "vender" should be spelled "vendor."
1306(b)(4)	Many patches require a reboot of equipment to take effect. This cannot be done on a monthly basis if the equipment is in service. Does this apply to all Operating Systems?
1306(b)(8) & (9)	Please define what is meant by "regular audit."
1307(2), pg 32-33	Suggested rewrite: (2) The responsible entity shall keep all records related to cyber security incidents for three calendar years. This includes, but is not limited to the following: (i) System and application log file entries related to the **security** incident, (ii) Video, and/or physical access records related to the **security** 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 **security** incidents and subsequent reports submitted to the ES-ISAC.
1307(6), pg 32	Again, this is an example of confusion with the use of the terms "incident" and "security incident". The term "incident" should not be used in this context. Suggest that this paragraph read: Rewrite to "(6) The responsible entity shall retain records of cyber security incidents for three calendar years."
1307(7), pg 32	Rewrite to "(7) The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."
1307(b)(5)	Should be re-numbered to (b) (1)
1307, pg 32	Per the 1300 definitions, this sentence should not include "incidents", only "security incidents", which are incidents defined as malicious or suspicious. A large number of incidents could be generated daily, the key is how many are "security incidents".
1307, pg 32	Suggest this sentence read: "The responsible entity shall develop and document a security incident response plan."
1307, pg 32	Suggest this sentence read: "The security incident response plan must address the following items:"

Section	Comment for NERC
1307, pg 32	Again, this is an example of confusion with the use of the terms “incident” and “security incident”. The term “incident” should not be used in this context. The IAW SOP is clear that “incidents” should not be reported. See http://www.esisac.com/publicdocs/IAW_SOP.pdf, page 4, section 5, which states: “Reporting is not necessary if it is considered highly probable that the cause is NOT of malicious origin, or until such time that a reportable cause is established.” Suggest that this paragraph in 1300 read: “Cyber Security Incident Reporting: The responsible entity shall report all cyber security incidents to the ESISAC in accordance with the Indications, Analysis & Warning Program (IAW) Standard Operating Procedure (SOP).”
1308	The language in the introduction "...will require a redundant or backup facility" is not included in the requirements or measures section. Clarify whether this is a requirement. Why exclude Transmission Owner and Generation owner from the requirements of this section? What does "post its recovery plan contact information" mean as is used in requirement 3?
1308(a)(1)	Annual exercise for each system is not warranted.
1308(b)(1)	To whom will the report be submitted?

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:		
Organization:		
Telephone:		
Email:		
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☒	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name: ISO-RTO Council Standards Review Committee

Lead Contact: **Karl Tammar**

Contact Organization: **NYISO**

Contact Segment: **2**

Contact Telephone: **(518) 356-6206**

Contact Email: **ktammar@nyiso.com**

Additional Member Name	Additional Member Organization	Region*	Segment*
Dale McMaster	**AESO**		**2**
Ed Riley	**CAISO**		**2**
Sam Jones	**ERCOT**		**2**
Don Tench	**IMO**		**2**
Peter Brandien	**ISO-NE**		**2**
Bill Phillips	**MISO**		**2**
Karl Tammar	**NYISO**		**2**
Bruce Balmat	**PJM**		**2**
Carl Monroe	**SPP**		**2**

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

It would be helpful to define and/or describe somewhere within the standard the industry groups, committees, and other structures frequently used and referenced.

We suggest changes to the following two definitions:

Incident: Remove the second bullet because the first bullet sufficiently covers any incident. The reference to "attempt" in the second bullet dilutes the definition and could cause excessive reporting.

Security Incident: Should read - Any malicious or suspicious activity which is known to have caused or could have resulted in an incident.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
The ISOs/RTOs have a number of regional concerns related to national, state, provincial, and local laws and requirements. These concerns will be submitted individually. Specific comments of common concern are summarized in the response to Question 3.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
General: The document could be improved through review to make each section consistent and homogeneous. Specific format inconsistencies that exist within the document are noted in the specific comments below.

We recommend that the following general statement be added as a preamble to this standard that recognizes that this standard is to be applied in a risk management context: "This standard is intended to ensure that appropriate security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed."

Please see the table below for commentes on specific portions of the standard.

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.	**Comments**
DEFINITIONS	**General:**
Cyber Assets: Those systems (including hardware, software, and data) and communication networks (including hardware, software, and data) associated with bulk electric system assets.	Identification of the compliance administration/monitor is not clear. Believed to be the RROs. This could be made clearer in the standard?
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.	Bulk Electric System Asset: For consistency, the word reliability should be used on its own and operability should be excluded. Both terms seen as the same.
Electronic Security Perimeter: The logical border surrounding the network or group of subnetworks (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.	Incident: Delete second bullet. Because the first bullet sufficiently covers any incidents. "Attempt" dilutes the definition and could cause excessive reporting.
Responsible Entity: The organization performing the reliability function, as identified in the Reliability Function table of the Standard Authorization Request for this standard.	Any malicious or suspicious activity which is known to have caused or could have resulted in an incident.
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	
(a) Requirements	
(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.	Disaster recovery plans should be specifically identified.
(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.	The use of "unauthenticated" personnel is anomalous to the rest of the document. "Unauthorized" is a better term. Even some authenticated personnel may not necessarily be authorized. The word "entity" should be "organization"
(iii) Protection Responsible entities must identify the information access limitations related to critical cyber assets based on classification level.	"as defined by the individual organizations" should be included after classification level, to read – "…classification level as defined by the individual organizations."

(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.	Where is 1.2?
(b) Measures	
(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.	5 (i) Seems to speak about critical cyber "information" but the last word refers to "assets". Should the last word in the sentence be "information"? This sentence should be made clearer.
(d) Compliance Monitoring Process	
(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.	This section should provide clarification to indicate the meaning of audit result, which we believe means compliance with the NERC 1300 standard and not other audits.

(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.	
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.	This paragraph would be clearer if it were rephrased. By commencing with the first sentence, it could be interpreted that the standard may be intending to speak to protection methods around bulk electric systems when it is only the cyber systems. If the second sentence were stated first, this would be clearer.
(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:	Replace “electric grid” with “bulk electric system” for consistency.

(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.	FORMATTING/NUMBERING ISSUE (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 i) the cyber asset uses a routable protocol, or ii) the cyber asset is dial-up accessible. B) 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.

(3) A senior management officer must approve the list of critical bulk electric system assets and the list of critical cyber assets.	The terms "senior management" and "officer" have legal meaning in companies. This should be clarified further.
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	
(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.	Using "escorted access" and "unescorted access" is better terminology than "unrestricted access" and is a better terminology to reinforce and enforce.
(l) Measures	
(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.	The ISOs/RTOs have a number of regional concerns related to national, state, provincial, and local laws and requirements. These concerns will be submitted individually.
(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.	(ii): This needs to align more closely with the previous benchmark of "24 hours" and escalate based on this bench mark.
1305 Physical Security	
(b) Measures	
(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.	"man trap" should be "Man-trap"
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	
(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.	The word 'timely' does not adequately reflect the risk management approach that should be used in applying patches.
(b) Measures	
(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.	It is not reasonable to expect a manager to sit at a terminal or otherwise review all access permissions. Management must "ensure" the review.
(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.	The company must identify in its policy a minimum retention period satisfactory to reconstruct a critical cyber asset.
(e) Levels of Noncompliance	
(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.	(i) and (ii): More clarity is required around these specific reviews.

(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.	(vii): These specific logs have not been referred to previously in this section of the standard yet we are being graded on these in compliance.
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).	Some of the reviewers were not clear on what ESISAC meant. Should be spelled out.
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	This introduction is repetitive and redundant. It could be shortened to one paragraph and still be effective.

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.	(3): "Post" is misleading and suggests posting to a web site or similar. It should be modified to reflect its real nature, which we feel is publishing to documents that a team would use in a crisis.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Robert Klumpp / Allan Berman	
Organization:	Long Island Power Authority	
Telephone:	(516) 545-4095 / (516) 545-5570	
Email:	rklumpp@keyspanenergy.com / aberman@keyspanenergy.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☒ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Reference attached Word document.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
Reference attached Word document.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
Reference attached Word document.

Long Island Power Authority
Comments On NERC Standard 1300 – Cyber Security
11/1/04

General Comments on the document

Throughout the document, references are made to other subsections that are not readily found. For example, lower case letters, numbers and roman numerals are used for bullets but then are not used for references. Additionally, bullets in a number of sections are mislabeled or are out of alphabetic order.

Definitions:
Critical Cyber Assets:
Comment: Is this meant to include off-site, stand-alone emergency systems such as an Alternate Control Center?

Incident:
Comment: Suggest modifying the definition of "Incident" as follows because the proposed definition is too broad.
"Incident: Any physical or cyber event that:

- disrupts the functional operation of a critical cyber asset
- compromises the electronic or physical security perimeters."

1301 Security Management Controls:
(a) Requirements
(2) Information Protection
(ii) Classification
Comment: Suggest changing paragraph to say "The responsible entity shall classify information related to critical cyber assets to aid personnel with access to this information in determining which and how information can be disclosed without jeopardizing its physical or cyber security. The relative sensitivity of information that should not be disclosed outside of the entity without proper authorization should be identified as well.

(a) Requirements
(3) Roles and Responsibilities
Comment: Where is Section 1.2 that is referenced in the following sentence? "Roles and responsibilities shall also be defined for the access, use, and handling of critical information as identified in section 1.2."

(a) Requirements
(5) Access Authorization
(iv) Access Revocation / Changes
Comment: Suggest that modifications, suspensions, and terminations of user access be authorized, implemented, and documented in 24 hours only if a user is terminated for disciplinary action. In other cases, suggest that up to 5 business days be permitted. This requirement should also be listed as a measure in section (b).

(b) Measures
(3) Roles and Responsibilities
(ii)
Comment: Suggest changing "… shall be identified by name, title, phone, address, and date of designation" to "…shall be identified by name, title, business phone, business address, and date of designation."

(b) Measures
(5) Access Authorization
(iii)
Comment: Suggest changing "… shall identify each designated person by name, title, phone, address, and date of designation" to "…shall be identified by name, title, business phone, business address, and date of designation."

(b) Measures
(6) Authorization to Place Into production
Comment: Suggest modifying "… shall be documented within 48 hours of the effective change" to "… shall be documented within 2 business days of the effective change".

(d) Compliance Monitoring Process
(3)
(iv)
Comment: This section states that audit results for the information security protection program should be made available to the compliance monitor upon request. The standard requires periodic reviews of security access and various policies and procedures but does not state that formal audits be performed. Please clearly state this requirement and detail what audits should be performed.

(d) Compliance Monitoring Process
(3)
(v)
Comment: Suggest changing "The list of approving authorities for critical cyber information assets." to "The list of individuals authorized to disclose information related to critical cyber assets."

1302 Critical Cyber Assets
General Comments:
Lettering of bullets must be corrected. Remove sub-bullets for sections with single requirements.

Regarding the identification, documentation and use of Critical Bulk Electric System Assets to identify Critical Cyber Assets

Entities adhering to this standard should have the responsibility and flexibility of identifying critical cyber assets without tracking the critical bulk electric system assets. If the intention of the standard is to strengthen cyber security, the focus should be guided in that direction.

Introduction
Comment: Suggest changing the last sentence to read "This standard requires that entities identify and protect critical cyber assets that support the reliable operation of the bulk electric system."

(a) Requirements
(2) Critical Cyber Assets
Comment: Isn't this description different than what's presented in the "Definitions" section of the document? If so, why?

(i) Compliance Monitoring Process
(2)
Comment: Are we to understand from this bullet that we will be audited annually to confirm compliance? Why is data kept for three calendar years, but audit records for three years? The use of the word "calendar" in some time-based requirements and not in others may lead to confusion. Was this intentional? Otherwise, please correct for consistency.

1303 Personnel & Training
General Comment: Lettering of bullets must be corrected.

(l) Measures
(2) Training
Comment: The *Awareness* section details periodic reinforcement of security requirements. However, the *Training* section does not detail any timeframes. Suggest that timeframes be associated with training.

(l) Measures
(4) Background Screening
(ii)
Comment: What constitutes "substantive change of personnel"?

Comment: This section states that the list of personnel with access to critical cyber assets etc… will be updated within two business days of any substantive change of personnel. However, Section 1301 (b)(5)(i) requires that the list of individuals that authorize access to critical cyber information be updated within five days. These sections seem to

contradict each other with respect to coordinating changes in personnel access and authorization.

(l) Measures
(4) Background Screening
(iii)
Comment: Suggest requiring that changes be made within 24 hours only for personnel who have had their access changed because of disciplinary action.

1304 Electronic Security
(a) Requirements
(1) Electronic Access Controls
Comment: Please clarify what is meant by the following statement. "Electronic access control devices shall display an appropriate use banner upon interactive access attempts."

1305 Physical Security

Introduction
1st bullet
Comment: Please clarify what is meant by " … an in-depth defense strategy to protect the physical perimeter …".

(b) Measures
(4)
Comment: Does this mean that access points with physical access controls (i.e. card key control) also need "CCTV" or "Alarm Systems"?

Comment: Under Alarm Systems, "These alarms must report back to a central security monitoring station or to an EMS dispatcher." Please define an EMS dispatcher.

(b) Measures
(5)
Comment: Must all escorted visitors be logged in one of these manners as part of this standard?

(b) Measures
(6)
Comment: Suggest changing the following sentence from:
"The responsible entity shall maintain documentation of annual maintenance and testing for a period of one year."
to
"The responsible entity shall perform and document maintenance and testing on physical security systems annually. This documentation shall be maintained for a period of one year."

(e) Levels of Noncompliance
(1) Level One
(ii)
How do you expect to determine and/or quantify gaps in access records for manual logs?

1306 Systems Security Mangement

(a) Requirements
(2) Account and Password Management
(ii) Generic Account Management
Comment: "Where technically supported, individual accounts must be used (in contrast to a group account)". Is this necessary in a Control Room that is staffed on a 24x7 basis?

(a) Requirements
(2) Account and Password Management
(iv) Acceptable Use
Comment: Suggest changing "… the audit of all account usage to and individually named person.." to "...the audit of all account usage to an individually named person.."

Comment: Please clarify what is meant by "personal registration"?

(a) Requirements
(6) Retention of Systems Logs
Comment: Please clarify what is meant by "… security related system events".

(a) Requirements
(8) Disabling Unused Network Ports/Services
Comment: What is meant by term inherent?

(a) Requirements
(9) Dial-up modems
Comment: Is a written policy for following a manual process (i.e. temporarily connecting a normally disconnected modem for maintenance / troubleshooting purposes) an acceptable form of a "secure dial-up modem connection"? If not, what constitutes a secure dial-up connection?

(a) Requirements
(10) Operating Status Monitoring Tools
Comment: Might this be considered more of a performance / reliability issue rather than a security issue?

(a) Requirements
(11) Back-up and Recovery
Comment: The standard states that "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." This appears to be unrelated to Cyber Security. "Archival data" can be interpreted as long-term "historic" data and not backups of critical cyber assets. In this context, what would be the purpose of restoring archival data annually?

(b) Measures
(1) Test procedures
Comment: How can testing of potential security vulnerabilities be quantified?

(b) Measures
(4) Integrity Software
Comment: Suggest that the following sentence be reworded for clarity. “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.”

(b) Measures
(5) Identification of Vulnerabilities and Responses
Comment: This first sentence of this section seems to require that personnel who maintain critical cyber assets have extensive knowledge in technology and techniques for identifying vulnerabilities including the tools and procedures that can identify them. Please clarify this requirement.

(b) Measures
(8) Disabling Unused Network Services/Ports
Comment: Re-label this section to read “Disabling Unused Network Ports/Services” to match section (a)(8).

Comment: While some organizations may have the in-house expertise to execute this requirement, others may rely upon vendor support in order to avoid disabling required ports and/or services and impacting their on-line production system. Additionally, a vendor’s security solution may be implemented without passing on details to the customer. While unfortunate, the vendor may do this for competitive business reasons. In such a case, accurate configuration documentation would be difficult to maintain.

(b) Measures
(9) Dial-up Modems
Comment: What is meant by “appropriate actions” in the following sentence? “The documentation shall verify that the responsible entity has taken the appropriate actions to secure dial-up access to all critical cyber assets.”

(b) Measures
(10) Operating Status Monitoring Tools
Refer to comments on section (a)(10).

(b) Measures
(11) Back-up and Recovery
Refer to comments on section (a)(11).

1307 Incident Response Planning

Comment: Would an EMS going down due to hardware/software problems and not necessarily a cyber security issue be considered a reportable incident?

1308 Recovery Plans

1st paragraph

Comment: What is meant by "triggering events" in the following sentence? "Recovery plans must address triggering events of varying duration and severity using established business continuity and disaster recovery techniques and practices". Suggest that it is not a good practice to "force" operations to relocate to an Alternate Control Center based on time but rather based on the unique circumstances. For instance, sometimes recovery time is pretty much known and it would be best not to relocate strictly because a time limit is reached. Other times, recovery time can not be estimated in which case it most likely is best to relocate after a certain period of time.

Comment: Suggest removing the following sentence:
"There is not requirement for recovery plans for substations and generation plants that have no critical cyber assets."

(a) Requirements

(2)

Comment: Same as comment for 1st paragraph of 1308.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Kurt Muehlbauer	
Organization:	Exelon Corporation	
Telephone:	312.394.3772	
Email:	kurt.muehlbauer@exeloncorp.com	
NERC Region		**Registered Ballot Body Segment**
☒ **ERCOT** ☐ **ECAR** ☐ **FRCC** ☒ **MAAC** ☒ **MAIN** ☐ **MAPP** ☒ **NPCC** ☒ **SERC** ☒ **SPP** ☐ **WECC** ☐ **NA - Not Applicable**	☒ ☐ ☒ ☐ ☒ ☒ ☐ ☐ ☐	1 - Transmission Owners 2 - RTOs, ISOs, Regional Reliability Councils 3 - Load-serving Entities 4 - Transmission-dependent Utilities 5 - Electric Generators 6 - Electricity Brokers, Aggregators, and Marketers 7 - Large Electricity End Users 8 - Small Electricity End Users 9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☒ Yes

☐ No

Comments

Exelon fully supports the protection of critical cyber assets that impact the reliability of the bulk electric system operation. Exelon respectfully submits the following comments to seek clarification on the draft standard and for consideration in the final standard.

Cyber Assets

The association of Cyber Assets to the Bulk Electric System should occur in the definition of Critical Cyber Assets. Exelon recommends that this definition be changed to: Systems and communication networks, including hardware, software, and data.

Security Incident

Section 1307 references the term cyber security incident. Exelon requests that the drafting team formally define the term cyber security incident or change the term being defined from security incident to cyber security incident.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
Exelon fully supports the protection of critical cyber assets that impact the reliability of the bulk electric system operation. Exelon respectfully submits the following comments to seek clarification on the draft standard and for consideration in the final standard.

Exelon does not believe the standard is ready for ballot until the following comments are addressed. If these comments are addressed, Exelon intends to support that the standard go to ballot.

1301 Security Management Controls

1301.b.1.iii
Please explain how deviations and exemptions impact levels of noncompliance

1301.a.5.iv
This section requires termination of user access to critical cyber assets to be accomplished within 24 hours of a change in user status. We agree that access must be updated within 24 hours for cases where a person loses his/her access rights due to cause. The NRC allows three days for a favorable termination and this standard should not be more demanding than the highly regulated nuclear industry. We believe that routine administrative status changes should be managed within six business days.

1301.b.5.i
This section states that the list of designated personnel must be updated within five days. This timeframe is unclear and we recommend changing five days to five business days.

1302 Critical Cyber Assets

There are unmatched references to 1302.1.2.1, 1302.1.1, 1302.1.2, 1302.2.1, 1302.2.2, and 1302.2.3.

Section numbering is incorrect starting with Measures.

1302.a.3
Responsibility for critical bulk electric system assets and critical cyber assets is likely to be shared between multiple business units. We recommend that this requirement read: At least one senior management official…

1302.a.2.i.A
For emphasis, we recommend underlining and.

1302.g.1.i

For clarity, we recommend that the sentence read: The responsible entity shall maintain its approved list of critical bulk electric systems assets as identified under…

1303 Personnel & Training

Section numbering is incorrect starting with Measures.

1303.a.4
This sentence reads: …unrestricted access to critical assets. We recommend that the sentence read: …unrestricted access to critical cyber assets.

Please define the term unrestricted access

1303.l.4.iii
This section requires access revocations within 24 hours of a change in status. We agree that access must be updated within 24 hours for cases where a person loses his/her access rights due to cause. The NRC allows three days for a favorable termination and this standard should not be more demanding than the highly regulated nuclear industry. We believe that routine administrative status changes should be managed within six business days.

The scope of access revocation is not clear. We recommend that the sentence begin: Physical and electronic access revocation…

1303.l.4.iv
1303.a.4 requires that personnel shall be subject to background screening prior to being granted unrestricted access to critical [cyber] assets. We recommend that the first sentence of 1303.l.4.iv read: The responsible entity shall conduct background screening of all personnel prior to being granted unrestricted access…

1303.l.4.vi
This section requires that background screening be conducted at least every five years, or for cause. Since employees of the responsible entity are under constant observation by management personnel and performance is reviewed on an on-going basis, we believe that it is not necessary to renew the background investigation for employees.

1304 Electronic Security

There are unmatched references to 1304.2.1, 1304.2.2, and 1304.2.3.

1304.b.1
The last sentence requires that the Electronic Security Perimeter document shall verify that all critical cyber assets are within the electronic security perimeter. The definition of a critical cyber asset includes software and data. If depicting software and data on a schematic is beyond the intent of the requirement, we recommend that the last sentence read: The document or set of documents shall verify that all critical cyber asset hardware is within the electronic security perimeter(s)

1305 Physical Security

1305.b.3

The term security cage is too restrictive and leaves little room for alternatives. We recommend that security cage be changed to internal perimeter and use security cage as an example.

1305.b.3
In the paragraph following the table, the term de-authorization is used. To be consistent with other sections of this standard, we recommend changing de-authorization to revocation.

1306 Systems Management

1306.a.2.iii
This access review requirement appears to be redundant with 1301.a.5.iii and 1303.l.4.iii. We recommend that the access control requirements should only appear in one section of the standard.

1306.b.2
We recommend that the access permission review occur within 24 hours for not only involuntary terminations, but also for suspensions.

1306.a.6
This section begins: All critical cyber security assets… We recommend that the sentence read: All critical cyber assets…

This section requires that the critical cyber asset must generate an audit trail for ALL security related system events. Audit capabilities will vary by system. Enabling full security audit functionality can generate a tremendous volume of events that have minimal or no value, can significantly impact system performance, and can greatly increase storage capacity requirements. We recommend that the responsible entity define requirements for security events that must be generated and to implement system auditing based on those requirements to the extent supported by the system.

1306.a.8
The use of the term inherent services is not clear. We recommend that the sentence read: The responsible entity shall disable unused services.

1306.b.2
The access review measurement is not consistent with 1301.a.5.iv. The measurement in 1306 is clearer and more complete that the one in 1301.

1306.b.10 and 1306.b.11
We recommend that these sections read: …shall maintain documentation…

1306.e.3.iii.B
Unmatched reference to 5.3.3.2

1307

The numbering under section (b) starts with (5) instead of (1).

1307.b.6
Records should be retained for cyber security incidents only. We recommend that the sentence read: The responsible entity shall retain all records related to cyber security incidents for three calendar years.

1307.c.2
Records should be retained for cyber security incidents only. We recommend that the sentence read: The responsible entity shall retain all records related to cyber security incidents for three calendar years.

1308

1308.d.3
Unmatched references to 1308.2.1 and 1308.2.4

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Richard Engelbrecht	
Organization:	Rochester Gas and Electric	
Telephone:	585 771 2267	
Email:	richard_engelbrecht@rge.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☒ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

RGE concurs with the following NPCC comment:

NPCC's participating members recommend that the definition of Critical Cyber Assets be;

"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).

NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.

NPCC's participating members recommend changing the Incident definition from

"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."

to

"Incident: Any physical or cyber event that:

disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
1. In general, there are too many areas which require interpretations which are defined or included in the FAQ's. Since the FAQ's would not be part of the approval these interpretations need to somehow be included within the standard.
2. An alternative to developing a definiton of Bulk Electric System would be to require the Reliabity Authority for each Control Area to identify the Bulk Electric System for its respective Control Area. The next step would be for each Responsible Entity to identify the Bulk Electric System Asset they are responsible for in that system, identify the critical operating system functions and tasks and then identify the Critical Cyber Assets.
3. This standard is not consistent in the level of detail for each area being adddressed. Also there is no process indicated for change to be made following approval. A different approach to consider would be to make the standard identifying roles and responsiblities; identification of what is required to be included within the standard and its objective; and the process for review and sanctions. A description of minimum level for each area or standard should be attached as a guideline. In that manner the Standards can be permanent and only adjust the attachment if warranted. The way the standards read now, they must be adhered to unless the responsible individual in the company grants an exemption or deviation. A standard should be a standard with no deviation. Minimum guidelines would be a more practical approach. A deviation or excemption to a guideline is a more pragmatic approach.

RGE also concurs with the following NPCC comments:

NPCC's participating members recommend that the definition of Critical Cyber Assets be;
"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).
NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.
NPCC's participating members recommend changing the Incident definition from

"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."
to

"Incident: Any physical or cyber event that:
disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
Correct references as covered in question 2.

Request clarification on what "information" is protected in 1301.a.2.

Change 1301.a.2 from;

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

to

"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets." (NPCC's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)

Change 1301.a.2.i from;

"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."

to

"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well." (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)

Change 1301.a.3 from;

"….entity's implementation of…"

to

"…entity's implementation and adherence of…"(NPCC's participating members believe it is important to stress that not only is it important to implement this Standard but to adhere to it as well.

The “24 hours” in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.

Change 1301.a.5.iv from;

"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."

to

"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven calendar days for all other users of a change in user access status. All access revocations/changes must be authorized and documented." (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)

change 1301.b.5.i from;

"5 days"

to

"7 calendar days" (NPCC's participating members believe that the 5 days may be not be sufficient time especially when considering holiday seasons)

1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency in the reference for retention of audit records.

1301.d.3.iv, request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor

1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii to ensure the protection of the identity/personal information of the affected individuals

Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor

1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.

1301.e.2.iii, change from;

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

to

"An authorizing authority has been designated but a formal process does not exist to

test, validate and deploy systems into production, or" (NPCC believes it was the drafting team's itent to deploy the system rather than promote which has a different connotation associated with it,)

Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change "Executive Management" to "Senior Management" for consistency and clarity.

1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).

NPCC Participating Members believe that the concept of the Bulk Electric System and association "definitions" may not be appropriate to capture the intent of the standard. NPCC suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.

Replace the 1302 preamble and 1302.a.1 and 1302.a.2 as shown below, with;

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 which support the reliable operation of the bulk electric system.

The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.

(a) Requirements
Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.

(1) Critical Bulk Electric System Operating Functions and Tasks

The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:

- monitoring and control
- load and frequency control
- emergency actions
- contingency analysis
- arming of special protection systems
- power plant control
- substation control
- real-time information exchange

(2) Critical Cyber Assets

(i) In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:

A) The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.

B) The consequences of the Operating Function or Task being compromised (i.e. "highjacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.

C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.

D) Known risks associated with particular technologies

Change 1302.g.1 from;

"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."

to

"1 Critical Bulk Electric System Operating Functions and Tasks
(i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."

Change 1302.g.2.i from;

"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."

to

"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure." (NPCC believes the use of the word additional is of no value as used here and recommends removal).

Change 1302.g.5 from;

"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"

to

"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval" (NPCC believes that it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations of operations is lost.)

Change 1302.g.5.i from;

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

to

"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."

Change 1302;
"critical bulk electric system assets"

to

"critical bulk electric system operating functions and tasks"

1303, NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for the NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk.

The FAQ describes supervised access, 1303 does not touch upon this topic.

Change 1303.a.4 from "unrestricted access" to "authorized access".

Change 1303.a.4 title to "Personnel Risk Assessment."

Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."

Change 1303.a.2 from;

"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."

to

"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"

1303.a.4 from;

"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."

to

"Personnel Risk Assessment: There must be a documented company personnel risk assessment process."

Add to 1303 Measures.2, a training measures for disaster recovery (1308) and incident response planning (1307).

The numbering of 1303 starting with Measures needs correction.

1303 Measures 4.i, request clarification. Does this include third party personnel?

Change 1303.Measures.4.i from;

"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)."

to

"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 respective security perimeter(s)." (NPCC believes there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)

Change 1303.Measures.4.ii from;

"two business days"

to

"seven calendar days", per earlier comments and to keep consistent with FERC Order.

1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days", per earlier comments

1303.Measure.4., remove;

Subsections iv, v and vi.

and replace with

"There must be a documented company personnel risk assessment process." NPCC's participating members feel these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities."

1303.Compliance Monitoring Process.2, NPCC's participating members do not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria
is not applied, or" to "Personnel risk assement program is practiced, but not properly documented, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."

Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii

From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.

Change 1304 a.2 Electronic Access Controls:
to

"The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" 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)."

Change 1304 a.3 Monitoring Electronic Access Control:
to
"The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."

Change 1304 a.4 from;

"The responsible entity shall ensure that all documentation reflect current configurations and processes."

to

The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.

1304.a.4 Remove -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. (This is a measure and should be removed here)

Compliance Monitoring Process;
Change 1304.d.3 from;

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

to

"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"

Level of non compliance
"Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.

1305 Physical Security;

Eliminate the bulleted items in the Preamble to Section 1305-they appear in the Requirement section.

Replace 1305 a.1 with;
"Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.
• The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),

• The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and
• The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."

Change the following - (a) Requirements;
"(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."

to

"(3) Physical Access Controls: The responsible entity shall implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.
(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.
(5) (We recommend deleting this bullet as the intent is captured in bullet "4").
(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."

Change Measures;

"(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."

to

"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility." (NPCC believes the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)

In 1306.a.1, last paragraph, modify the second sentence to read as follows;

"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."

1306.a.2.ii change "pooding" and "puffing" to "putting" (it appears a pdf translation problem as some documents the group printed have it and others did not)

1306.a.2.ii remove "Generic" from the title

1306.a.2.iii, use "at least annually" instead of "at least semi-annually"

Change 1306.a.3 from;
"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."

to

"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets." (NPCC believes that it upgrades are a subset of the applicable security patches.)

Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."

Change 1306.a.4 from;

"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."

to

"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."

1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).

Change 1306.a.6 from

"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."

to

"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three calendar years in an exportable format, for possible use in further event analysis."

1306.a.7 Remove "Configuration Management" from the title

1303.a.8 Remove the word "inherent" it is not clear what is meant by it.

1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.

1306, remove 1306.a.11 since 1308 addresses back-up and recovery.

1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.

1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days".

1306.b.3, remove;

"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."

and change

"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."

to

"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."

1306 b.3 first sentence-eliminate the word "management".

1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.

1306.b.4 third sentence Change
"..so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."

to

"..mitigate risk of malicious software".

1306.b.4 Remove the second sentence.

1306.b.4 Replace the fourth sentence with;

"Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."

1306.b.5 remove the first sentence.
Based on the common use of third parties for outsourcing of this associated work of vulnerabilty assessment, it is not reasonable to maintain the information called for in sentence one.

Change 1306.b.6 from;

"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."

to

"Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis."

1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"

Remove 1306.b.11, since 1306.a.11 was removed.

1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."

1306.d.3.iii, change "system log files" to "audit trails"

1306.e.2, change "the monthly/quarterly reviews" to "the reviews"

1306.e.2.ii.C, change "anti-virus" to "malicious"

1306, the Compliance levels should be updated to match the above measures.

1307, spell out and provide clarification on the acronyms throughout.

Change 1307, from;

"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."

to

"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."

1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;

"Incident and Cyber Security Incident Reporting"

to

"Security Incident Reporting".

and also Change from;

"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

to

"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

Refer to our definition of a "security incident", change 1307.b.5 from;

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

to

"The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements."

Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."

to

"The responsible entity shall retain records of security incidents for three calendar years."

Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."

to

"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."

1307.d.1 there is a 90 day reference that does not appear in the measures.

In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.

Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	William J. Smith	
Organization:	Allegheny Energy	
Telephone:	(724) 838-6552	
Email:	wsmith1@alleghenypower.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT	☒	1 - Transmission Owners
☒ ECAR	☐	2 - RTOs, ISOs, Regional Reliability Councils
☐ FRCC	☒	3 - Load-serving Entities
☐ MAAC	☐	4 - Transmission-dependent Utilities
☐ MAIN	☒	5 - Electric Generators
☐ MAPP	☒	6 - Electricity Brokers, Aggregators, and Marketers
☐ NPCC	☐	7 - Large Electricity End Users
☐ SERC	☐	8 - Small Electricity End Users
☐ SPP	☐	9 - Federal, State, Provincial Regulatory or other Government Entities
☐ WECC		
☐ NA - Not Applicable		

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Cyber Asset - The definition does not specify computer assets, which could be interpreted to include non-cyber assets such as motor control centers or physical switches that could be defined as hardware.
Critical Cyber Assets - The definition should be standardized with other NERC documents and within the document itself. The criteria for identifying critical cyber assets (Section 1302.a.2) should be part of the definition.
Physical Security Perimeter - Reword the definition to address networks that are not confined to a specific area or room, such as power station control networks that may exist throughout a power station and connect to devices directly on the plant floor and not in a room.
Incident and Security Incident should be combined into one definition that addresses secirity incidents only. Wording such as "could have lead to a disruption" and "could have resulted in" should be revised to read "disrupts, or could have directly resulted in a disruption" and "could have directly resulted in" respectively.
Also, the Security Incident definition should be specific enough to insure activities such as "denied access" card reads are not condidered a suspicious activity.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
The most significant concern is that this standard does not appropriately address the diverse environments of centralized power control centers, power stations and tranmission substations. Implied in the statndard is an enviroment similar to that of a central power control center. The physical, computing, and user environments are very different in each of these types of facilities. Revise the standard to accommodate the enviroments for each of these.
Specific to power stations and substations, a separate physical perimeter for critical cyber assets may be difficult to reliably and completely achieve in all cases, while at the same time not providing additional benefit. Control rooms are a good example of this because a power station provides much easier sabotage targets once an individual is inside the plant. Revising the standard to require only a protected elecronic perimeter and a physically protected perimeter where appropriate and beneficial for these diverse environments is appropriate.
Revise the standard to separate logical user access requirements into 2 categories: 1) accessing assets form outside the protected electronic perimeter, and 2) accessing assets from inside the protected electronic perimeter. Revise the standard to make provisions for user access points (operator console) inside the electronic perimeter that must always be available for use and cannot be password protected.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
See attached Word document that includes Section Specific Comments.

NERC Standard 1300 – Cyber Security
Section Specific Comments
From
Allegheny Energy

1. 1301- Security Management Controls

   Section (a)(2) - This section indicates that the design information for a "critical cyber asset" should be protected – in order to prevent someone from gaining critical information that may allow a system compromise. This may include a lot of power station and substation engineering material that is currently open to access by power station, substation, and central services personnel. This data may also be in the hands of the vendors that supplied the system. Revise the standard to indicate that as long as the electronic security perimeters of a critical cyber asset are sufficiently protected, that exclusions are then permitted pertaining to the protection of power station design information.

   Section (a)(2)(i)/(ii)/(iii) – preface the first reference to "information" with "relevant" in each paragraph.

   Section (a)(3) – The second paragraph should be reworded to "The responsible entity should define roles and responsibilities associated with the management of critical cyber assets". The concept of "custodians" should be removed.

   Section (A)(4) – The governance section is unnecessary and should be removed since the cyber security policy in section 1301 requires that senior management acknowledge responsibility for cyber security.

   Section (a)(6) – Reword the paragraph to state "The responsible entity shall institute and document a process for the testing and assessment of new or replacement systems and software patches/changes". The answer to FAQ 9 confuses the "approving authority" role and does not recognize that companies may have different roles for a system owner.

2. 1302 – Critical Cyber Assets

   The answer to FAQ 6 states that Critical Cyber Assets with dial-up access, which do not use a routable protocol, do not require the physical security perimeter requirements for critical cyber assets. Allegheny Energy believes that a routable protocol can also be secured in a sufficient manner to provide secure remote access. Therefore, Critical Cyber Assets located in substations with a sufficient local electronic security perimeter should not require the physical security perimeter requirements of critical cyber assets. Additionally, those attempting to compromise the physical security perimeter surrounding a critical cyber asset

located within a substation would most likely have the ability to compromise the Critical Bulk Electric System Assets associated with the critical cyber asset first. The NERC guideline titled “Physical Security – Substations” addresses substation security in sufficient detail.

(a) Clarification is required on the selection of critical assets. The requirements begins by stating “that responsible entities shall identify their critical bulk electric system assets using their preferred risk-based assessment”, then defines the bulk electric systems assets (differently than under the definitions), and then lists the bulk electric system assets.

Does the listed bulk electric system assets serve as an overall view of “possible” bulk electric systems assets with each company able to subtract from this list based on their own risk-based assessment?

(a)(2)(i)(A) Reword to “the cyber asset will cause an interruption or allow control of a critical bulk electric system asset, and”

B) Reword to “the cyber asset uses a routable protocol for remote communications, or”

D) Add “not” in between the words “do” and “use”. Also, this item would be better suited in Section 1305 – Physical Security and not in the definition section.

3. 1303 – Personnel & Training

Personnel having access to critical cyber assets should not be required to have a higher level of screening than other employees, as long as screening performed for all employees is at a sufficient level for those with access to critical cyber assets.

If contractors and vendors are included in the standard, they should specifically be mentioned as part of “personnel”.

Also, generating stations operations do not generally allow for background screening for ALL personnel, especially contractors, accessing critical cyber access areas, such as control rooms. Since generating station personnel typically staff this area, background screening should not be required.

4. 1304 – Electronic Security

Clarification is needed in this section as to whether it applies to just access to the security perimeter, such as through a firewall, or whether it also includes all human and electronic access such as user consoles.

1304 bullet 1,2 - “All access points” should be “all electronic perimeter access points”.

1304(b)(2) - The second sentence is confusing and should be broken into bullets or other clear separation of the documentation requirements.

1304(a)(1) - "Communications links connecting discrete electronic perimeters are not..." These should be considered as separate critical cyber assets if the data can be intercepted and modified in such a way to cause disturbances. Should encryption and access protection of such connecting data streams be addressed by this standard?

5. 1305 Physical Security

Critical Cyber Assets located **in** substations and generating stations with a sufficient local electronic security perimeter should not require the physical security perimeter requirements of critical cyber assets. (Refer to comments under Question 2.)

Also, anyone with direct physical access to the critical cyber assets in either instance can easily manually control the transmission and generating bulk electric assets.

The NERC Security Guideline concerning Substation Physical Security and typical generating physical security provides the guidance and protection required for these assets.

Do all remote workstations that access a dial-up enabled critical cyber asset automatically become critical assets themselves?

1305(b)(4) - The last two sentences are confusing as to what is being asked for. Not sure what "verify access records for authorized access against access control rights" means as well as "shall have a process for creating unauthorized incident access reports"?

6. 1306 Systems Security Management

Generally, this section is onerous and does not account for the many differences in electronic systems. Rewriting the section as recommended by the EEI Security Committee would provide the flexibility for the various legacy systems that do not lend themselves for many of the mandated controls.

Specific concerns include:

1306(a)(1) - Test procedures should also apply to devices that manage the Critical Cyber Asset Electronic perimeter (firewalls).

1306(b)(4) - The last sentence is a fragment and confusing.

1306(b)(10) - Remove the “a” between maintain and documentation

1306(e)(3)(iii)(B)(3) - Quarterly Audits – Where are the quarterly audits mandated?

.
1306(a)(2)(ii) - Where generic accounts (a single account used by many people) are used, the “scope” (type and locations of access, user rights of these accounts) of these accounts should be as small as possible to minimize the potential access “footprint”. Where generic accounts are used outside the electronic security perimeter to access data from a Critical Cyber Asset, only limited read only access should be allowed. Revise the standard to allow these types of generic accounts.

1306(a)(3) - Installations of patches on control system computers may require a plant outage before this can be done without potentially disrupting plant operation. The word “timely” in this section infers that the patches are to be installed as soon as possible. Revise the standard to be clearer that the patches are to be installed as directed by formal security patch management practice.

Also, does this apply to all levels of patches for all operating systems and applications?

1306(a)(4) - Some real-time software does not work correctly along with virus software. In such cases, manufactures of such software should be encouraged to document incompatibilities. Revise to standard to allow for this exclusion.

1306(a)(5) - Hiring a 3rd party to do intrusion testing can be vulnerability in itself. Revise the standard to exclude penetration testing as a diagnostic review.

1306(a)(7) - Can more detail be provided on what is meant by audit trails for all security related system events?

1306(a)(11) - For Power Stations, it should be sufficient to store backups onsite in a safe location. (A safe location would be a secure location, protected from fire, explosion, electromagnetic, and chemical hazards.). Revise the standard to indicate this.

1306(b)(2):
1. In this and other places, access permissions are to be reviewed and revised within 24 hours. Recommend that only “for cause” terminations adhere to the 24-

hour time frame. Normal access permission revisions due to retirement, transfer, etc. should be completed within five business days.

2. Is the review within 5 days meant to also include action taken in 5 days?

1307 Incident Response Planning

Allegheny Energy agrees with EEI that the definitions for Incident and Security Incident should be combined to reflect only Security Incidents. (Also refer to Definitions comments above.)

1307(d)(3)(ii) – Is there an assumption that all companies will have reportable cyber security incidents? Change wording to "Verified cyber security incidents have not been adequately documented and reported to the ESISAC."

1308 Recovery Plans

1308.paragraph 3: This paragraph belongs in the FAQ instead of the standard and should be removed, rewritten and clarified.

1308.paragraph 3: The first sentence of this section potentially contradicts the last sentence. In a power station, indeed a severe enough problem will lead to reconstruction of more than just the cyber assets. This paragraph should be more specific on what is required. Power station cyber assets should have sufficient plans to recover from system loss due to equipment failure, malfunction, or other failure. Plans for reconstruction because of catastrophic plant failure should not be required since more complete redesign and reconstruction of the entire plant may be required that cannot be planted for. Revise the standard to indicate this.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:		
Organization:		
Telephone:		
Email:		
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT** ☐ **ECAR** ☐ **FRCC** ☐ **MAAC** ☐ **MAIN** ☐ **MAPP** ☐ **NPCC** ☐ **SERC** ☐ **SPP** ☐ **WECC** ☐ **NA - Not Applicable**	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name: EEI Security Committee

Lead Contact: **L.W. Brown**

Contact Organization: **Edison Electric Institute**

Contact Segment:

Contact Telephone: **202/508-5618**

Contact Email: **LwBrown@EEI.org**

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

SEE ATTACHED GENERAL & SPECIFIC COMMENTS…

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
SEE ATTACHED GENERAL & SPECIFIC COMMENTS…

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
SEE ATTACHED GENERAL & SPECIFIC COMMENTS…

"ATTACHED EEI SECURITY COMMITTEE
GENERAL and SPECIFIC COMMENTS"
(as referenced in the file:
"Standard 1300 Comment Form from EEI")

Comments of the Edison Electric Security Committee on Proposed Draft NERC Standard 1300, Cyber Security | **November 1, 2004**

Background

We appreciate the hard work, expertise, integrity, and cooperation reflected in this proposal. Much good progress has been made beyond the original Emergency Action Standard 1200 language. As with any document created by committee, however, there nonetheless remain items that require further clarification and development before the Standard is ready for submittal to voting. Therefore, we hope you consider the below comments as being proffered with constructive intent.

These comments and suggestions were developed based on four hours of discussion during two conference calls among EEI member-company security and IT staff, and including the participation of some members of the Standard 1300 Drafting Team, to discuss the intent, implications, application, and impacts of the proposed language, and include some specific suggestions drafted and provided by participants of the calls. They reflect a consensus among those discussion participants. You will, as a result, see many of these comments mirrored in most (though certainly not all) individual company comments, and those individual comments are likely to raise additional issues and concerns.

Committee Comments and Suggestions

One overarching point of great importance: If not within this standard, NERC standards in general (or at least the official, published criteria for auditing and enforcement) must have an appropriate "exceptions" policy. There will always be situations when "strict compliance" is in fact **not** the optimal approach for a utility or other responsible entity to follow.

The FAQs need to be "cleaned up" and made completely consistent with the standard. Some of the more obvious specific inconsistencies or other problems will be pointed out in the comments below.

Numbering/formatting needs to be made consistent, and also needs to be checked and "cleaned up" for consistency and readability.

Definitions

Even if terms are not defined in this section, they need to be used with greater consistency, including the use of only one term to represent one concept. For example: are there intentional differences among "key staff," "employee," and "personnel"? If so, why, and what are those differences?

"Critical Cyber Assets" –

Use the CIPC-approved definition – using a different one creates confusion (not to mention wasteful duplication of effort).

It should be explicitly clarified that the term "telemetry" does not include "telecommunications" equipment in general.

"Bulk Electric System Assets" –

There needs to be one single industry definition, but it ought not to be located here. Rather, it should be part of another NERC standard.

What is meant by the term "large quantities of customers"? If it cannot be defined, it should be addressed in the FAQ, referring to the IAW-SOP definition.

"Incident" & "Security Incident" – The original language is inadequate/inappropriate for usage in subsect.1307, especially regarding the reporting of all "incidents." Merge the two definitions into a single definition one for "Security Incident":

> Any malicious act or suspicious event that compromises or was an attempt to compromise the electronic or physical security perimeter of a critical cyber asset, or, disrupts or was an attempt to disrupt the operation of a critical cyber asset.

Reference throughout is made to **"compliance monitor"** without definition. Who is this intended to be – employee or independent contractor?

Add subsection **(a)(1)(ii)** from Section 1302.

Section 1301

(a)(3)(1st parag.) – The proposed language makes it appear that only one responsible member of senior management shall be chosen from each responsible entity. This ignores that there are major operating subdivisions. Revise the operative phrase to read: "shall

assign at least one member of senior management, consistent with the corporate structure and division of responsibilities, with responsibility for."

(a)(5)(iv) – The 24-hour rule for change/termination of access is too short for general use, and is inconsistent with the limits established in 1306(b)(2). This should only apply to dismissals "for cause" – routine transfers should allow at least three days, ideally five, and perhaps even seven days depending on circumstances and other relevant corporate policy. Even the NRC allows three days for a "favorable" termination, and we understand that FERC allows seven days regarding market-access related changes. Further, Sarbanes-Oxley requirements for corporate governance leave the time to address favorable termination up to the company. Moreover, for some equipment 24 hours is not realistic, as that equipment may require a manual visit (e.g., at substations) or call-up.

(a)(6) – This subsection should be moved to 1306 – it fits more into that subject area (revise and renumber format).

(d)(1) – What is meant by "onsite reviews every three years"? The period is acceptable if such a review is part of the triennial NERC audit – it is far too frequent if to be conducted by hired independent auditors.

Section 1302

The terms "critical cyber assets" and "critical bulk electric system assets" are defined differently within this section (compare opening paragraph and parag. [a][1]), and both are different from that used in the Definitions Section. Moreover, the FAQ says that there is **no** definition. The standard should use one definition, in particular the CIPC-approved definition. See comments at Definitions Section.

(a)(1)(i)(A) –

Clarify that "telemetry" does not include "telecommunication" equipment.

Check formatting and revise/correct as necessary.

(a)(1)(ii) – Move this subsection to the Definitions Section (revise and renumber format).

(a)(1)(iii) –

This subsection raises a number of complicated issues (especially applicable to voltage support):

Does "generating resources" include physical and market resources?

If it includes market resources, how is a determination by the buyer that a resource is critical to be communicated to the seller and/or generator?

What if they do not agree to such a designation?

How is their performance to be evaluated, and by whom?

Who has responsibility for the electronic or physical perimeter (or how is it determined) if the perimeter includes assets from both a transmission and a generator owner?

Define the term "common system" – its meaning is not clear from the context alone.

(a)(1)(iv)(B) – What is meant by the term "initial"? Its meaning is not clear from the context alone.

(a)(1)(v) – Define the term "common system" – its meaning is not clear from the context alone.

(a)(1)(vii)(A) –

The standard needs to clearly and explicitly exclude nuclear assets.

Check formatting and revise/correct as necessary.

(a)(2)(i)(A) –

Underline "and" to emphasize it, as it is important and could be overlooked with the existing formatting.

Check formatting and revise/correct as necessary.

(a)(2)(i)(D) –

Appears to have dropped a negative: the operative clause should read "which do not use a routable protocol."

It would be better, however, to revise the phrase to read "which use an insecure routable protocol," as the original concept is too restrictive (even correcting the missing negative – see above). Inclusion of all assets that use routable protocols is excessive – only those that use such protocols and are also connected to the Internet or a public telecommunications network should be included. The implication in the proposed draft is that non-routable protocols are more secure than routable protocols when used for communications with substation equipment. This is not correct. Even non-routable protocols can be exploited with readily available technology. A modern, properly secured routable protocol connection (using at a minimum encryption and certificates) is significantly more secure than legacy non-routable protocols. (Legacy protocols, while

proprietary, have been in use in many cases over thirty years worldwide, and documentation was widely disseminated. When they were developed, most of these legacy protocols required special hardware to implement, but today can be emulated easily using software. Various methods can be used to impose malicious traffic on a circuit.) Since most of the cyber equipment installed in substations is embedded, applying the proposed standard will have little effect. Also, the equipment was not designed with security or versatility in mind, and cannot be upgraded easily or just for security reasons. The proper way to protect these (generally substation) assets is to secure the communications paths to them, rather than to impose control-center type security methods on them. The standard should simply address the point of vulnerability – the communications interface – and insure that is secured.

Check formatting and revise/correct as necessary.

(a)(2)(i)(E) –

The reference to "1302.1.2.1." does not appear to be matched to any text.

Check formatting and revise/correct as necessary.

Consider moving this subsection to Section 1306, as "other" cyber assets are not critical assets even when located within a security perimeter, and their protection could be considered part of overall system security management.

(g)(1)(i) –

The reference to "1302.1.2.1." does not appear to be matched to any text.

Check formatting and revise/correct as necessary.

(g)(3)(i) –

The reference to "1302.1.2.1." does not appear to be matched to any text.

Check formatting and revise/correct as necessary.

Section 1303

(a)(4) – The term "unrestricted access" does not appear anywhere else – delete, or (even better) clarify and use consistently (i.e., some access may be restricted and thus may not require as high a level of employee/contractor clearance).

At an appropriate location, add subsection (b)(2) from Section 1306, as that is more appropriate for this section (revise and renumber format).

(l)(1) & (l)(2) – It should be made more clear that only "Awareness," and not formal "Training," is required quarterly.

(l)(4)(iii) –

The stipulation of 24 hours is too short for all except dismissals "for cause" (see earlier comments above). Routine transfers, retirements, etc., should have at least three days, ideally five, and perhaps even seven, as determined by the utility to be appropriate and consistent with other corporate policy.

Check formatting and revise/correct as necessary.

(l)(4)(iv) –

Clarify that the minimum check is required "if and only if" there is unrestricted access (see comment above on [a][4]).

Check formatting and revise/correct as necessary.

(n)(2)(i)(4th bullet) –

What is meant by the term "reviews"? Its meaning is not clear from the context alone.

Check formatting and revise/correct as necessary.

(o)(3)(v), (vi), & (vii) – The subparagraphs should be renumbered – such as: (o)(4), (4)(i), and (4)(ii) – and in general check formatting and revise/correct as necessary.

Section 1304

(a)(2)(2nd parag.) –

Clarify that the specified screen is intended for the user to see, saying essentially that they should "follow policy".

The sentence should begin: "Where technically feasible, electronic access." This will recognize that some older equipment cannot be made to display such screens

(e)(2)(2nd parag.) – The phrase "for less than one day" is unclear in context – substitute "Access to any critical cyber asset remains unmonitored for some period that does not exceed 24 hours."

Section 1305

(a)(2) – Reference to "the nearest secured 'four wall boundary'" is overly prescriptive and duplicative, or at least needs to be clarified and/or limited to appropriate facilities. For instance, multiple layers of security already exist generally for attended facilities such as generating plants (e.g., outer perimeter screening and other measures similar to Section 1305[b]). Of particular concern is the extreme difficulty (both in time and money) involved with preventing "surfing" or "tailgating," especially at unattended facilities. Similar difficulties are attendant upon attempts to monitor all egress.

(b)(3)(table)(4th item) – This is too restrictive a definition – consider changing the name from "Security Cage" to "Additional Perimeter" or "Internal Perimeter." In any event, change the definition to read: "An additional, internal secured perimeter within a secured area that permits additional control of physical access to a cyber asset within a larger (usually secured) perimeter, such as by means of a 'cage' or cabinet."

(b)(3)(text)(2nd parag.) –

The phrase "documentation [re implementation] for each physical access point" will lead to far too much paperwork for numerous, identical physical access points. Where there are several identical or substantially equivalent access points for one or a group of security perimeters, this language should be interpreted as requiring only records indicating the controls implemented for the type of access point, and the location of each such individual point. It would be better to change the language to read: "for all physical access points."

The term "de-authorization" is unclear – change to "revocation."

(b)(4)(table)(2nd item) – The wording implies that an audible or visual alarm must go off at every access. This would lead users to turn off or ignore the alarm. Only unauthorized or forced access events should be alarmed. This item should be revised to read as follows: "Access Control System" – "A system that logs and records each access event, including those of unauthorized or forced entry (which must give rise to an alarm). When an alarm is appropriate, the alarm system must be based on" [REMAINDER OF TEXT AS IN ORIGINALLY PROPOSED DRAFT].

(b)(5)(table)(1st item) – Manual logging will be difficult or impossible at unmanned locations, and is not even required by the NRC at all locations. Moreover, for safety reasons, access to unmanned substations must be reported by phone, etc., in almost all circumstances. The supporting text should be modified to read: "A log book or sign-in sheet or other record of physical access accompanied by remote verification."

Section 1306

FIRST – Overall, this standard is far too detailed and onerous for all cyber equipment, especially for non-critical cyber facilities that happen to be located within a secured critical cybersecurity perimeter (or as otherwise determined through the corporate cybersecurity risk assessment to be of little concern). For such equipment, there are much simpler means to assure security, such as securing the communications path – see comment above at Section 1302(a)(2)(i)(D). Examples of such equipment include that using dial-up access at substations or transmission and generation facilities. For instance, given the number of pieces of non-critical equipment at critical locations, the documentation of testing specified by this standard is far too onerous. Therefore, we urge this standard to be made applicable only to the most important facilities and perimeters, such as control centers and energy management systems. A separate, "lite" version of this standard should be made applicable to the remaining equipment standard.

SECOND – The standard should explicitly indicate that it does not apply to "serial" devices.

If the first general comment above is not adopted, the opening or introductory paragraph should have something like the following text added:

> Many of the requirements in this section will not be applicable in the substation environment, since substations are typically unmanned and legacy technology used in them is much more restrictive. Each responsible entity will have to modify or adjust the requirements below to deal with environmental, technical, logistical, personnel, and access differences between such facilities and attended facilities such as control centers or power plants.

Add subsection (a)(6) from Section 1301 (revise and renumber format).

Consider adding subsection (a)(2)(i)(E) from Section 1302 (if so, revise and renumber format).

(a)(1)(2nd parag.) – Emergency repairs should be excluded from the scope of covered "significant changes."

(a)(2) – The last sentence should have a phrase inserted to clarify the intent, so that the operative clause reads: "must establish account management practices for all appropriate accounts (e.g., administration, system, generic and guest accounts)."

(a)(2)(i) – Implementation of strong passwords may not be possible on legacy equipment. The sentence should read "Where practicable, strong passwords for accounts must be used in the absence of more sophisticated methods such as multi-factor access controls."

(a)(2)(ii) – The phrase "audit trail of the account use" should clarify whether it includes any and all actions while logged on.

(a)(2)(iv) – There is a typo at the end of the third line: "and" should instead be "an."

(a)(3) – As proposed, this is impossible to implement for all legacy equipment. In addition, the last sentence is overly prescriptive – compensating measures are not necessary or possible in every instance. The last sentence should be revised: "Where installation of a patch is not practicable or possible, alternative compensating measures must be evaluated, and that evaluation, as well as any such measures actually taken, must be documented."

(a)(4) – The listed malicious software is inconsistent and not complete – use a broader term to cover it, such as "malware" (which is included in the list). Revise the subsection to read as follows:

> A formally documented process governing the application of anti-malware system integrity tools must be employed to prevent, limit, and/or mitigate their introduction or exposure to critical cyber assets at and within the electronic security perimeter.

(a)(5) – Controlled penetration testing is almost always done by third parties, and is very expensive – certainly far too expensive and intrusive to require on a yearly basis. Reference to such testing should be removed from the standard and placed – only as an example – in the FAQ.

(a)(6) – Legacy equipment may not be able to generate audit trails. The first sentence should begin with the phrase "Where practicable, critical cyber security assets must generate…"

(a)(8) – Delete the phrase "inherent and" – it is unclear and unnecessary, since it cannot or should not be disabled if used, and if unused is already covered.

(a)(11) – Annual testing is overly burdensome for very large systems, as it is unlikely to have enough benefit to offset the associated costs/inconveniences. In fact, the requirement of any testing may be overly prescriptive, as the issue is broadly ensuring retrievable storage. That may be done by many means that do not lend themselves to testing per se (e.g., at off-site, underground vaults for computer tapes).

(b)(1) – It must be clarified that the test "environment" need not be a <u>separate</u> environment, as long as it is <u>controlled</u> for safety and reliability, especially regarding telecommunications and substation environments that cannot be duplicated to create a "test" environment.

(b)(2) –

Move the entire subsection to 1303, where it better fits the subject matter, and also reword it to bring it into conformity with that section (revise and renumber format).

Clarify that passwords need not be "cracked" to ensure they comply with the policy, but rather that technological or system tools should be used to ensure the required compliance, and that those means should be documented.

(b)(3) – The required "monthly review of all available vender [sic]" patches is over-broad. For instance, users of Solaris V.8 should not have to review patches for V.7. The language should be revised to read: "monthly review of all available and applicable vender" patches.

Section 1307

Retitle this section to be more specific and clear: "Incident Reporting and Response Plan."

(a)(2) – Delete this entire subsection (and revise and renumber format), consistent with the revision in the Definitions to remove reference to "Incident." The standard should only be applicable to "security" (malicious and/or suspicious) incidents. Equipment and system failures, especially for large companies, are too common and unimportant to necessitate reporting.

(a)(4) – The IAW-SOP should be under revision, and this reference should perhaps even be to the CIPIS, rather than the IAW-SOP.

(b) – Formatting: revise and renumber.

(b)(2)(as revised – "(b)(6)" as drafted), and (c)(2) – As noted above for alarms, the record-keeping requirement is too onerous, especially for large systems, resulting in unnecessarily voluminous files. Records should be kept long-term only regarding "security incidents" Regular files should be "turned over" after one year.

Section 1308

(text)(1st parag.) – The first sentence, by listing only certain entities, appears to exclude generation and transmission owners. They should be included. The sentence should begin: "The responsible entity must establish…"

(text)(3rd parag.) – Move this entire paragraph to the FAQ, as it merely explains the meaning or intent of the standard. Also the second sentence appears to make a requirement by using a phrase that includes the word "require." That it is intended instead

to be merely explanatory is supported by the fact that there is no reference to redundant/backup facility in the "Requirements" or "Measures" subsections. Therefore, revise the sentence (even if relocated to the FAQ) to read "one control center per bulk transmission service area, often with a redundant or backup facility."

(a)(1) – To make this consistent with the third sentence of the second paragraph in the text portion of this standard, this should be revised to read (in part) "exercise its recovery plans annually where there is a low probability of a severe-consequence event."

(a)(3) – As worded, this is confusing, overly prescriptive, and unclear. It should read "The responsible entity shall maintain and communicate to all appropriate personnel an up-to-date recovery plan, including all necessary contact and communication information."

Conclusion

For all of the aforesaid reasons, we urge you to make the suggested changes and clarify the identified problematic areas in the manner indicated.

Respectfully submitted,

for the EEI Security Committee

by Laurence W. Brown,
Director, Legal Affairs, Retail Energy Services,
Edison Electric Institute

LwBrown@EEI.org
202/508-5618

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Charles Yeung	
Organization:	Southwest Power Pool	
Telephone:	(501) 614-3200	
Email:	cyeung@spp.org	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☒ SPP ☐ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☒	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Critical Cyber Assets: Some cyber systems that would not normally be defined as critical cyber assets contribute to the critical data or decision making processes of a critical cyber asset. Likewise, some systems that would not normally be defined as critical cyber assets generate reliability data and may use a critical cyber asset to transmit that data for use by another organization's critical cyber asset for reliability purposes. For example, a RTO market system routinely calculates generation deployment instructions on a regular periodic basis (perhaps 15 minutes). The deployment instructions are sent to generation authorities for use as unit set points. Some RTO market systems calculate a net scheduled interchange value and transmit that data via ICCP (a critical cyber asset) to the balancing authority for inclusion in ACE calculation and regulation control. Compromise of the market system could theoretically result in invalid information being used in reliability operations with resulting consequences. The definition needs to clarify to what extent such systems would come under the umbrella of this standard.

Bulk Electric System Asset: The definition needs to quantify the subjective term "large quantities of customers" either as MW load served or percentage of customers served. "Large quantites" is too vague. The definition needs to quantify the term "extended period of time." Is this hours? Days? Weeks? The definition needs to be consistent with 1302 (a) (1).

Physical Security Perimeter: The FAQ indicates that environmental systems are specifically not included in the physical security perimeter requirement. The standard does need to address these systems in some fashion since the compomise (damage or destruction) of such equipment could result in extended outages of critical cyber assets due to loss of power or air conditioning.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
See comments for Questions 1 and 3.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
General comment: Southwest Power Pool participated in drafting of comments submitted by the ISO-RTO Council and concurs with all comments in that filing. In those comments, the ISO-RTO Council recognizes certain members may have additional comments that would be filed individually. We submit these comments in addition to the ISO-RTO Council filing as they are specific to SPP's opinions and do not believe they conflict with the ISO-RTO Council comments.

General comment: Standard needs to use consistent terminology. For example, the standard refers to the following terms, all assumed to be equivalent: "critical information," "critical cyber information," and "critical cyber asset information."

General comment: References to periods of time should be clarified to indicate whether the time reference is clock/calendar hours/days or business days. For example, does 1301 (b) (5) (i) Access Authorization refer to 5 calendar days or 5 business days? Likewise, does the reference in 1301 (b) (6) to 48 hours refer to 2 calendar days or 2 business days?

1301 (b) (1) (iv) Cyber Security Policy: Does the requirement to document extensions to deviations or exemptions presume that deviations and exemptions have an automatic expiration date coincident with the annual review? If not, why would extensions even be necessary?

1302 (a) (1) Critical Bulk Electric System Assets: The definition needs to quantify the subjective term "large quantities of customers" either as MW load served or percentage of customers served. "Large quantites" is too vague. The definition needs to quantify the term "extended period of time." Is this hours? Days? Weeks?

1302 (a) (1) (i) Critical Bulk Electric System Assets: Presumed incorrectly placed comma, alters meaning. Should the requirement read ". . . such as telemetry, monitoring and control, . . ." or ". . .such as telemetry monitoring and control, . . ."?

1303 Personnel & Training: Bullet resequencing needs to be consistent. Numbering goes from (a) Requirements to (l) Measures.

1303 (l) (4) (ii) Background Screening: Requirement should read ". . . any substantive change of personnel or substantive change in responsiblity of authorized personnel."

1303 (l) (4) (iv) Background Screening: The Social Security Number verification is a USA-only requirement. The SSN equivalent in Canada is precluded by Canadian law from being used in this context.

1304 (a) (4) Documentation Review and Maintenance: Define "timely." Term is too vague and subjective. Needs to be consistent with 1304 (b) (4) Documentation Review and Maintenance.

1304 (b) (4) Documentation Review and Maintenance: 90 days to update the referenced documents is excessive, certainly not "timely." Maximum of 30 days is recommended.

1305 (b) (1) Documentation Review and Maintenance: 90 days to update the physical security plan following a modification to the perimeter or physical security methods is excessive. Maximum of 30 days is recommended.

1305 (b) (4) Monitoring Physical Access Control: Is the expectation of this requirement that physical intrusions be prevented, or merely captured "on tape" for later use if an incident occurs? If CCTV is the only methodology used for physical access monitoring, should there be an expectation of real-time human monitoring?

1306 (a) (1) Test Procedures: Should "critical cyber security assets" be reworded as "critical cyber assets"? If not, this term needs to be defined.

1306 (a) (1) Test Procedures: It is impractical to devise specific procedures to test all known vulnerabilities in an effort to ensure the security patch or alternate mitigation is effective. A reasonable assumption must be made that if all known security patches are installed or alternate mitigation strategies have been implemented, the specific operating system vulnerability has been addressed. Test procedures, in conjunction with the annual controlled penetration test, should confirm that designed security access controls are functioning properly. This could include, for example, verification that multi-factor network access authentication or the requirement for digital certificates to gain access to an application system is not disabled by the update.

1306 (a) (2) (iv) Acceptable Use: ". . . usage to and individually named person . . ." should read ". . . usage to an individually named person . . ."

1306 (a) (2) (iv) Acceptable Use: What does the term "personal registration" for any generic accounts mean?

1306 (a) (3) Security Patch Management: There are occasions where a security patch cannot be applied and no mitigation strategy is available. The standard may want to require the asset owner to work with the vendor to resolve the incompatibility between the system and the patch. Otherwise, the asset owner can just say "hey, cannot fix this" and drop it at that.

1306 (a) (10) Operating Status Monitoring Tools: What is the expectation when the automated tools detect a problem? Should the standard prescribe a requirement for notification, or is simply looking at logs and reports some time after the fact good enough? If the latter, then why prescribe the tools at all?

1306 (b) (1) Test Procedures: Requirement should be reworded to require documentation of testing of security features or access controls, not vulnerabilities. It is impractical to devise at test procedure for all known vulnerabilities (see comment to 1306 (a) (1) Test Procedures).

1306 (b) (2) Account Password Management: The requirement for documentation and verification that accounts comply with the password policy could be construed to require that the password itself be verified. It is hard enough to verify that the password has been changed within a certain period of time on some operating systems. The FAQ, at least, needs to elaborate on this requirement.

1306 (b) (3) Security Patch Management: The requirement needs to address layered application patches (e.g. MS Office, Apache, Tomcat, JBoss, Hummingbird Exceed) as well.

1306 (b) (4) Integrity Software: Maintaining a record of the version level of the integrity software currently in use is cumbersome and problematic. Most anti-virus products routinely update version levels as part of the scheduled updates, often several times per week. The standard needs to require that the integrity software be maintained up to date and documentation needs to demonstrate how

that is done and how it is verified (particularly necessary when the software is configured for automatic, unattended updates).

1306 (b) (6) Retention of Logs: This requirement needs to specify the retention period, consistent with retention periods defined elsewhere in the standard.

1307 Incident Response Planning: Bullet resequencing needs to be consistent. Numbering of sub bullets in (b) Measures picks up where (a) Requirements left off. Sections following (b) Measures start with repeated (b).

1307 (b) (6)\ Measures: ". . . records of incidents and cyber security incidents. . ." needs to be reworded. Does the first "incidents" refer to physical incidents?

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	John Lim	
Organization:	Con Edison	
Telephone:	212-460-2712	
Email:	limj@coned.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☒ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☒	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☒	5 - Electric Generators
	☒	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Bulk Electric System Asset: "would have a significant impact on the ability to serve large quantities of customers for an extended period of time" and "or would cause significant risk to public health and safety" are subjective and not necessarily related to the operation of the bulk electric system. The scope of this standard should be focused on critical cyber assets affecting the reliable operation of the bulk electric system.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?

1302: A definition of what constitutes a bulk electric system asset and what makes it critical must be clear enough to allow responsible entities to identify it. Con Edison believes that the definition of "bulk electric system" and "critical bulk electric asset" is outside the scope of a cyber security standard. Wording such as "as defined by NERC and the applicable regional reliability coordinating organization" can be used to defer the definition of these to the appropriate group within NERC and the regions. The FAQ can provide additional clarifications based on current definitions or work in progress in NERC.

In section 1303, in the background screening requirement, clarify what "unrestricted access" means. The FAQ should clarify whether THIS standard should require background screening for system operators using the control application or just personnel with "unrestricted access" (both physical or logical) with the ability to damage or otherwise compromise the critical cyber asset hardware, software, data or network component. Also in this section, the requirement to revoke access within 24 hours is too restrictive. Section 1301 allows 5 days for updating access records for changes. We suggest 24 hours only for terminations for cause, and 7 days for all other cases of status changes, and that these be consistently applied in all sections where access updates are required.

In 1306,
Account and Password Management: In some legacy systems, there may not be any account or password management capabilities. The requirement should provide the capability for the entity to claim a waiver for this section in such cases.
Vulnerability Assessment: a vulnerability assessment of the critical bulk electric cyber assets may be part of the overall organization's full vulnerability assessment program. These assignments can take up to 3 months to complete in a large organization. We suggest that the requirement be changed from "annual" to "at least once every 2 years".

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
The implementation of the measures, procedures and controls to provide 100% compliance can require significant efforts in manpower and investment. The implementation plan should allow for a multi-year progression towards 100% compliance without penalties.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Robert Pellegrini	
Organization:	United Illuminating	
Telephone:	203-499-2413	
Email:	Robert.Pellegrini@uinet.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☒ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

NPCC's participating members recommend that the definition of Critical Cyber Assets be;

"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).

NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.

NPCC's participating members recommend changing the Incident definition from

"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."

to

"Incident: Any physical or cyber event that:

disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?

NPCC's participating members feel there is much redrafting to be done to the standard and that the following items may be considered "show stoppers" by some.

Standard 1300 is based on what the critical BES assets are, which is defined in 1302.a.1. Per question 1, NPCC's participating members do not agree with that definition and have made suggestions as to what the Drafting Team may do to address the issue.

NPCC's participating members also believe the need to change the Incident definition, to the one shown in Question 1 is important.

As previously discussed and commented on in various forums, NPCC supports the NERC decision to move away from monetary sanctions.

NPCC's participating members have also expressed concern over the incremental administrative tasks and documentation requirements to be compliant with this standard and hopes the Standard Drafting Team will consider this during the development of the associated "Implementation Plan".

Throughout the document, the compliance levels should be updated to measure the proposed revisions suggested below. NPCC has made some recommendations in this regard.

There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected and recognized with consideration of this Standard.

The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to gauge the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. It is NPCC's hope that this will be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.

NPCC’s participating members agrees with the intent of Section 1303. The term “background screening” however has too many issues for NPCC participating members and recommend that this section’s title become “Personnel Risk Assessment”. Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk and have made recommendations later in the form that will make this Section acceptable.

The references within the standard made to other portions of Standard 1300 are not correct. Without clear references, NPCC cannot determine if the document is acceptable or not. For

example, 1301.a.3 says "as identified and classified in section 1.2." Where is this section? Each one of these incorrect references must be corrected.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

Correct references as covered in question 2.

Request clarification on what "information" is protected in 1301.a.2.

Change 1301.a.2 from;

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

to

"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets." (NPCC's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)

Change 1301.a.2.i from;

"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."

to

"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well." (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)

Change 1301.a.3 from;

"….entity's implementation of…"

to

"…entity's implementation and adherence of…"(NPCC's participating members believe it is important to stress that not only is it important to implement this Standard but to adhere to it as well.

The “24 hours” in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.

Change 1301.a.5.iv from;

"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."

to

"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven calendar days for all other users of a change in user access status. All access revocations/changes must be authorized and documented." (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)

change 1301.b.5.i from;

"5 days"

to

"7 calendar days" (NPCC's participating members believe that the 5 days may be not be sufficient time especially when considering holiday seasons)

1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency in the reference for retention of audit records.

1301.d.3.iv, request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor

1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii to ensure the protection of the identity/personal information of the affected individuals

Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor

1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.

1301.e.2.iii, change from;

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

to

"An authorizing authority has been designated but a formal process does not exist to

test, validate and deploy systems into production, or" (NPCC believes it was the drafting team's itent to deploy the system rather than promote which has a different connotation associated with it,)

Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change "Executive Management" to "Senior Management" for consistency and clarity.

1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).

NPCC Participating Members believe that the concept of the Bulk Electric System and association "definitions" may not be appropriate to capture the intent of the standard. NPCC suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.

Replace the 1302 preamble and 1302.a.1 and 1302.a.2 as shown below, with;

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 which support the reliable operation of the bulk electric system.

The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.

(a) Requirements
Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.

(1) Critical Bulk Electric System Operating Functions and Tasks

The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:

- monitoring and control
- load and frequency control
- emergency actions
- contingency analysis
- arming of special protection systems
- power plant control
- substation control
- real-time information exchange

(2) Critical Cyber Assets

(i) In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:

A) The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.

B) The consequences of the Operating Function or Task being compromised (i.e. “highjacked”) for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.

C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.

D) Known risks associated with particular technologies

Change 1302.g.1 from;

"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."

to

"1 Critical Bulk Electric System Operating Functions and Tasks
(i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."

Change 1302.g.2.i from;

"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."

to

"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure." (NPCC believes the use of the word additional is of no value as used here and recommends removal).

Change 1302.g.5 from;

"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"

to

"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval" (NPCC believes that it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations of operations is lost.)

Change 1302.g.5.i from;

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

to

"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."

Change 1302;
"critical bulk electric system assets"

to

"critical bulk electric system operating functions and tasks"

1303, NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for the NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk.

The FAQ describes supervised access, 1303 does not touch upon this topic.

Change 1303.a.4 from "unrestricted access" to "authorized access".

Change 1303.a.4 title to "Personnel Risk Assessment."

Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."

Change 1303.a.2 from;

"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."

to

"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"

1303.a.4 from;

"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."

to

"Personnel Risk Assessment: There must be a documented company personnel risk assessment process."

Add to 1303 Measures.2, a training measures for disaster recovery (1308) and incident response planning (1307).

The numbering of 1303 starting with Measures needs correction.

1303 Measures 4.i, request clarification. Does this include third party personnel?

Change 1303.Measures.4.i from;

"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)."

to

"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 respective security perimeter(s)." (NPCC believes there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)

Change 1303.Measures.4.ii from;

"two business days"

to

"seven calendar days", per earlier comments and to keep consistent with FERC Order.

1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days", per earlier comments

1303.Measure.4., remove;

Subsections iv, v and vi.

and replace with

"There must be a documented company personnel risk assessment process." NPCC's participating members feel these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities."

1303.Compliance Monitoring Process.2, NPCC's participating members do not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria
is not applied, or" to "Personnel risk assement program is practiced, but not properly documented, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."

Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii

From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.

Change 1304 a.2 Electronic Access Controls:
to

"The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" 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)."

Change 1304 a.3 Monitoring Electronic Access Control:
to
"The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."

Change 1304 a.4 from;

"The responsible entity shall ensure that all documentation reflect current configurations and processes."

to

The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.

1304.a.4 Remove -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. (This is a measure and should be removed here)

Compliance Monitoring Process;
Change 1304.d.3 from;

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

to

"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"

Level of non compliance
"Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.

1305 Physical Security;

Eliminate the bulleted items in the Preamble to Section 1305-they appear in the Requirement section.

Replace 1305 a.1 with;
"Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.
• The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),

• The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and
• The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."

Change the following - (a) Requirements;
"(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."

to

"(3) Physical Access Controls: The responsible entity shall implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.
(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.
(5) (We recommend deleting this bullet as the intent is captured in bullet "4").
(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."

Change Measures;

"(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."

to

"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility." (NPCC believes the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)

In 1306.a.1, last paragraph, modify the second sentence to read as follows;

"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."

1306.a.2.ii change "pooding" and "puffing" to "putting" (it appears a pdf translation problem as some documents the group printed have it and others did not)

1306.a.2.ii remove "Generic" from the title

1306.a.2.iii, use "at least annually" instead of "at least semi-annually"

Change 1306.a.3 from;
"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."

to

"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets." (NPCC believes that it upgrades are a subset of the applicable security patches.)

Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."

Change 1306.a.4 from;

"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."

to

"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."

1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).

Change 1306.a.6 from

"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."

to

"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three calendar years in an exportable format, for possible use in further event analysis."

1306.a.7 Remove "Configuration Management" from the title

1303.a.8 Remove the word "inherent" it is not clear what is meant by it.

1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.

1306, remove 1306.a.11 since 1308 addresses back-up and recovery.

1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.

1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days".

1306.b.3, remove;

"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."

and change

"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."

to

"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."

1306 b.3 first sentence-eliminate the word "management".

1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.

1306.b.4 third sentence Change
"..so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."

to

"..mitigate risk of malicious software".

1306.b.4 Remove the second sentence.

1306.b.4 Replace the fourth sentence with;

"Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."

1306.b.5 remove the first sentence.
Based on the common use of third parties for outsourcing of this associated work of vulnerabilty assessment, it is not reasonable to maintain the information called for in sentence one.

Change 1306.b.6 from;

"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."

to

"Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis."

1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"

Remove 1306.b.11, since 1306.a.11 was removed.

1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."

1306.d.3.iii, change "system log files" to "audit trails"

1306.e.2, change "the monthly/quarterly reviews" to "the reviews"

1306.e.2.ii.C, change "anti-virus" to "malicious"

1306, the Compliance levels should be updated to match the above measures.

1307, spell out and provide clarification on the acronyms throughout.

Change 1307, from;

"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."

to

"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."

1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;

"Incident and Cyber Security Incident Reporting"

to

"Security Incident Reporting".

and also Change from;

"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

to

"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

Refer to our definition of a "security incident", change 1307.b.5 from;

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

to

"The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements."

Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."

to

"The responsible entity shall retain records of security incidents for three calendar years."

Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."

to

"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."

1307.d.1 there is a 90 day reference that does not appear in the measures.

In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.

Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	S. Kennedy Fell	
Organization:	New York Independent System Operator	
Telephone:	518-356-7537	
Email:	sfell@nyiso.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☒ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☒	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

The NYISO recommends that the definition of Critical Cyber Assets be;

"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).

The NYISO does not agree with definition in 1302.a.1. The NYISO supports the idea of having a stand alone definitions document to accompany the entire set of standards.

The NYISO also recommends changing the Incident definition from

"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."

to

"Incident: Any physical or cyber event that:

disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
As previously discussed, the NYISO supports NERC decision to move away from monetary sanctions, however the NYISO would like to reinforce their position the it does not support monetary sanctions.

The NYISO is concerned about the incremental administrative tasks and documentation requirements to support the 1300 standard.

With the increased requirements within the 1300 standard , the NYISO believes the requirements need to be phased in over 1 to 2 years. Additionally, audit compliance would commence after the entity is to be fully compliant.

Standard 1300 is based on what the critical BES assets are, which is defined in 1302.a.1. Per question 1.

The references within the standard made to other portions of Standard 1300 are not correct. For example, 1301.a.3 says "as identified and classified in section 1.2." Each one of these incorrect references must be corrected.

Throughout the document, the compliance levels need to be updated to measure the proposed revisions suggested below.

Confidentiallity and disclosure is a growing concern as the industry moves towards mandatory standards. There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected with consideration of this and all Standard.

The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to guage the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. It is the NYISO's hope that this will be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.

The NYISO agrees with the intent of Section 1303. The term “background screening” however has too many issues for the NYISO and recommends that this section’s title become “Personnel Risk Assessment”. Portions of 1303 are too prescriptive and the NYISO feels that the responsible entity should have more latitude in determining what is an acceptable level of risk and have made recommendations later in the form that will make this Section acceptable.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

Correct references as covered in question 2.

Request clarification on what "information" is protected in 1301.a.2.

Change 1301.a.2 from;

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

to

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

Change 1301.a.2.i from;

"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."

to

"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well."

Change 1301.a.3 from;

"….entity's implementation of…"

to

"…entity's implementation and adherence of…

The “24 hours” in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.

Change 1301.a.5.iv from;

"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."

to

"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven business days for all other users of a change in user access status. All access revocations/changes must be authorized and documented."

change 1301.b.5.i from;

"5 days"

to

"7 calendar days"

In 1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency.

In 1301.d.3.iv, request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor

In 1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii

Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor

In 1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.

In 1301.e.2.iii, change from;

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

to

"An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or"

Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change "Executive Management" to "Senior Management" for consistency and clarity.

In 1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days(should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).

The NYISO believes that the concept of the Bulk Electric System and association "definitions" may not be appropriate to capture the intent of the standard. The NYISO suggests the substantive

changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.

Replace the 1302 introduction and 1302.a.1 and 1302.a.2 as shown below, with;
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 which support the reliable operation of the bulk electric system.

The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.

(a) Requirements
Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.

(1) Critical Bulk Electric System Operating Functions and Tasks

The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks affected by cyber assets may include but are not limited to the following:

- monitoring and control
- load and frequency control
- emergency actions
- contingency analysis
- arming of special protection systems
- power plant control
- substation control
- real-time information exchange

(2) Critical Cyber Assets

(i) In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:

A) The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.

B) The consequences of the Operating Function or Task being compromised (i.e. “highjacked”) for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.

C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.

D) Known risks associated with particular technologies

Change 1302.g.1 from;

"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."

to

"1 Critical Bulk Electric System Operating Functions and Tasks
(i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."

Change 1302.g.2.i from;

"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its additional critical bulk electric system assets."

to

"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets."

Change 1302.g.5 from;

"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"

to

"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval"

Change 1302.g.5.i from;

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

to

"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."

Change 1302;
"critical bulk electric system assets"

to

"critical bulk electric system operating functions and tasks"

1303, The NYISO agrees with the intent of Section 1303. The term “background screening” however has too many issues for the NYISO and recommends that this section’s title become “Personnel Risk Assessment”. Portions of 1303 are too prescriptive and the NYISO feels that the responsible entity should have more latitude in determining what is an acceptable level of risk.

The FAQ describes supervised access, 1303 does not touch upon this topic. Change 1303.a.4 from "unrestricted access" to "authorized access". Change 1303.a.4 title to "Personnel Risk Assessment." Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."

Change 1303.a.2 from;

"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."

to

"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"

1303.a.4 from;

"(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."

to

"(4) Personnel Risk Assessment: There must be a documented company personnel risk assessment process."

Add to 1303 Measures.2, a training measure section for disaster recovery (1308) and incident response planning (1307).

The numbering of 1303 starting with Measures needs correction.

1303 Measures 4.i, request clarification. Does this include third party personnel?

Change 1303.Measures.4.i from;

"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)."

to

"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 respective security perimeter(s)."

Change 1303.Measures.4.ii from;

"two business days"

to

"seven calendar days", per earlier comments and keep consistent with FERC Order.

1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or diciplinary action, or seven days", per earlier comments

1303.Measure.4., remove;

Subsections iv, v and vi.

and replace with

"There must be a documented company personnel risk assessment process." The NYISO feels these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities."

1303.Compliance Monitoring Process.2, The NYISO does not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria is not applied, or" to "Personnel risk assement program is practiced, but not properly documented, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."

Correct the identation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii

From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.

1304 a.2 Electronic Access Controls:
The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" 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).

1304 a.3 Monitoring Electronic Access Control:
The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized

Change 1304 a.4 from;

"The responsible entity shall ensure that all documentation reflect current configurations and processes."

to

The responsible entity shall ensure that all documentation required comply with 1304 a 1 through 1304 a.3 reflect current configurations and processes.

1304 a.4 Remove -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. (This is a measure and should be removed here)

Compliance Monitoring Process;
Change 1304.d.3 from;

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

to

"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"

Level of non compliance
"Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.

1305 Physical Security;

Eliminate the bulleted items in the Preamble to Section 1305-they appear in the Requirement section.

Replace 1305 a.1 with Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.
• The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),
• The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and
• The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets.

Change the following - (a) Requirements;
"(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."

to

"(3) Physical Access Controls: The responsible entity shall implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.
(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.
(5) (We recommend deleting this bullet as the intent is captured in bullet "4").
(6) Maintenance and testing: The responsible entity shall implement a

comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."

Change Measures;

"(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."

to

"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility."

In 1306.a.1, last paragraph, modify the second sentence to read as follows;

"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."

1306.a.2.ii change "pooding" and "puffing" to "putting"

1306.a.2.ii remove "Generic" from the title

1306.a.2.iii, use "at least annually" instead of "at least semi-annually"

Change 1306.a.3 from;
"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."

to

"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets.
Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."

Change 1306.a.4 from;

"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."

to

"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."

1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).

Change 1306.a.6 from

"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."

to

"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three years in an exportable format, for possible use in further event analysis."

1306.a.7 Remove "Configuration Management" from the Title

1303.a.8 Remove the word "inherent" it is not clear what is meant by it.

1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.

1306, remove 1306.a.11 since 1308 addresses back-up and recovery.

1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.

1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days".

1306.b.3, remove;

"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."

and change

"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."

to

"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other

compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."

In 1306 b.3 first sentence-eliminate the word "management".

1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.

1306.b.4 third sentence Change
"..so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."

to

"..mitigate risk of malicious software".

1306.b.4 Remove the second sentence.

1306.b.4 Replace the fourth sentence with;

"Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."

1306.b.5 remove the first sentence. Based on a third party outsourcing of this associated work of vulnerabilty assessment.

Change 1306.b.6 from;

"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."

to

"Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three years in an exportable format, for possible use in further event analysis."

1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"

Remove 1306.b.11, since 1306.a.11 was removed.

1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."

1306.d.3.iii, change "system log files" to "audit trails"

1306.e.2, change "the monthly/quarterly reviews" to "the reviews"

1306.e.2.ii.C, change "anti-virus" to "malicious"

1306, the Compliance levels should be updated to match the above measures.

1307, spell out and provide clarification on the acronyms throughout.

1307.d.1 there is a 90 day reference that does not appear in the measures.

Change 1307, from;

"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."

to

"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."

1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;

"Incident and Cyber Security Incident Reporting"

to

"Security Incident Reporting".

and also Change from;

"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

to

"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

Refer to our definition of a "security incident".

Change 1307.b.5 from;

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

to

"The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements."

Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security

incidents for three calendar years."

to

"The responsible entity shall retain records of security incidents for three calendar years."

Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."

to

"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."

In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.

Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Robert E. Strauss	
Organization:	New York State Electric & Gas Corp. (NYSEG)	
Telephone:	607-762-5662	
Email:	restrauss@nyseg.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☒ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

NYSEG concurs with the following NPCC comment:

NPCC's participating members recommend that the definition of Critical Cyber Assets be;

"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).

NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.

NPCC's participating members recommend changing the Incident definition from

"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."

to

"Incident: Any physical or cyber event that:

disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
1. In general, there are too many areas which require interpretations which are defined or included in the FAQ's. Since the FAQ's would not be part of the approval these interpretations need to somehow be included within the standard.
2. An alternative to developing a definiton of Bulk Electric System would be to require the Reliabity Authority for each Control Area to identify the Bulk Electric System for its respective Control Area. The next step would be for each Responsible Entity to identify the Bulk Electric System Asset they are responsible for in that system, identify the critical operating system functions and tasks and then identify the Critical Cyber Assets.
3. This standard is not consistent in the level of detail for each area being adddressed. Also there is no process indicated for change to be made following approval. A different approach to consider would be to make the standard identifying roles and responsiblities; identification of what is required to be included within the standard and its objective; and the process for review and sanctions. A description of minimum level for each area or standard should be attached as a guideline. In that manner the Standards can be permanent and only adjust the attachment if warranted. The way the standards read now, they must be adhered to unless the responsible individual in the company grants an exemption or deviation. A standard should be a standard with no deviation. Minimum guidelines would be a more practical approach. A deviation or excemption to a guideline is a more pragmatic approach.

NYSEG also concurs with the following NPCC comments:

NPCC's participating members recommend that the definition of Critical Cyber Assets be;
"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).
NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.
NPCC's participating members recommend changing the Incident definition from

"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."
to

"Incident: Any physical or cyber event that:
disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
Correct references as covered in question 2.

Request clarification on what "information" is protected in 1301.a.2.

Change 1301.a.2 from;

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

to

"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets." (NPCC's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)

Change 1301.a.2.i from;

"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."

to

"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well." (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)

Change 1301.a.3 from;

"….entity's implementation of…"

to

"…entity's implementation and adherence of…"(NPCC's participating members believe it is important to stress that not only is it important to implement this Standard but to adhere to it as well.

The “24 hours” in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.

Change 1301.a.5.iv from;

"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."

to

"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven calendar days for all other users of a change in user access status. All access revocations/changes must be authorized and documented." (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)

change 1301.b.5.i from;

"5 days"

to

"7 calendar days" (NPCC's participating members believe that the 5 days may be not be sufficient time especially when considering holiday seasons)

1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency in the reference for retention of audit records.

1301.d.3.iv, request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor

1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii to ensure the protection of the identity/personal information of the affected individuals

Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor

1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.

1301.e.2.iii, change from;

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

to

"An authorizing authority has been designated but a formal process does not exist to

test, validate and deploy systems into production, or" (NPCC believes it was the drafting team's itent to deploy the system rather than promote which has a different connotation associated with it,)

Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change "Executive Management" to "Senior Management" for consistency and clarity.

1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).

NPCC Participating Members believe that the concept of the Bulk Electric System and association "definitions" may not be appropriate to capture the intent of the standard. NPCC suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.

Replace the 1302 preamble and 1302.a.1 and 1302.a.2 as shown below, with;

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 which support the reliable operation of the bulk electric system.

The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.

(a) Requirements
Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.

(1) Critical Bulk Electric System Operating Functions and Tasks

The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:

- monitoring and control
- load and frequency control
- emergency actions
- contingency analysis
- arming of special protection systems
- power plant control
- substation control
- real-time information exchange

(2) Critical Cyber Assets

(i) In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:

A) The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.

B) The consequences of the Operating Function or Task being compromised (i.e. "highjacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.

C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.

D) Known risks associated with particular technologies

Change 1302.g.1 from;

"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."

to

"1 Critical Bulk Electric System Operating Functions and Tasks
(i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."

Change 1302.g.2.i from;

"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."

to

"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure." (NPCC believes the use of the word additional is of no value as used here and recommends removal).

Change 1302.g.5 from;

"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"

to

"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval" (NPCC believes that it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations of operations is lost.)

Change 1302.g.5.i from;

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

to

"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."

Change 1302;
"critical bulk electric system assets"

to

"critical bulk electric system operating functions and tasks"

1303, NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for the NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk.

The FAQ describes supervised access, 1303 does not touch upon this topic.

Change 1303.a.4 from "unrestricted access" to "authorized access".

Change 1303.a.4 title to "Personnel Risk Assessment."

Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."

Change 1303.a.2 from;

"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."

to

"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"

1303.a.4 from;

"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."

to

"Personnel Risk Assessment: There must be a documented company personnel risk assessment process."

Add to 1303 Measures.2, a training measures for disaster recovery (1308) and incident response planning (1307).

The numbering of 1303 starting with Measures needs correction.

1303 Measures 4.i, request clarification. Does this include third party personnel?

Change 1303.Measures.4.i from;

"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)."

to

"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 respective security perimeter(s)." (NPCC believes there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)

Change 1303.Measures.4.ii from;

"two business days"

to

"seven calendar days", per earlier comments and to keep consistent with FERC Order.

1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days", per earlier comments

1303.Measure.4., remove;

Subsections iv, v and vi.

and replace with

"There must be a documented company personnel risk assessment process." NPCC's participating members feel these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities."

1303.Compliance Monitoring Process.2, NPCC's participating members do not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria
is not applied, or" to "Personnel risk assement program is practiced, but not properly documented, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."

Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii

From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.

Change 1304 a.2 Electronic Access Controls:
to

"The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" 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)."

Change 1304 a.3 Monitoring Electronic Access Control:
to
"The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."

Change 1304 a.4 from;

"The responsible entity shall ensure that all documentation reflect current configurations and processes."

to

The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.

1304.a.4 Remove -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. (This is a measure and should be removed here)

Compliance Monitoring Process;
Change 1304.d.3 from;

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

to

"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"

Level of non compliance
"Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.

1305 Physical Security;

Eliminate the bulleted items in the Preamble to Section 1305-they appear in the Requirement section.

Replace 1305 a.1 with;
"Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.
• The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),

• The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and
• The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."

Change the following - (a) Requirements;
"(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."

to

"(3) Physical Access Controls: The responsible entity shall implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.
(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.
(5) (We recommend deleting this bullet as the intent is captured in bullet "4").
(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."

Change Measures;

"(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."

to

"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility." (NPCC believes the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)

In 1306.a.1, last paragraph, modify the second sentence to read as follows;

"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."

1306.a.2.ii change "pooding" and "puffing" to "putting" (it appears a pdf translation problem as some documents the group printed have it and others did not)

1306.a.2.ii remove "Generic" from the title

1306.a.2.iii, use "at least annually" instead of "at least semi-annually"

Change 1306.a.3 from;
"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."

to

"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets." (NPCC believes that it upgrades are a subset of the applicable security patches.)

Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."

Change 1306.a.4 from;

"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."

to

"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."

1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).

Change 1306.a.6 from

"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."

to

"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three calendar years in an exportable format, for possible use in further event analysis."

1306.a.7 Remove "Configuration Management" from the title

1303.a.8 Remove the word "inherent" it is not clear what is meant by it.

1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.

1306, remove 1306.a.11 since 1308 addresses back-up and recovery.

1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.

1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days".

1306.b.3, remove;

"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."

and change

"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."

to

"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."

1306 b.3 first sentence-eliminate the word "management".

1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.

1306.b.4 third sentence Change
"..so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."

to

"..mitigate risk of malicious software".

1306.b.4 Remove the second sentence.

1306.b.4 Replace the fourth sentence with;

"Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."

1306.b.5 remove the first sentence.
Based on the common use of third parties for outsourcing of this associated work of vulnerabilty assessment, it is not reasonable to maintain the information called for in sentence one.

Change 1306.b.6 from;

"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."

to

"Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis."

1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"

Remove 1306.b.11, since 1306.a.11 was removed.

1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."

1306.d.3.iii, change "system log files" to "audit trails"

1306.e.2, change "the monthly/quarterly reviews" to "the reviews"

1306.e.2.ii.C, change "anti-virus" to "malicious"

1306, the Compliance levels should be updated to match the above measures.

1307, spell out and provide clarification on the acronyms throughout.

Change 1307, from;

"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."

to

"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."

1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;

"Incident and Cyber Security Incident Reporting"

to

"Security Incident Reporting".

and also Change from;

"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

to

"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

Refer to our definition of a "security incident", change 1307.b.5 from;

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

to

"The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements."

Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."

to

"The responsible entity shall retain records of security incidents for three calendar years."

Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."

to

"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."

1307.d.1 there is a 90 day reference that does not appear in the measures.

In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.

Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Laurent Webber	
Organization:	Western Area Power Administration	
Telephone:	720-962-7216	
Email:	webber@wapa.gov	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT	☒	1 - Transmission Owners
☐ ECAR	☐	2 - RTOs, ISOs, Regional Reliability Councils
☐ FRCC	☐	3 - Load-serving Entities
☐ MAAC	☐	4 - Transmission-dependent Utilities
☐ MAIN	☐	5 - Electric Generators
☒ MAPP	☐	6 - Electricity Brokers, Aggregators, and Marketers
☐ NPCC	☐	7 - Large Electricity End Users
☐ SERC	☐	8 - Small Electricity End Users
☐ SPP	☒	9 - Federal, State, Provincial Regulatory or other Government Entities
☒ WECC		
☐ NA - Not Applicable		

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Critical Cyber Assets definition. The later part of the first sentence, such as…at a minimum, implies that all these assets perform critical bulk electric system functions which is not consistent with criteria in 1302 (for example, small generators). Removing it is recommended since specifics are addressed in 1302. The definition of Critical Bulk Electric System assets in 1302 should also be modified by eliminating item (ii), item (B) under (iv), and item (vi). Including substation equipment in this standard is not workable for numerous reasons. NERC should establish a cyber security standard that will advance the cause of security AND be workable to implement. Substation equipment should be captured by utilities under item vii (risk-based assessment) as needed. Need to include definitions of the terms: Owners, Custodians, and Users. It would be a good idea to include a definition of Sensitive Information or something similar that refers to information pertaining to critical cyber assets…. The idea is to be more definitive about what information should be protected pursuant to 1301(a)(2). For the definition of Incident, recommend the phrase or could have lead to a disruption of be removed. How would one measure/determine if it could have lead to a disruption? It would be interpreted differently by each entity. For the definition of Incident, the phrase or was an attempt to compromise should be eliminated. This will be interpreted by each individual entity and may result in thousands of reports daily. For the definition of Security Incident, recommend the phrases are known to and or could have resulted in be removed. They are vague and would be interpreted differently by each entity. Responsible Entity. Since definitions are to be included in a separate glossary, rewording the last part of the sentence, as identified in the Reliability Function table of the Standard Authorization Request for this standard, is suggested. The definition of critical asset in 1302(a)(2) should be clarified. For example, one of the key determinants to whether a device is considered a critical asset is whether it uses a routable protocol. At the very least, what is considered a routable protocol should be defined in the glossary. Also, the and-or Boolean logic of this section is confusing. Possibly a decision tree chart would help clarify the logic.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?

NERC should utilize existing Cyber Security standards (see series 800, Computer Security) from the National Institute of Standards and Technology (NIST) that are already well-developed, tested, and recognized by GAO, OMB, and Federal sector, instead of having electric utility people create a whole new set of such standards. Since all Federal Government agencies are currently mandated to follow the NIST guidelines, the imposition of different NERC guidelines imposes an unnecessary redundant and burdensome level of documentation and audits that result in increased cost without a commensurate improvement in security. Section 1302, Critical Cyber Assets, (a)(1). The standard is not clear whether the Largest Single Contingency for a Reportable Disturbance is specifically for the Entity or the Reserve Sharing Group (as an Entity may belong to a Reserve Sharing Group). Question: The FAQ defines the MOST SEVERE SINGLE CONTINGENCY as the largest single generator in the system. Does this mean only a single generating unit and not a generating station? What about greater single contingency losses as represented by the transmission facilities (subs, high voltage lines) that carry aggregated power from multiple units in a single station and, therefore, carry more power than any individual generators in a Reserve Sharing Group? Wouldn't those facilities then represent the most severe single contingency? Section 1302, Critical Cyber Assets, (a)(2). The logistics for items A-E should be clarified; it is confusing. Section 1302, Critical Cyber Assets, (a)(2). There should be more clarification/restatement of requirements for dial-up cyber assets that do and do not support routable protocols (what requires a physical perimeter and what does not, and what requires an electronic perimeter and what does not). Is there a typo in 1302(a)(2)(i)(D): it reads, which do use a routable protocol, should is say which do NOT use a routable protocol? All required minimum review periods should be a standard period of one year. Having so many review periods and having numerous periodicities is not practicable. Under 1301(a)(3), the sentence that reads, This person must authorize any deviation or exception from the requirements of this standard, should be changed to read, The person that must authorize any deviation or exception from the requirements of this standard must be specified in the responsible entity's governance documentation. In several places in the standard, the issue of authorized access and tracking that access is discussed. It is usually unclear if this is meant to include only those that have access with administrative privileges or if it extends to those that utilize the assets as users (dispatchers using an EMS, for example). One example of such a gray area can be found in 1301(a)(5)(ii), for example, but there are many such areas. NERC should not focus on access by those that only have rights to use the system, and should clarify in all such contexts that the reference is only to those with administrative access. Section 1303, Measures (4)(iv), is one of many examples of too much proscriptive detail. All the background screening criteria should be altered/simplified to only say that a utility must have a policy related to the screening and must follow that policy and be able to show the records that the policy was followed. Section 1303, Requirement (4), the phrase prior to being granted unrestricted access to critical assets should be removed since it conflicts with Section 1303, Measure (4)(iv). This standard is an expansion to standard 1200 and has a direct related impact on implementation and resource requirements. It would be helpful if the implementation plan were provided. Under 1301(d)(3)(ii), remove the word and at the end of the sentence. Under 1301(e)(1), what is the difference between (iv) and (v)? Under 1306(a)(2), please rephrase the second sentence, The responsible entity must

establish…, to make it clear. Reference 1303, Personnel and Training (1)(2)(iv) - Training on recovery of critical cyber assets should be tied to the system or structure (Under NIST this is part of the Security Plan) and not general Cyber Security Awareness training. This comment also applies to 1308 Recovery Plans (a)(4). Reference 1306, System Security Management (b)(2) - Please remove the following from the second sentence in that section "that all accounts comply with the password policy." There is no way to audit whether account passwords comply with the password policy outside of cracking them. The only way to ensure that passwords comply with the password policy is to check for compliance on the front end when the user creates the password.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
Generally agree with the thoughts and principles behind the new standard; however, are concerned about the considerable expansion in the number and types of critical cyber assets, as well as the increased specificity throughout the standard. Will there be an expanded implementation timeframe in which to address the standard (beyond first quarter 2006)? Also, a general comment that the standard requires a significant amount of diligence (especially in the tracking, authorization, and management of sensitive information) and will undoubtedly lead to staffing increases. Standard 1300 refers to certain sections (1302.1.1,1302.1.2, etc.) but no such section exists since the document appears to use a different section numbering scheme. Section 1302, Critical Cyber Assets. Section headings are out of sequence (a…g). Standard 1300, Cyber Security, Page 2. The items in the text box are not consistent with this standard (refers to Purchasing/Selling Entity which is not applicable, but omits Transmission Operator, etc.). Section 1303, under Requirements (1). It appears the phase, Responsible entity shall comply with the following requirements of this standard, should precede items 1 through 4, not be part of item 1. Section 1307, Incident Response Planning. The meaning of the acronym ESISAC should be stated. It would also be helpful to state how to access ESISAC. The formatting requirements to translate this data (for submission to NERC for this standard review) into a database are unreasonable. This commenting process must be designed to work effectively for the industry and not be hindered by special NERC formatting requirements. NERC indicates in the first paragraph of this form to submit comments with Version 0 in the subject line. That looks to be an error.

Western Area Power Administration Comment Form
Draft 1 of Proposed Cyber Security Standard (1300)

Question 1: Do you agree with the definitions included in Standard 1300:
No:

Comments:

Critical Cyber Assets definition. The later part of the first sentence, "such as…at a minimum," implies that all these assets perform critical bulk electric system functions which is not consistent with criteria in 1302 (for example, small generators). Removing it is recommended since specifics are addressed in 1302.

The definition of Critical Bulk Electric System assets in 1302 should also be modified by eliminating item (ii), item (B) under (iv), and item (vi). Including substation equipment in this standard is not workable for numerous reasons. NERC should establish a cyber security standard that will advance the cause of security AND be workable to implement. Substation equipment should be captured by utilities under item vii (risk-based assessment) as needed.

Need to include definitions of the terms: Owners, Custodians, and Users. It would be a good idea to include a definition of "Sensitive Information" or something similar that refers to "information pertaining to critical cyber assets…." The idea is to be more definitive about what information should be protected pursuant to 1301(a)(2).

For the definition of Incident, recommend the phrase "or could have lead to a disruption of" be removed. How would one measure/determine if it "could have" lead to a disruption? It would be interpreted differently by each entity.

For the definition of Incident, the phrase "or was an attempt to compromise" should be eliminated. This will be interpreted by each individual entity and may result in thousands of reports daily.

For the definition of Security Incident, recommend the phrases "are known to" and "or could have resulted in" be removed. They are vague and would be interpreted differently by each entity.

Responsible Entity. Since definitions are to be included in a separate glossary, rewording the last part of the sentence, "as identified in the Reliability Function table of the Standard Authorization Request for this standard," is suggested.

The definition of critical asset in 1302(a)(2) should be clarified. For example, one of the key determinants to whether a device is considered a critical asset is whether it uses a routable protocol. At the very least, what is considered a routable protocol should be defined in the glossary. Also, the and-or Boolean logic of this section is confusing. Possibly a decision tree chart would help clarify the logic.

Question 2: Do you believe this standard is ready to go to ballot?
No:

Comments:

NERC should utilize existing Cyber Security standards (see series 800, Computer Security) from the National Institute of Standards and Technology (NIST) that are already well-developed, tested, and recognized by GAO, OMB, and Federal sector, instead of having electric utility people create a whole new set of such standards. Since all Federal Government agencies are currently mandated to follow the NIST guidelines, the imposition of different NERC guidelines imposes an unnecessary redundant and burdensome level of documentation and audits that result in increased cost without a commensurate improvement in security.

Section 1302, Critical Cyber Assets, (a)(1). The standard is not clear whether the Largest Single Contingency for a Reportable Disturbance is specifically for the Entity or the Reserve Sharing Group (as an Entity may belong to a Reserve Sharing Group).

Question: The FAQ defines the MOST SEVERE SINGLE CONTINGENCY as the largest single generator in the system. Does this mean only a single generating unit and not a generating station? What about greater single contingency losses as represented by the transmission facilities (subs, high voltage lines) that carry aggregated power from multiple units in a single station and, therefore, carry more power

than any individual generators in a Reserve Sharing Group? Wouldn't those facilities then represent the most severe single contingency?

Section 1302, Critical Cyber Assets, (a)(2). The logistics for items A-E should be clarified; it is confusing.

Section 1302, Critical Cyber Assets, (a)(2). There should be more clarification/restatement of requirements for dial-up cyber assets that do and do not support routable protocols (what requires a physical perimeter and what does not, and what requires an electronic perimeter and what does not). Is there a typo in 1302(a)(2)(i)(D): it reads, "which do use a routable protocol," should is say "which do NOT use a routable protocol"?

All required minimum review periods should be a standard period of one year. Having so many review periods and having numerous periodicities is not practicable.

Under 1301(a)(3), the sentence that reads, "This person must authorize any deviation or exception from the requirements of this standard," should be changed to read, "The person that must authorize any deviation or exception from the requirements of this standard must be specified in the responsible entity's governance documentation."

In several places in the standard, the issue of authorized access and tracking that access is discussed. It is usually unclear if this is meant to include only those that have access with administrative privileges or if it extends to those that utilize the assets as users (dispatchers using an EMS, for example). One example of such a gray area can be found in 1301(a)(5)(ii), for example, but there are many such areas. NERC should not focus on access by those that only have rights to use the system, and should clarify in all such contexts that the reference is only to those with administrative access.

Section 1303, Measures (4)(iv), is one of many examples of too much proscriptive detail. All the background screening criteria should be altered/simplified to only say that a utility must have a policy related to the screening and must follow that policy and be able to show the records that the policy was followed.

Section 1303, Requirement (4), the phrase "prior to being granted unrestricted access to critical assets" should be removed since it conflicts with Section 1303, Measure (4)(iv).

This standard is an expansion to standard 1200 and has a direct related impact on implementation and resource requirements. It would be helpful if the implementation plan were provided.

Under 1301(d)(3)(ii), remove the word "and" at the end of the sentence.

Under 1301(e)(1), what is the difference between (iv) and (v)?

Under 1306(a)(2), please rephrase the second sentence, "The responsible entity must establish…," to make it clear.

Reference 1303, Personnel and Training (1)(2)(iv) - Training on recovery of critical cyber assets should be tied to the system or structure (Under NIST this is part of the Security Plan) and not general Cyber Security Awareness training. This comment also applies to 1308 Recovery Plans (a)(4).

Reference 1306, System Security Management (b)(2) - Please remove the following from the second sentence in that section "that all accounts comply with the password policy." There is no way to audit

whether account passwords comply with the password policy outside of cracking them. The only way to ensure that passwords comply with the password policy is to check for compliance on the front end when the user creates the password.

Question 3: Please enter any additional comments you have regarding Standard 1300 below:
Generally agree with the thoughts and principles behind the new standard; however, are concerned about the considerable expansion in the number and types of critical cyber assets, as well as the increased specificity throughout the standard. Will there be an expanded implementation timeframe in which to address the standard (beyond first quarter 2006)? Also, a general comment that the standard requires a significant amount of diligence (especially in the tracking, authorization, and management of sensitive information) and will undoubtedly lead to staffing increases.

Standard 1300 refers to certain sections (1302.1.1,1302.1.2, etc.) but no such section exists since the document appears to use a different section numbering scheme.

Section 1302, Critical Cyber Assets. Section headings are out of sequence (a…g).

Standard 1300, Cyber Security, Page 2. The items in the text box are not consistent with this standard (refers to Purchasing/Selling Entity which is not applicable, but omits Transmission Operator, etc.).

Section 1303, under Requirements (1). It appears the phase, "Responsible entity shall comply with the following requirements of this standard," should precede items 1 through 4, not be part of item 1.

Section 1307, Incident Response Planning. The meaning of the acronym ESISAC should be stated. It would also be helpful to state how to access ESISAC.

The formatting requirements to translate this data (for submission to NERC for this standard review) into a database are unreasonable. This commenting process must be designed to work effectively for the industry and not be hindered by special NERC formatting requirements. NERC indicates in the first paragraph of this form to submit comments with Version 0 in the subject line. That looks to be an error.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Dave Little and Bonnie Dickson	
Organization:	Nova Scotia Power Inc.	
Telephone:	902 428 7708	
Email:	david.little@nspower.ca	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☒ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

NSPI does not agree with definition in 1302.a.1. and recommends that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.

NSPI recommends that the definition of Critical Cyber Assets be;

Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).

The Incident definition should be changed from

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.

to

Incident: Any physical or cyber event that: disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
Overall Comments

We have reviewed the proposed 1300 standard and would like to start by complimenting the Standards Development Team for their hard work and for the professional product they have produced. We have also worked with our CEA (Canadian Electricity Association) and its members; and our NPCC associations/teams to create joint comments on this proposed standard for submission. We would, however, like to take this opportunity to directly comment on this proposed standard on behalf of our company. In this portion of our submission, we would like to make directional comments on this proposed standard and its implementation.

The first comment really speaks at the grass roots of this standard and how it should be interpreted and/or implemented.

Our industry is composed of companies that have very little in common except our product. Our location, our size, our construction, our position and impact on the grid all differentiate us one from another. The concept of singular standards is viable but the "across the board" application of them will not be a success without introducing the concept of variable risk. We believe that it is the responsibility of each entity to implement its own risk assessments (cyber/physical/HR) based on a continuum of risk that includes factors like geopolitical location/risks, architecture of infrastructure/systems/operations, and the impact that cyber/physical events can have on the bulk power systems, our customers and public good. We believe that these risk assessments are the domain of the responsible entity and should be the singular driving force to the application of all policies and standards including the NERC 1300 Standard. We, along with many of our industry partners, believe that standards should be implemented in accordance with an entity's real risks. This means that all measures; cyber, physical and human resource are to be subjugated to an entity's risk assessment. The phrase "in accordance with an entity's risk assessments" is notably absent in your standards and yet, ultimately, key to its success.

The second topic echoes many of the comments we have heard both directly from our associates but also over and over in your Web Conference in October. We are referring to the issues and continual discussions with regards to the definitions included in this proposed standard. The industry's preoccupation with these definitions just echoes how critical they are to the interpretation and eventual success of this standard. We endorse the concept of centralized definitions that this standard and others would depend upon to function. The creation of clear, concise centralized definitions would provide the bedrock upon which these and other standards could solidly be understood and applied.

We are including many other detail comments based on the 1300 proposed standards. These comments are organized section by section in the same manner as the proposed standard and make specific comment or recommended changes to the wording and interpretation of this proposed standard.

Standard 1300 is based on the definition of critical BES assets , (defined in 1302.a.1).
Per question 1, We do not agree with that definition and have made suggestions as to what the Drafting Team may do to address the issue.

Also we feel the need to change the Incident definition as shown in Question 1 is important.

Throughout the document, the compliance levels should be updated to measure the proposed revisions suggested below.

There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected with consideration of this Standard.

The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to guage the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. It is NPCC's hope that this will be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.

We are in general agreement with the intent of Section 1303, however a perscriptive approach to be applied to all entities regardless of size, geography etc. is not reasonable. Responsible entities should have more latitude in determining what is an acceptable level of risk and have made recommendations later in the form that will make this Section acceptable.
The term -background screening- has too many issues, we recommend that this section’s title become - Personnel Risk Assessment-.

As noted in previous comments NSPI supports the NERC decision to move away from monetary sanctions.

We would also like to express our concern over the significant incremental administrative tasks and documentation requirements to be compliant with this standard and hope the Standard Drafting Team will consider this during the development of the associated Implementation Plan.

We would like to thank you for entertaining our comments and look forward to the next release of this standard.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
General comments

Rework the numbering / letering of sub sections to be consistant between the sections. Example: all requirements and measures should start at 1.

Each page should have the subsection numbering as part of the header. Now one has to flip back several pages to see the section number, when searching the document.

1301
Request clarification on what "information" is protected in 1301.a.2.

Change 1301.a.2 from;
The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets. (some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)
to
The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets.

Change 1301.a.2.i from;
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.
to
The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well. (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)

Change 1301.a.3 from;
….entity's implementation of…
to
…entity's implementation and adherence of…

The 24 hours in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.

Change 1301.a.5.iv from;
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.
to

Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven business days for all other users of a change in user access status. All access revocations/changes must be authorized and documented. (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)

change 1301.b.5.i from;
5 days

to
7 calendar days (the 5 days may be not be sufficient time especially when considering holiday seasons)

In 1301.d.3.iv, request clarification that this -audit - applies to only audits on RS 1300, carried out by the compliance monitor

In 1301.d.3.ii, change from - address and phone number - to business contact information. Also on page 5, 1301.b.5.iii to ensure the protection of the identity/personal information of the affected individuals

Recommend that under Regional Differences, it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor

In 1301.e.1.iii, request clarification on -30 days of the deviation-. Also please explain the difference between -deviation and -exception. This does not match the FAQ 1301 Question 4.

In 1301.e.2.iii, change from;
An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or
to
An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or

Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change -Executive Management to -Senior Management- for consistency and clarity.

In 1301.e.4.xi, repeat of the earlier 24 hours if a user is terminated for cause or for disciplinary actions, or within 7 calendar days(should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).

1302
The Critical Bulk Electric System Assets section is too perscriptive in defining the included elements. We suggest that the focus should be on function and suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.
Replace the 1302 introduction and 1302.a.1 and 1302.a.2 as shown below, with;
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 which support the reliable operation of the bulk electric system.

The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.

(a) Requirements
Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.

(1) Critical Bulk Electric System Operating Functions and Tasks

The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks affected by cyber assets may include but are not limited to the following:

- monitoring and control
- load and frequency control
- emergency actions
- contingency analysis
- arming of special protection systems
- power plant control
- substation control
- real-time information exchange

(2) Critical Cyber Assets

(i) In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:

A) The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.

B) The consequences of the Operating Function or Task being compromised (i.e. “highjacked”) for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.

C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.

D) Known risks associated with particular technologies

Change 1302.g.1 from;
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.
to
1 Critical Bulk Electric System Operating Functions and Tasks
(i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1.

Change 1302.g.2.i from;
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.
to
The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure.

Change 1302.g.5 from;
Critical Bulk Electric System Asset and Critical Cyber Asset List Approval
to
Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval (it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations is lost.)

Change 1302.g.5.i from;
A properly dated record of the senior management officer's approval of the list of critical bulk electric system assets must be maintained.
to
A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained.

Change 1302;
critical bulk electric system assets
to
critical bulk electric system operating functions and tasks

1303,
We agree with the intent of Section 1303. The term - background screening- however has too many issues, we recommend that this section's title become - Personnel Risk Assessment. Portions of 1303 are too prescriptive, the responsible entity should have more latitude in determining what is an acceptable level of risk.

The FAQ describes supervised access, 1303 does not touch upon this topic. Change 1303.a.4 from -unrestricted access- to -authorized access. Change 1303.a.4 title to -Personnel Risk Assessment. Change 1303.a.4 to -A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks.

Change 1303.a.2 from;

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.
to
The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets

1303.a.4 from;
(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.
to
(4) Personnel Risk Assessment: There must be a documented company personnel risk assessment process.

Add to 1303 Measures.2, a training measure section for disaster recovery (1308) and incident response planning (1307).

The numbering of 1303 starting with Measures needs correction.

1303 Measures 4.i, request clarification. Does this include third party personnel?

Change 1303.Measures.4.i from;

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).
to
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 respective security perimeter(s).)." (there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)

Change 1303.Measures.4.ii from
two business days
to
seven calendar days, per earlier comments and keep consistent with FERC Order.

1303.Measure.4.iii, change -24 hours- to -24 hours if terminated with cause or diciplinary action, or seven days-, per earlier comments

1303.Measure.4., remove;
Subsections iv, v and vi.
and replace with
There must be a documented company personnel risk assessment process." NPCC's participating members feel these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities.

1303.Compliance Monitoring Process.2, We do not agree with -background screening documents for the duration of employee employment. and suggest changing the last bullet in (i) to - Verification that Personnel Risk Assessment is conducted.

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change 24 hours to be consistent with earlier comments. Change personnel termination to personnel change in access status .

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of Background investigation program exists, but consistent selection criteria is not applied, or to Personnel risk assement program is practiced, but not properly documented, or

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to Personnel risk assement program exists, but is not consistently applied, or

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to Personnel risk assement program does not exist, or

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from two days to 24 hours with cause or seven days (as mentioned earlier). Change personnel termination to personnel change in access status .

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to Access control list exists, but is incomplete.

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from two days to 24 hours with cause or seven days (as mentioned earlier). Change personnel termination to personnel change in access status.

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from cover two of the specified items to cover two or more of the specified items.

Correct the identation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii

1304
1304 a.2 Electronic Access Controls:
The responsible entity shall implement a combination of organizational, add and/or technical, add and/or 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).

1304 a.3 Monitoring Electronic Access Control:
The responsible entity shall implement a combination of organizational,again add and/or technical, add and/or procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized

Change 1304 a.4 from;
The responsible entity shall ensure that all documentation reflect current configurations and processes.
to
The responsible entity shall ensure that all documentation required comply with 1304 a 1 through 1304 a.3 reflect current configurations and processes.

1304 a.4 Remove -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. (This is a measure and should be removed here)

Compliance Monitoring Process;
Change 1304.d.3 from;
The responsible entity shall make the following available for inspection by the compliance monitor upon request:
to
The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:

Level of non compliance
Level three-Supporting documents exist, but not all transactions documented have records - this part is ambiguous and should be clarified.

1305 Physical Security;
Eliminate the bulleted items in the Preamble to Section 1305-they appear in the Requirement section.

Replace 1305 a.1 with Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.
• The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),
• The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and
• The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets.

Change the following - (a) Requirements;
(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.
to

(3) Physical Access Controls: The responsible entity shall implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.
(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.
(5) (We recommend deleting this bullet as the intent is captured in bullet "4").
(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity.

Change Measures;
(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.
to
The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility.(the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)

1306
In 1306.a.1, last paragraph, modify the second sentence to read as follows;
Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible.

1306.a.2.ii remove Generic from the title

1306.a.2.iii, use at least annually instead of at least semi-annually

Change 1306.a.3 from;
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
to
A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets. ." (upgrades are a subset of the applicable security patches.)

Remove the last sentence in 1306.a.3, In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented.

Change 1306.a.4 from;
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.
to

A formally documented process governing mitigation of the importation of malicious software into critical cyber assets.

1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).

Change 1306.a.6 from
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.
to
It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three years in an exportable format, for possible use in further event analysis.

1306.a.7 Remove Configuration Management from the Title

1306.a.8 Remove the word inherent it is not clear what is meant by it.

1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.

1306, remove 1306.a.11 since 1308 addresses back-up and recovery.

1306.b.1, remove Test procedures must also include full detail of the environment used on which the test was performed. Also replace potential with known in the last sentence. Also in the last sentence insert the words if possible at the end of the sentence.

1306.b.2, instead of 24 hours use the above wording on 24 hours for cause, or seven days.

1306.b.3, remove;
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.

and change
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.
to
The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability.

In 1306 b.3 first sentence-eliminate the word management

1306.b.4, remove anti-virus, anti-Trojan, and other from the first sentence.

1306.b.4 third sentence Change
..so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware.

to
..mitigate risk of malicious software.

1306.b.4 Remove the second sentence.

1306.b.4 Replace the fourth sentence with;
Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented.

1306.b.5 remove the first sentence.
Based on the common use of third parties for outsourcing of this associated work of vulnerabilty assessment, it is not reasonable to maintain the information called for in sentence one.

Change 1306.b.6 from;
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.
to
Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three years in an exportable format, for possible use in further event analysis.

1306.b.7 In the final sentence remove the word all and change the heading by deleting and Configuration Management

Remove 1306.b.11, since 1306.a.11 was removed.

1306.d.2, change from The compliance monitor shall keep audit records for three years. to The compliance monitor shall keep audit records for three calendar years

1306.d.3.iii, change system log files to audit trails

1306.e.2, change the monthly/quarterly reviews to the reviews

1306.e.2.ii.C, change anti-virus to malicious

1306, the Compliance levels should be updated to match the above measures.

1307
1307, spell out and provide clarification on the acronyms throughout.

1307.d.1 there is a 90 day reference that does not appear in the measures.

Change 1307, from;
Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified.
to
Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified.

1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard.
Change from;
Incident and Cyber Security Incident Reporting
to
Security Incident Reporting.

and also Change from;
The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP).
to
The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP).

Refer to our definition of a security incident .

Change 1307.b.5 from;
The responsible entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and cyber security incident reporting requirements.
to
The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements.

Change 1307.b.6 from The responsible entity shall retain records of incidents and cyber security incidents for three calendar years
to
The responsible entity shall retain records of security incidents for three calendar years

Change 1307.b.7 from The responsible entity shall retain records of incidents reported to ESISAC for three calendar years.
to
The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years

1308
In 1308, to remain consistent with the scope of Critical Cyber Assets, it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.

Following this concept, the third paragraph in the 1308 preamble should be removed. The requirement for a Backup Control Centre is covered by other NERC Standards. The topic is well outside the scope of this document and does not belong in a Cyber Security Standard.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Kathleen M. Goodman	
Organization:	ISO New England Inc.	
Telephone:	(413) 535-4111	
Email:	kgoodman@iso-ne.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☒ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☒	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Comments Bulk Electric System Asset – There are too many different definitions being used by various groups. BES should not be defined in a cyber security standard. It should make reference to a standard definition provided elsewhere. The lack of one standard definition elsewhere does not justify it here. NERC must address this.

The use of the term "attempt" in the basic incident description implies "malicious activity." Suggest rewording as follows:

Incident: Any physical or cyber event that disrupts or compromises the functional operation of a critical cyber asset and/or the security perimeters.

Security Incident: Any malicious or suspicious activity that is known to have caused an incident.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
No. There are too many inconsistencies in structure of the document, in the use of terms such as "monitoring", what is meant by audit data, etc. Also inconsistent between Requirements, Measures, Monitoring, and Non-compliance. The current draft requires significant clarification and re-write. This includes putting more focus on risk assessment in identifying critical BES functions and tasks, and security solutions to protect critical cyber assets.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

GENERAL COMMENTS:
1. Numbering system is not consistent throughout document. Makes referencing difficult for providing comments.
2. Identification of the compliance monitor is not clear. Is this NERC, Regional Management, or the Regional Reliability Operators. Could this be made clearer in the standard?
3. Several references appear to "reliability" and/or "operability." Unless there is a meaningful distinction between the two, you should drop references to "operability."
4. The 1300 standard must be very clear in that it does not mandate what department within a responsible entity is accountable for security training and/or background screening, and related records management.
5. Compliance Monitoring -- identify specific data that is kept for three years. Need to provide clarification to indicate the meaning of audit results, which we believe means compliance with the NERC 1300 standard and not other audits. For (3)'s, please state clearly that this is to be done with respect to applicable confidentiality agreements in place. This information can be highly sensitive. These need to be clarified in all sections 1301 through 1308.

1301 PREAMBLE:
The role/description of "Monitoring," as presented in the FAQ should be added directly to the standard in 1301 as a governance requirement of the responsible entity. Reference FAQ page 2, sub-header Monitoring.
(This is recognized to be different from the role of the NERC/Regional Compliance Monitor, which is defined independently.)

1301 REQUIREMENTS:

(2) Information Protection:
Rewrite as: "…protection of critical information pertaining … "
(i) Identification - Disaster Recovery/Business Continuity plans should also be protected at a minimum
(ii) Classification - The use of unauthenticated personnel is anomalous to the rest of the document. Unauthorized is a better term. Even some authenticated personnel may not necessarily be authorized.
(iii) Protection - Where are differing classification levels defined?

(3) Roles and Responsibilities
Where is 1.2?

(5.iv) 24-hour requirement is unrealistic in most cases. Requirement should be within 24 hours for facility and remote access for terminations with cause or other disciplinary action. Next Business Day for all other access.

(6) Authorization to Place Into Production
Needs to be worded to be specific to placing Critical Cyber Asserts Into Production.

1301 MEASURES:

(2) Information Protection:
Remove the use of the word “security” and “secure” and only use “protection” or “protect.”

(5) Access Authorization –
(i) Seems to speak about critical cyber “information” but the last word refers to “assets.” Should the last word in the sentence be “information?” Also, change 5 days to seven days.
(ii) Reviewing of user access rights every quarter is excessive. We recommend annually on revalidation.
(6) Authorization to Place Into Production
Needs to be worded to be specific to placing Critical Cyber Asserts Into Production. Also, change 48 hours to seven days.

1301 Compliance Monitoring

(2) identify specific data that is kept for three years This needs to be clarified in all sections 1301 through 1308.

(3.iv) This should provide clarification to indicate the meaning of audit results which we believe means compliance with the NERC 1300 standard and not other audits. This needs to be clarified in all sections 1301 through 1308.

1301 Levels Noncompliance
(1.iii) Request clarification on "30 days of the deviation." Also, please explain the difference between "deviation" and "exception." This does not match the FAQ 1301 Question 4.

1302 PREAMBLE:
There is great concern that reference to bulk electric system assets, and those assets deemed critical, is addressing the physical security of those assets. This must be clarified as physical security of BES assets does NOT belong in a cyber security standard.

Suggest rewriting as:
“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 which support the reliable operation of the bulk electric system.

“The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.”

1302 Requirements:
This paragraph would be clearer if it were rephrased. By commencing with the first sentence, it could be interpreted that the standard may be intending to speak to protection methods around bulk electric systems when it is only the cyber systems. If the second sentence was stated first, this would be clearer.

Suggest rewriting as:

"Responsible entities shall identify their Critical Cyber Assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard."

(1) Rewrite as:
"(1) Critical Bulk Electric System Operating Functions and Tasks
The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system operating at the levels of 115 kV and above. Critical operating functions and tasks affected by cyber assets may include but are not limited to the following:
- monitoring and control
- load and frequency control
- emergency actions
- contingency analysis
- arming of special protection systems
- power plant control
- substation control
- real-time information exchange"

(2) Critical Cyber Assets:
Rewrite as:
"In determining the set of Critical Cyber Assets, responsible entity will incorporate the following in its preferred risk assessment procedure:
- The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.
- The consequences of the Operating Function or Task being compromised (i.e. "high-jacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.
- Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.
- Known risks associated with particular technologies."

The criteria nesting/indents is confusing. Rephrase to read as:
(i) The responsible entity shall identify cyber assets to be critical using the following criteria:
B) The cyber asset supports a critical bulk electric system asset, and
i) the cyber asset uses a routable protocol, or
ii) the cyber asset is dial-up accessible.
C) 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.

(3) The terms "senior management" and "officer" have legal meaning in companies. This should be clarified throughout the standard.

1302 Measures:
(1) Rewrite as:
"(1) Critical Bulk Electric System Operating Functions and Tasks
(i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.Requirements.1."

(2) Rewrite as:
"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its Critical Cyber Assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure."

(5) Change title to: "Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval"
(5.i) through (5.ii) This should read as, senior Operating System Manager

1303 Preamble:
The 1300 standard must be very clear in that it does not mandate what department within a responsible entity is accountable for security training and/or background screening, and related records management.

1303 Requirements:
Remove the word "unrestricted." It is possible to grant unsupervised access with some restrictions.

(2) Training:
Include disaster recovery (re; 1308.a.4) as training requirement

(4) Background Screening
(4.i) through (4.ii) these have nothing to do with performing background screening – Remove.
(4.iii) What does this have to do with conducting/documenting background screening? Otherwise, see previous 1301.Requirements.5.iv -- 24-hour requirement is unrealistic in most cases. Requirement should be within 24 hours for facility and remote access for terminations with cause or other disciplinary action. Next Business Day for all other access.
(4.iv) through (vi) which is attempts to legislate employment practices and is too overreaching -- e.g., it states that we must discipline consistently and comport with our collective bargaining agreements. These are not appropriate subjects for a NERC standard. Likewise for the specifics on background checks, which are sensitive and subject to various laws (including the Fair Credit Reporting Act). We prefer not to see potentially conflicting standards established here.

1303 Levels Noncompliance
(1.ii) - ...access control list was not updated within 2 business days - completely different requirement - where did 2 business days come from? This needs to align more closely with the previous benchmark of "24 hours" and escalate based on this benchmark.

(2.ii) - ...access control list was not updated within 2 business days - completely different requirement - where did 2 business days come from?

(3.ii) - ...access control list was not updated within 2 business days - completely different requirement - where did 2 business days come from?

1304 Preamble
no requirement to view logs or "be alerted" as mentioned in the FAQ (page 10, question 6 "monitor access....and to be alerted so you can respond). Does monitor mean just mean logged, or viewed and acted upon, as necessary? Need better clarification of term "monitoring."

1304 Compliance Monitoring
Please state clearly that this is to be done with respect to applicable confidentiality agreements in place. This information can be highly sensitive.

1305 Preamble
Second bullet should explicitly state "Critical Cyber Asset" …
Throughout 1305, the use of tables, lists, and examples is both confusing and too restrictive. As a standard, if those are the only identified, then other equitable solutions are not allowed by exclusion. Remove all tables, lists, and examples, to allow appropriate risk management decisions.

1305 Measures:
(4) Should not report back to the EMS Dispatcher. The primary functions of our system operators should not be impaired by requiring them to be security guards, as we have all learned all too well in the blackout, a power system degrade and collapse can happen within seconds. Their job is grid reliability, not manage cyber security.
(5) Do not mandate all these logs. The Logs required should be consistent with the risk assessment based solution implemented.

1305 Levels Noncompliance
(2.i) Strikeout reviewed last six months. Requirement is for 90 day update, annual review.

1306 Requirements
(1) Remove. Change Management is a separate process from System Management. This belongs in (7) Change Control.

(2) Remove the words "end user," as being too exclusive.
(2.i) Remove 2nd sentence and examples.
(2ii) Remove "Generic" from title.
(2.iii) This is inconsistent with 1301.b.5.v -- Reviewing of user access rights every quarter or semi-annually is excessive. We recommend annually on revalidation.

(3) Security Patch Management - remove "upgrades," upgrades are a different animal and beyond the scope of security patch management.

(4) Integrity Software - Change the word "application" to "use."

(5) Reword write as:
At a minimum, a vulnerability assessment shall be performed at least annually that includes a diagnostic review of the access points to the electronic security perimeter. The responsible entity will implement a documented management action plan for remediation of vulnerabilities and shortcomings, if any, identified in the assessment.

(6) Retention of System Logs - Need clarification of what logs. Recommend only requiring the minimum baseline of firewall, IDS, and OS System Logs. Trying to specify further can cause conflicts with differing hardware and software platforms, which may require too many exceptions. No reference should be made to application logs.

(7) Remove "and Configuration Management." This is where you address testing. Within NERC and Critical Cyber Asset scope, this is limited to those Critical Cyber Assets.

(8) Rewrite as:
The responsible entity shall disable unused ports and services.

(10) Remove this section. Status of performance/efficiency is not a cyber security concern. This was resolved in the 1300 SAR.

(11) Remove. This should be addressed in one place, in 1308.

1306 Measures
(1) Remove section.
(2) Must review access permissions within 5 working days - yet another requirement that does not agree with 1301.a.5.iv, 1303.b.4.iii, etc. It is not reasonable to expect a manager to sit at a terminal or otherwise review all access permissions. Management must "ensure" the review.

(7) Remove " … and Configuration Management" from title.
(8) Rewrite last sentence as: "Documentation shall verify that the responsible entity has taken the appropriate actions to secure ports and network services."

(10) Remove section.
(11) Remove section – see 1308.

1306 Levels Noncompliance
(2) Bullet/numbering is confusing. More clarity is required around these specific reviews.
(3) Bullet/numbering is confusing. More clarity is required around these specific reviews.
Date/time requirements not consistent through out standard.
(3.vii) These specific logs have not been referred to previously in this section of the standard. Recommend only requiring the minimum baseline of firewall, IDS, and OS System Logs. Trying to specify further can cause conflicts with differing hardware and software platforms, which may require too many exceptions. No reference should be made to application logs.

1307 Preamble
… must be monitored on a continuous basis - different terminology - previously used 24 hours a day, 7 days a week Need to clarify and be consistent through standard. Remove "or cyber security incidents" from last sentence.

1307 Requirements
Rewrite/remove a few words in this section to clarify:
"(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 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) 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) Security Incident Reporting: The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis & Warning Program (IAW) Standard Operating Procedure (SOP)."

(4) What is the IAW SOP? Needs more explanation. If it is some other standard, NERC standard process does not allow cross referencing.

1307 Measures
(6) Rewrite as "The responsible entity shall retain records of incidents for three calendar years."
(7) Rewrite as: "The responsible entity shall retain records of security incidents reported to ES-ISAC for three calendar years."
(7) ESISAC - Who is this, spell it out - also abbreviation is not used consistently. Is it ESISAC or ES-ISAC?

1307 Compliance Monitoring
(2) Remove words " … and cyber security … "
(2.v) Replace "reportable" with "security"

1308 Preamble
1. This introduction is repetitive and redundant. It could be shortened to one paragraph and still be effective.
2. To remain consistent with the scope of "Critical Cyber Assets," it should be more clearly stated that this section only speaks to the operative recovery of those Critical Cyber Assets.

1308 Requirements
(3) What does "post" mean? This information could be considered confidential, protected, etc, etc...

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	A. Ralph Rufrano	
Organization:	NYPA	
Telephone:	(914) 681-6265	
Email:	rufrano.r@nypa.gov	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☒ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

NPCC's participating members recommend that the definition of Critical Cyber Assets be;

"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).

NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.

NPCC's participating members recommend changing the Incident definition from

"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."

to

"Incident: Any physical or cyber event that:

disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?

NPCC's participating members feel there is much redrafting to be done to the standard and that the following items may be considered "show stoppers" by some.

Standard 1300 is based on what the critical BES assets are, which is defined in 1302.a.1. Per question 1, NPCC's participating members do not agree with that definition and have made suggestions as to what the Drafting Team may do to address the issue.

NPCC's participating members also believe the need to change the Incident definition, to the one shown in Question 1 is important.

As previously discussed and commented on in various forums, NPCC supports the NERC decision to move away from monetary sanctions.

NPCC's participating members have also expressed concern over the incremental administrative tasks and documentation requirements to be compliant with this standard and hopes the Standard Drafting Team will consider this during the development of the associated "Implementation Plan".

Throughout the document, the compliance levels should be updated to measure the proposed revisions suggested below. NPCC has made some recommendations in this regard.

There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected and recognized with consideration of this Standard.

The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to gauge the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. It is NPCC's hope that this will be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.

NPCC’s participating members agrees with the intent of Section 1303. The term “background screening” however has too many issues for NPCC participating members and recommend that this section’s title become “Personnel Risk Assessment”. Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk and have made recommendations later in the form that will make this Section acceptable.

The references within the standard made to other portions of Standard 1300 are not correct. Without clear references, NPCC cannot determine if the document is acceptable or not. For

example, 1301.a.3 says "as identified and classified in section 1.2." Where is this section? Each one of these incorrect references must be corrected.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

Correct references as covered in question 2.

Request clarification on what "information" is protected in 1301.a.2.

Change 1301.a.2 from;

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

to

"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets." (NPCC's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)

Change 1301.a.2.i from;

"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."

to

"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well." (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)

Change 1301.a.3 from;

"….entity's implementation of…"

to

"…entity's implementation and adherence of…"(NPCC's participating members believe it is important to stress that not only is it important to implement this Standard but to adhere to it as well.

The “24 hours” in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.

Change 1301.a.5.iv from;

"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."

to

"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven calendar days for all other users of a change in user access status. All access revocations/changes must be authorized and documented." (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)

change 1301.b.5.i from;

"5 days"

to

"7 calendar days" (NPCC's participating members believe that the 5 days may be not be sufficient time especially when considering holiday seasons)

1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency in the reference for retention of audit records.

1301.d.3.iv, request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor

1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii to ensure the protection of the identity/personal information of the affected individuals

Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor

1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.

1301.e.2.iii, change from;

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

to

"An authorizing authority has been designated but a formal process does not exist to

test, validate and deploy systems into production, or" (NPCC believes it was the drafting team's itent to deploy the system rather than promote which has a different connotation associated with it,)

Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change "Executive Management" to "Senior Management" for consistency and clarity.

1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).

NPCC Participating Members believe that the concept of the Bulk Electric System and association "definitions" may not be appropriate to capture the intent of the standard. NPCC suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.

Replace the 1302 preamble and 1302.a.1 and 1302.a.2 as shown below, with;

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 which support the reliable operation of the bulk electric system.

The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.

(a) Requirements
Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.

(1) Critical Bulk Electric System Operating Functions and Tasks

The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:

- monitoring and control
- load and frequency control
- emergency actions
- contingency analysis
- arming of special protection systems
- power plant control
- substation control
- real-time information exchange

(2) Critical Cyber Assets

(i) In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:

A) The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.

B) The consequences of the Operating Function or Task being compromised (i.e. “highjacked”) for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.

C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.

D) Known risks associated with particular technologies

Change 1302.g.1 from;

"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."

to

"1 Critical Bulk Electric System Operating Functions and Tasks
(i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."

Change 1302.g.2.i from;

"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."

to

"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure." (NPCC believes the use of the word additional is of no value as used here and recommends removal).

Change 1302.g.5 from;

"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"

to

"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval" (NPCC believes that it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations of operations is lost.)

Change 1302.g.5.i from;

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

to

"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."

Change 1302;
"critical bulk electric system assets"

to

"critical bulk electric system operating functions and tasks"

1303, NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for the NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk.

The FAQ describes supervised access, 1303 does not touch upon this topic.

Change 1303.a.4 from "unrestricted access" to "authorized access".

Change 1303.a.4 title to "Personnel Risk Assessment."

Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."

Change 1303.a.2 from;

"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."

to

"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"

1303.a.4 from;

"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."

to

"Personnel Risk Assessment: There must be a documented company personnel risk assessment process."

Add to 1303 Measures.2, a training measures for disaster recovery (1308) and incident response planning (1307).

The numbering of 1303 starting with Measures needs correction.

1303 Measures 4.i, request clarification. Does this include third party personnel?

Change 1303.Measures.4.i from;

"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)."

to

"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 respective security perimeter(s)." (NPCC believes there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)

Change 1303.Measures.4.ii from;

"two business days"

to

"seven calendar days", per earlier comments and to keep consistent with FERC Order.

1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days", per earlier comments

1303.Measure.4., remove;

Subsections iv, v and vi.

and replace with

"There must be a documented company personnel risk assessment process." NPCC's participating members feel these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities."

1303.Compliance Monitoring Process.2, NPCC's participating members do not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria
is not applied, or" to "Personnel risk assement program is practiced, but not properly documented, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."

Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii

From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.

Change 1304 a.2 Electronic Access Controls:
to

"The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" 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)."

Change 1304 a.3 Monitoring Electronic Access Control:
to
"The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."

Change 1304 a.4 from;

"The responsible entity shall ensure that all documentation reflect current configurations and processes."

to

The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.

1304.a.4 Remove -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. (This is a measure and should be removed here)

Compliance Monitoring Process;
Change 1304.d.3 from;

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

to

"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"

Level of non compliance
"Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.

1305 Physical Security;

Eliminate the bulleted items in the Preamble to Section 1305-they appear in the Requirement section.

Replace 1305 a.1 with;
"Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.
• The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),

• The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and
• The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."

Change the following - (a) Requirements;
"(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."

to

"(3) Physical Access Controls: The responsible entity shall implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.
(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.
(5) (We recommend deleting this bullet as the intent is captured in bullet "4").
(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."

Change Measures;

"(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."

to

"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility." (NPCC believes the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)

In 1306.a.1, last paragraph, modify the second sentence to read as follows;

"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."

1306.a.2.ii change "pooding" and "puffing" to "putting" (it appears a pdf translation problem as some documents the group printed have it and others did not)

1306.a.2.ii remove "Generic" from the title

1306.a.2.iii, use "at least annually" instead of "at least semi-annually"

Change 1306.a.3 from;
"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."

to

"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets." (NPCC believes that it upgrades are a subset of the applicable security patches.)

Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."

Change 1306.a.4 from;

"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."

to

"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."

1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).

Change 1306.a.6 from

"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."

to

"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three calendar years in an exportable format, for possible use in further event analysis."

1306.a.7 Remove "Configuration Management" from the title

1303.a.8 Remove the word "inherent" it is not clear what is meant by it.

1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.

1306, remove 1306.a.11 since 1308 addresses back-up and recovery.

1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.

1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days".

1306.b.3, remove;

"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."

and change

"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."

to

"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."

1306 b.3 first sentence-eliminate the word "management".

1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.

1306.b.4 third sentence Change
"..so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."

to

"..mitigate risk of malicious software".

1306.b.4 Remove the second sentence.

1306.b.4 Replace the fourth sentence with;

"Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."

1306.b.5 remove the first sentence.
Based on the common use of third parties for outsourcing of this associated work of vulnerabilty assessment, it is not reasonable to maintain the information called for in sentence one.

Change 1306.b.6 from;

"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."

to

"Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis."

1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"

Remove 1306.b.11, since 1306.a.11 was removed.

1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."

1306.d.3.iii, change "system log files" to "audit trails"

1306.e.2, change "the monthly/quarterly reviews" to "the reviews"

1306.e.2.ii.C, change "anti-virus" to "malicious"

1306, the Compliance levels should be updated to match the above measures.

1307, spell out and provide clarification on the acronyms throughout.

Change 1307, from;

"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."

to

"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."

1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;

"Incident and Cyber Security Incident Reporting"

to

"Security Incident Reporting".

and also Change from;

"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

to

"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

Refer to our definition of a "security incident", change 1307.b.5 from;

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

to

"The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements."

Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."

to

"The responsible entity shall retain records of security incidents for three calendar years."

Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."

to

"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."

1307.d.1 there is a 90 day reference that does not appear in the measures.

In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.

Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	David Kiguel	
Organization:	Hydro One Networks Inc.	
Telephone:	416-345-5313	
Email:	David.Kiguel@HydroOne.com	
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT** ☐ **ECAR** ☐ **FRCC** ☐ **MAAC** ☐ **MAIN** ☐ **MAPP** ☒ **NPCC** ☐ **SERC** ☐ **SPP** ☐ **WECC** ☐ **NA - Not Applicable**	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☒	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name: Hydro One Networks Inc.

Lead Contact: **David Kiguel**

Contact Organization: **Hydro One Networks Inc.**

Contact Segment: **1**

Contact Telephone: **416-345-5313**

Contact Email: **David.Kiguel@HydroOne.com**

Additional Member Name	Additional Member Organization	Region*	Segment*
Ian Bradley	**Hydro One Networks Inc.**	**NPCC**	**1**
Mike Penstone	**Hydro One Networks Inc.**	**NPCC**	**1**
Chris Price	**Hydro One Networks Inc.**	**NPCC**	**1**
Dave Baumken	**Hydro One Networks Inc.**	**NPCC**	**1**
Andy Poray	**Hydro One Networks Inc.**	**NPCC**	**1**

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Hydro One Networks Inc. (Hydro One) recommends that the definition of Critical Cyber Assets be:

"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange such that the loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets." (We recommend this definition be used in 1302).

Hydro One does not agree with the definition of Critical Bulk Electric System Assets in 1302.a.1. We recommend that NERC creates a Glossary of Definitions that the NERC Standards can reference. This Glossary should be the sole depository of definitions used by all Standards. Definitions such as this and others used in the standards are a matter that should be addressed by a definitions team/committee where input from stakeholders in the industry is obtained and final approval by the BOT is required for their usage.

Hydro One recommends changing the Incident definition from

"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."

to

"Incident: Any physical or cyber event that disrupts, or could lead to a disruption of the functional operation of a critical cyber asset."

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?

The items listed below are what Hydro One would consider show stoppers in the balloting of the Standard.

Standard 1300 is based on what are the critical BES assets, which is defined in 1302.a.1. As stated in our response to question 1, Hydro One does not agree with that definition and have made suggestions as to what may the Drafting Team may do to address the issue.

Hydro One believes that the concept of the Bulk Electric System and associated "definitions" used in the development of the Standard may not be appropriate to capture its intent. We suggest substantive changes as shown in question 3. We strongly believe that the Standard is to be based on the the concept of "Critical Functions and Tasks" that relate to the inter-connected transmission system. Each Responsible Entity should then define and use a Risk Assessment approach to:
(a) identify Critical BES facilities;
(b) identify what Cyber Assets are located within those BES facilities; and
(c) identify what assets in (b) are critical.

The Risk Assessment approach should be based on the degree of degradation in the performance of critical BES operating tasks.

We also feel the need to change the Incident definition as shown in Question 1 is important.

The references made within the Standard to other portions of 1300 are not correct. Without clear references, it is not possible to decide whether the document is acceptable or not. For example, 1301.a.3 says "as identified and classified in section 1.2." Where is this section? Every one of these incorrect references needs to be corrected.

Throughout the document, the Compliance levels should be updated to measure revisions we suggest below.

There should be a statement in the Standard that reflects:
(a) all applicable confidentiality agreements obligations;
(b) entity's disclosure of information policies; and
(c) regulatory and legal obligations regarding Confidential Information.

The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard 1200. In order to assess the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. This should be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.

While we agree with the intent of Section 1303, the use of the term "background screening" however has too many issues and we recommend that this section's title become "Personnel Risk Assessment." Portions of 1303 are too prescriptive and our position is that that the responsible entity should have more latitude in determining what is an acceptable level of risk. We have made recommendations later in the comment form that will make this Section acceptable.

As previously discussed and submitted with our comments to other standards, Hydro One supports NERC decision to move away from monetary sanctions, and would like to again emphatically state that Hydro One does not support monetary sanctions.

Hydro One is also concerned about the incremental administrative tasks, documentation requirements and capital expenditures that may be required to support compliance with the 1300 standard. We expect the Drafting Team will consider the associated costs during the development of the associated Implementation Plan.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
1. Priority 1 (show stoppers)

Hydro One believes that the concept of the Bulk Electric System and associated "definitions" may not be appropriate to capture the intent of the standard. We suggest the substantive changes as shown below to address this issue using the concept of Critical Functions and Tasks that relate to the inter-connected transmission system, using a Risk Assessment approach to be defined by the responsible entity.

Consistent with the above, we recommend to replace the 1302 introduction and 1302.a.1 and 1302.a.2 as shown below.

"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 which support the reliable operation of the bulk electric system.

The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.

(a) Requirements
Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.

(1) Critical Bulk Electric System Operating Functions and Tasks

The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks affected by cyber assets may include but are not limited to the following:

- monitoring and control
- load and frequency control
- emergency actions
- contingency analysis
- arming of special protection systems
- power plant control
- substation control
- real-time information exchange

(2) Critical Cyber Assets

(i) In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:

A) The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.

B) The consequences of the Operating Function or Task being compromised (i.e. “highjacked”) for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.

C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.

D) Known risks associated with particular technologies."

Change 1302.g.1 from

"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."

to

"1 Critical Bulk Electric System Operating Functions and Tasks
(i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."

Change 1302.g.2.i from

"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."

to

"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure."

Change 1302.g.5 from

"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"

to

"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval"

Change 1302.g.5.i from

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

to

"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."

In 1302, change

"critical bulk electric system assets"

to

"critical bulk electric system operating functions and tasks."

1303:
Hydro One agrees with the intent of Section 1303. However, the term “background screening” has too many issues and we recommend that this section’s title become “Personnel Risk Assessment”. Portions of 1303 are too prescriptive and the responsible entity should have more latitude in determining what is an acceptable level of risk.

On background screening, "Social Security Number (SSN)" is a unique identification number used strictly in the United States. The Canadian equivalent to it is "Social Insurance Number (SIN)". However, Canadian law prescribes SIN to be used specifically for income tax purposes only, and for nothing else. Hence, the use of SSN or SIN in the standard is inappropriate. We recommend the re-phrasing of Section 1303, b, (4), (iv) as:
"The responsible entity shall conduct background screening of all personnel prior to being granted access to critical cyber assets. A minimum of an appropriate identity verification and a criminal check with a seven year retrospective scope are required. Entities may conduct more detailed reviews depending upon the criticality of the position. Update screening shall be conducted at least every five years, or for cause. These requirements are subject to all applicable laws, and to existing collective bargaining unit agreements. "
Hydro One supports the notion of applying for a waiver, in case the entities fail to reach an agreement on background checks with bargaining units. However, at the same, we support providing a proof of efforts by the entities to reach agreements in the next contract negotiation. Additionally, Canadian entities are tightly constrained as to any forms of drug testing. Hence, CEA member would have difficulty supporting any move in the current and future standards to include drug testing, except for just cause.

Change 1303.a.4 title to "Personnel Risk Assessment."
Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."

---

2. Medium Priority (Important)

Change 1301.a.2 from

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

to

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

Change 1301.a.2.i from

"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."

to

"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centres, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well."

Change 1301.a.5.iv from

"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."

to

"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven business days for all other users of a change in user access status. All access revocations/changes must be authorized and documented."

In 1301.d.3.iv, we request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor. No other audits are to be addressed by Standard 1300.

We recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process and therefore each Region is responsible for designating the Compliance Monitor
---

1304 a.2 Electronic Access Controls:
The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" 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).

1304 a.3 Monitoring Electronic Access Control:
The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized
---

1303.Compliance Monitoring Process.2, we do not agree with "background screening documents for the duration of employee employment." Change the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."

Change 1303.a.2 from

"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."

to

"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets."

In 1303.Measures.4.iii, change "24 hours" to "24 hours if terminated with cause or diciplinary action, or seven days otherwise", per earlier comments
---

Remove iv, v and vi. Replace with "There must be a documented company personnel risk assessment process."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven days otherwise" (as mentioned earlier). Change "personnel termination" to "personnel change in access status."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Compliance Monitoring Process

Change; 1304 d.3
The responsible entity shall make the following available for inspection by the compliance monitor upon request:

to

The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements and obligations:

Replace 1305 a.1 with Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.
• The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),
• The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and
• The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets.

In 1305 Physical Security, Change the following - (a) Requirements
(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.

to

(3) Physical Access Controls: The responsible entity shall implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.
(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.
(5) We recommend deleting this bullet as the intent is captured in bullet "4".
(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity.

Measures

Change

(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.

to

The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility.

In 1306.b.3 Change

"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.

to

"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."

In 1306.b.6, change

"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."

to

"Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three years in an exportable format, for possible use in further event analysis."

1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from "Incident and Cyber Security Incident Reporting" to "Security Incident Reporting". Change from "The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)." to "The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

Refer to our definition of a "security incident".

In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.

Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.
---

3. Lower Priority; mostly editorial and clarifications

Correct references as covered in question 2.

Request clarification on what "information" is protected in 1301.a.2.

In Section 1301.a.3

change
"….entity's implementation of…"

to

"…entity's implementation and adherence of…"

The “24 hours” in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.

Change 1301.b.5.i from "5 days" to "7 calendar days".

In 1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency.

In 1301.d.3.ii, change "address and phone number" to "business contact information". Same on page 5, 1301.b.5.iii
---

In 1301.e.1.iii, we request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.

In 1301.e.2.iii, change from

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

to

"An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or"

Remove 1301.e.4.v. The content is implied and redundant with 1301.e.4.i. If kept, change "Executive Management" to "Senior Management."

In 1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (FERC ORDER 2004b-Standards of Conduct).

The FAQ describes "supervised access." However 1303 does not touch upon this topic.

Change 1303.a.4 from "unrestricted access" to "authorized access".

In 1303 Measures.2, add a training measure section for disaster recovery (1308) and incident response planning (1307).

The numbering of 1303 starting with Measures needs correction.

1303 Measures 4.i, requires clarification. Does this measure include third party personnel?

Change 1303.Measures.4.i from

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).

to

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 respective security perimeter(s).

In 1303.Measures.4.ii, change from "two business days" to "seven calendar days", as per earlier comments.

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria is not applied, or" to "Personnel risk assement program is practiced, but not properly documented, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two
---

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three
---

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."

Change 1303. Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."

Correct the identation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii
---

From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.

1304 a.4 Change - The responsible entity shall ensure that all documentation reflect current configurations and processes.

to

The responsible entity shall ensure that all documentation required comply with 1304 a 1 through 1304 a.3 reflect current configurations and processes.

1304 a.4 Remove -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. (This is a measure and should be removed here)

Level of non compliance
Level three
Supporting documents exist, but not all transactions documented have records - this part is ambiguous and should be clarified
---

1305 Physical Security

Eliminate the bulleted items in the Preamble to Section 1305-they appear in the Requirement section.

In 1306.a.1, last paragraph, modify the second sentence -Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible.

Change "pooding" and "puffing" to "putting" in 1306.a.2.ii

Remove "Generic" from the title of 1306.a.2.ii

In 1306.a.2.iii, use "at least annually" instead of "at least semi-annually"

In 1306.a.3 change

"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.

to

"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets.
Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."

In 1306.a.4 Change

"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."

to

"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."

In 1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).

In 1306.a.6 change

"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."

to

"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three years in an exportable format, for possible use in further event analysis."

In 1306.a.7 Remove "Configuration Management" from the Title

In 1303.a.8 Remove the word "inherent" it is not clear what is meant by it.

Request clarification of 1306.a.10. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.

Remove 1306.a.11 since 1308 addresses back-up and recovery.

In 1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.

In 1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days".

In 1306.b.3, remove
"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."

In 1306 b.3 first sentence-eliminate the word "management".

In 1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.

1306.b.4 third sentence Change

"so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."

to

"mitigate risk of malicious software".

1306.b.4 Remove the second sentence.

1306.b.4 Replace the fourth sentence with "Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."

In 1306.b.5, remove the first sentence. Based on a third party outsourcing of this associated work of vulnerabilty assessment.

1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"

Remove 1306.b.11, since 1306.a.11 was removed.

In 1306.d.2, change

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

to

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

In 1306.d.3.iii, change "system log files" to "audit trails"

In 1306.e.2, change "the monthly/quarterly reviews" to "the reviews"

In 1306.e.2.ii.C, change "anti-virus" to "malicious"

In 1306, the Compliance levels should be updated to match the above measures.

In 1307, spell out and provide clarification on the acronyms throughout.

In 1307.d.1 there is a 90 day reference that does not appear in the measures.

In the beginning of 1307, change

"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."

to

"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."

Change 1307.b.5 from

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

to

"The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements."

Change 1307.b.6

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

to

"The responsible entity shall retain records of security incidents for three calendar years."

Change 1307.b.7

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

to

"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Pete Henderson	
Organization:	IMO	
Telephone:	905.855.6258	
Email:	Peter.Henderson@theIMO.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☒ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☒	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

The definition of "Incident" should be revised by deleting the second bullet. The first bullet sufficiently covers any incident.

The definition of "Security Incident" should read, 'Any malicious or suspicious activity which is known to have caused, or could have resulted in, an incident'.

The standard often refers to industry groups, committees and other structures. It would be helpful to have these defined and/or described somewhere within the standard.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
a. The current draft fails to properly emphasize that this standard is to be applied in a risk management context. It is therefore overly prescriptive in certain areas such as records retention durations and records revision frequencies.
b. Throughout the document, there are a number of inconsistencies in the way clauses are referred to, and places where clauses are referred to that do not exist. For instance, there are a number of references to 1302.1.2, yet there is no such clause. These references need to be properly correlated if the standard is to be useful.
c. It is noted in the "Background Information" section of the Comment Form that "An implementation plan will be developed at a later date for posting with a subsequent draft of this standard". As a subsequent draft is clearly contemplated by the drafting team, balloting at this time would be inappropriate.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
General Comments

1. A general statement should be made in a preamble to this standard that recognizes that this standard is to be applied in a risk management context. The following words are proposed: "This standard is intended to ensure that appropriate security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed."

2. This standard includes a number of new requirements that do not appear in NERC 1200. In order to both gauge the impact of these new requirements and make viable plans to come into compliance, it is essential to understand whether it is intended to phase in implementation of the standard and the schedule for that phasing.

3. In a number of places, the draft standard specifies that documentation is to be reviewed for accuracy and completeness within a specified time interval (sometimes annually, sometimes quarterly, sometimes every 90 days, etc). The required frequency of document review should be established by the responsible entity based on the risk associated with inaccurate or incomplete information rather than specified in terms of a prescribed time interval applicable to all responsible entities. It may be reasonable to prescribe that document review should occur no less frequently than once per year. Wording of the following form is suggested:

"The responsible entity shall update all documents in a timely fashion following the implementation of changes. Periodic reviews shall be conducted to ensure the accuracy of these documents. The responsible entity shall establish the required minimum frequency of these reviews based on the risk associated with these documents being out of date or inaccurate. At a minimum, documentation shall be reviewed annually."

If this comment is accepted, it will be necessary to revise the definitions of the various levels of non-compliance.

4. In a number of places the draft standard specifies the length of time for which access records, firewall logs, intrusion detection logs and the like are to be retained. The retention period for logs and access records and so on should not be prescribed by this standard. Rather, retention periods should be based on the usefulness of those records at a subsequent date, the cost of retention, and the risk associated with premature deletion. That is a judgement which is best made by "the responsible entity". It is appropriate to require that required retention periods are formally documented and approved by the responsible entity.

If this comment is accepted, it will be necessary to revise the definitions of the various levels of non-compliance. A requirement to retain logs for a longer period should a cyber security incident be detected within the normal retention period is reasonable and should be retained.

5. Throughout the document, there are a number of inconsistencies in the way clauses are referred to, and places where clauses are referred to that do not exist. For instance, there are a number of references to 1302.1.2, yet there is no such clause.

SPECIFIC COMMENTS
1301 Security Management Controls
(a) Requirements (5) - Access Authorization
Re (ii) Authorizing Access: If, as per 1301 (a) (5) (i) there is a process for access management which is instituted, then subsection (ii) is redundant.

As written, subsection (ii) does not appear to contemplate an access authorization scheme which allows access based on role. Rather, it assumes an authorization scheme based on name. This is overly prescriptive.

(b) Measures (5) - Access Authorization
Similar to the comment on Subsection 1301 (a) (5) (ii) above, this subsection does not appear to contemplate an access authorization scheme which allows access based on role. Rather, it assumes an authorization scheme based on name. This is overly prescriptive.

1303 Personnel & Training
(a) Requirements (4) Background Screening
The wording of this requirement should be consistent with 1303 (1) (4) (iv): viz: “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 in accordance with federal, state, provincial, and local laws, and subject to applicable collective bargaining unit agreements.

(I) Measures (4) - Background Screening
In subsection (vi) it is adequate to specify that updated screening should be done for cause. Periodic re-screening (every 5 years) is not required as good management practice includes observing changes in employee behaviour and circumstance that would prompt further investigation as necessary.

Subsection (iv) The Social Security Number (SSN)" is a unique identification number used strictly in the United States. The closest Canadian equivalent is the "Social Insurance Number (SIN)". However, Canadian law strictly limits the uses to which the SIN number can be put, and for this reason it is inappropriate for the standard to prescribe the use of SIN numbers for background checking.

(n) Compliance Monitoring Process (2)
The phrase, “where not prohibited by law or applicable collective bargaining agreements” should be added to the phrase, “Document(s) for compliance, training, awareness, and screening”.

(o) Levels of Noncompliance

(1) Level One
Nowhere in the Requirements portion of 1303 is there a reference to “consistent selection criteria”, so subsection (o) (1) (iii) should not be a measure of non-compliance.

(3) Level Three
1303 (o) (3) (iv) should be 1303 (o) (4).

1304 Electronic Security
(a) Requirements (4) Documentation Review and Maintenance

This should be reworded to, "The responsible entity shall ensure that all documentation required to comply with 1304 (a) (1) through 1304 (a) (3) reflects current configurations ……"

Delete the last sentence of this sub-section as it is redundant given 1304 (b) (4)

1306 Systems Security Management
(a) Requirements (1) Test Procedures:
The sentence, "Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment" should be deleted. In practice, testing cannot always be done on a non-production environment, nor is it always necessary to do so. For instance, under some circumstances testing can be done without disrupting normal production by performing the tests on otherwise redundant environment components which are still, strictly speaking, "in production".

Futhermore, testing cannot always be done without risk. The final sentence of this sub-section should be modified to read, "All testing must be performed in a manner that precludes, or minimizes, the risk of adversely affecting the production system and operation."

(a) Requirements (3) - Security Patch Management
Delete the phrase "and configuration management" as it is redundant given the first sentence and the remainder of the sub-section.

(a) Requirements (7) - Change Control and Configuration Management
Delete reference to Configuration Management in the title as the subsequent text identifies no requirements in this area.

(a) Requirements (8) - Disabling Unused Network Ports/Services
The reference to "inherent services" is confusing and requires clarification or deletion.

(b) Measures (1) - Test Procedures
The requirement in 1306 (a) (1) is to mitigate risk from known vulnerabilities. Therefore, in the final sentence of 1306 (b) (1), the word "potential" should be replaced by "known".

Delete the words, "on a controlled non-production system" as comments elsewhere.

(b) Measures (4) - Integrity Software
Delete the words "or" and "also" from the final sentence.

(b) Measures (7) - Change Control and Configuration Management
Delete the word "all" from the final sentence. As above in Requirements (7) delete reference to Configuration Management in the title as the subsequent text identifies no requirements in this area

(e) Levels of Noncompliance
(1) Level One
The requirement in 1306 (e) (1) (ii) requires clarification or deletion. The Measures in 1306 do not specify the need to update documentation, and in some cases (eg. passwords) the requirement is to document quarterly, not annually.

(3) Level Three
The wording of (ii) is confusing and requires clarification

Sub-section (3) (iii) (A) appears to specify that failure to perform a quarterly audit of password compliance with policy is a level 3 non-compliance, where as 1306 (e) (2) (ii) (A) states that it is a level 2 non-compliance.

The reference to 5.3.3.2 is confusing and should be corrected or deleted.

1307 Incident Response Planning
(d) Levels of Noncompliance
1307 (d) (1) and 1307 (d) (2) (i) require revision. Neither 1307 (a) nor 1307 (b) specify a requirement to update documentation within 90 days or review documentation annually.

In a case where records related to the response to a reportable security incident are incomplete, it is unclear whether 1307 (d) (2) (ii) or 1307 (d) (3) (i) applies.

1307 (d) (3) (ii) should be reworded to state that a failure to report a reportable incident to ESISAC is a level 3 non-compliance.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Joanne Borrell	
Organization:	FirstEnergy Solutions	
Telephone:	330.315.6857	
Email:	jkborrell@fes.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☒ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☒	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Definition for Bulk Electric System Asset is not consistent with its intent. This is a high level component that is facility based and should be reflected as "Bulk Electric System Facility".

There is definition or criteria stated for the Risk Assessment. There should be three definative levels for the risk assessment starting at the top with Bulk Electric System Facility, then Critical Cyber Assets (System Functions) and Cyber Assets. This should be spelled out in the standard and not added as a FAQ.

Applicability: Should contain a disclaimer that the NUKES are not included, currently if you want that information you have to go to the SAR.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
See response to question 3

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

Definitions: Bulk Definitions need to be clear and consistent from one NERC document to the next if a true “consensus” throughout the industry is desired by NERC prior to balloting.

By placing additional security restrictions/costs on routable (IP) technology, NERC will (in effect) slow the migration from older technologies to more flexible future technologies involving (IP).

During the Standard 1200 process, the NERC Responses to the Ballot Comments provided a different definition than the language contained in Standard 1200 in some cases. Example: Standard 1200 clearly stated an “isolated” test environment was required. NERC Responses clearly stated that an “isolated” test environment was NOT required. This led to mis-understandings about what the real requirements were. Although the Standard 1300 process is young, there appears to be too much reliance on the FAQ’s to embellish the requirements. Documents, such as the FAQ’s, should be used to provide examples. The intent of the requirements should be fully explained in the Standard 1300 language, not the FAQ’s.

ABC is concerned that requirements, such as excessive documentation, will mean that resources are utilized to comply with requirements that do not truly enhance actual security.

ABC believes that some estimate of the costs vs. the benefit of the requirements must be understood before moving toward implementation.

General Question

If a company goes through the process and finds that it has NO critical cyber assets, does that company have any additional obligations under Standard 1300? If so, please explain.

Definitions Section

Page 1
The definition of "Cyber Assets" (on page 1 of the draft) is vague and leaves room for interpretation, and how it is interpreted could have drastic impact. The term "cyber" in the heading implies computerized equipment, particularly that which can be networked together via electronic communications, however the definition does not specifically state that. ABC seeks clarification from NERC regarding "non-computer" devices such as protective relays, solid-state transducers, etc. that are not networked nor communicated to in any way.

Definitions section needs to clearly define “routable protocol” in the definitions including what is a routable protocol and what is not a routable protocol. While the definition may be familiar to many, this concept is key to identifying the critical cyber assets, yet no definition is provided.

Definitions section also needs to define “dial up accessible” for same reasons noted above.

1301 Security Management Controls Section

Page 3: Several sections of 1301 will require coordination at executive level across business units throughout corporations. These types of sweeping administrative documentation requirements will prove extremely time consuming and, therefore, expensive to implement under the proposed 1300 language. Some are already inherent in the organization charts, operating procedures, and job descriptions of the corporation. Standard 1300, as proposed, will simply create redundant corporate documentation in these cases because (while documentation may exist) it may not be in a format readily available for Standard 1300 audit review. If no relevant threat information exists or the costs and benefits do not warrant implementation, ABC recommends section such as those listed below be eliminated or modified.

Governance section, which requires entities to document structure for decision making at executive level.
o The Cyber Security Policy section of 1301 requires that senior management acknowledge responsibility for cyber security. Therefore the 'decision making' at the executive level is covered in the Policy section, making the governance section un-necessary.

Roles & Responsibilities requiring participants to "maintain in its policy the defined roles & responsibilities…"
o If The Roles & Responsibilities section is not deleted entirely, then at least delete the second paragraph: 'The responsible entity shall also define the roles and responsibilities of critical cyber asset owners, custodians, and users…identified and classified in section 1.2'. From the existing numbering system used, it is not clear what "1.2" refers to.

Page 4: "Authorization to Place into Production," part of Section 1301, requires entities to "identify the controls for testing…and document that a system has passed testing criteria." ABC agrees that a testing procedure is required. However 1301 language as proposed requires redundant documentation over and above requirements as spelled out on p. 26 and 28 in the "Test Procedures" part of Section 1306. Section 1306, "Test Procedures" (p. 28) states "…change control documentation shall include records of test procedures, results of acceptance of successful completion…documentation shall verify that all changes to critical cyber assets were successfully tested…prior to being rolled into production…" Recommendation: Section 1301 authorization to Place into Production section (for the most part) is redundant to Section 1306 Test Procedures. If the following sentence was added to Section 1306, Test Procedures, then all of "Authorization to Place into Production" section could be eliminated. "Responsible entities shall designate approving authority that will formally authorize that a system has passed testing criteria." Appropriate references to associated non-compliance items would also have to be eliminated.

NERC's recently published FAQ's on Standard 1300 actually adds additional issues. Standard 1300 calls for "…entities to...identify controls…designate approving authorities that will formally authorize and document that a system has passed testing criteria….approving authority shall be responsible for verifying that a system meet minimum security configurations standards." There is nothing in the Standard 1300 which states the approving party cannot be an operator, programmer, or owner of the system. Yet in the FAQ for Standard 1300, NERC states " …assign accountability to someone other than the operator, programmer, or owner of the systems to ensure that …" testing has been completed. It appears that NERC is adding yet more requirements, ie., (separation of duties,) through the use of FAQ posting. ABC recommends that if requirements are not spelled out in the Standard language, additional requirements (such as this type of separation of duties) should not be introduced via the FAQ publications.

Page 4: Access Changes: By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 & 1306)
Need clarification & consistency from NERC on exactly WHAT the access change requirements are.
- 1301 states: "Responsible entities shall… ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."
- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)… and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.
- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who…are not allowed access…(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.
- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations…24 hours.

Further on the subject of Access requirements, commentors stated that the 24-hour access limitation for updating records was un-duly severe in the Standard 1200 comments. NERC Responses to Cyber Security Standard 1200 Ballot Comments 6-11-03 posted to the NERC website provided the following:

"NERC acknowledges the validity of these comments and will address them more fully in the final standard... we will expect that a system will be in place to periodically update access authorization lists on at least a quarterly basis. That protocol will also ensure that access be suspended as soon as possible and no later than 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems. Routine administrative changes resulting from retirements, resignations, leaves, etc. should be handled within the normal course of business but not in excess of three business days after occurrence…."

While ABC acknowledges that Standard 1300 is a different standard from 1200, we wish to remind NERC of the statement that they will address objections to the excessively stringent 24 hour access update requirement in the 'final standard." Since objections have not been addressed, NERC still needs to do this.

Regarding requirements for updating access records, ABC recommends:
(1) The requirement should be stated as recommended by NERC above 'Access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat…Routine administrative changes …should be handled within three business days after occurrence."
(2) The requirement should only be defined in one section of the document rather than currently proposed language which includes multiple conflicting requirements within the same Standard.
(3) If the item is used to identify non-compliance, all references throughout the document should reflect the revised requirements.

Page 3: (a) (2) (i) "The responsible entity shall identify "all" information, regardless of media type, related to critical cyber assets." It is impossible to certify that ALL information is identified and protected. ABC recommends that the word "all" should be deleted and language changed to: "The responsible entity shall identify information related to critical cyber assets."

Page 3: ABC seeks guidance from NERC regarding the minimum levels of 'protection' to be afforded this information.

Page 7: Levels of non-compliance, particularly for Level four are excessive. There are eleven (11) different items identified that can trigger a non-compliance item. This is far too many non-compliance triggers, and too burdensome. Recommendation: If the sections on Governance and Roles & Responsibilities are omitted as suggested above, then these items will also be omitted from Levels of Non-compliance, making the document manageable: Level 2 delete (iii); Level 3 delete (iv); Level 4 delete (iv), (v), (vi), (viii). If Governance and Roles & Responsibilities sections remain part of the document, then NERC should select 2 to 4 items from the list of 11 Level 4 triggers that will provide an indication of compliance and delete the remainder.

Page 7 (4) (xi) The item which seeks a violation if one access change is not accomplished within 24 hours needs to be either eliminated or else modified to reflect the above recommendation that a violation is only warranted if the access is not suspended in 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems.
1302 – Critical cyber assets
Page 10: Critical Cyber Assets: "…the cyber asset supports a critical bulk electric system asset." Examples: Environmental and performance software supports generation assets but is not critical to continuation of power. In the 10/18 Webcast, NERC used the word "control" rather than "supports". ABC recommends that the word "supports" be changed to reflect the intent that the cyber asset is essential to continued operation of the critical bulk electric system asset, i.e., loss of that cyber assets causes loss of the critical bulk electric system asset.
Page 10: "Critical Cyber Assets", as defined on page 10 of the draft, narrows the definition to cyber assets that "support critical bulk electric system assets" AND "uses a routable protocol" or "is dial-up accessible". Because a proper understanding of what constitutes a critical cyber asset, ABC has several questions and seeks clarification from NERC on protocols in use throughout the organization today as well as protocol proposed for the next generation of communication from remote locations to ABC's Energy Management System.
ABC interprets Standard 1300 to exclude devices such as remote terminal units that communicate over dedicated point to point communication circuits. An example of this would include RTU's communicating via Landis & Gyr 8979 RTU protocol over 4-wire dedicated Bell 3002 circuits. ABC seeks clarification on the following:

ABC currently uses a "non-routable" protocol (e.g. ABC's current Landis & Gyr 8979 RTU protocol) that are communicated using PVCs (private virtual circuits) over a frame relay network. ABC seeks clarification on routable protocol reference and how NERC believes it applies here.

ABC needs clarification on 'routable protocol' reference and how requirements apply to proposed use of "DNP over IP" using frame relay.

ABC seeks clarification of the 'dial up accessible' reference regarding DNP.

Is an electronic relay interpreted by NERC to be a computerized cyber asset?

If a relay is constructed to allow remote data retrieval but prohibit any configuration changes, is it excluded from the requirements?

Page 9 Generation: Proposed Standard 1300 references other documents (Policy 1) that are open to interpretation by Regional Councils. Rather than spelling out the rules for generation that needs to be considered a Critical Bulk Electric System Assets, Standard 1300 refers to another document (Policy 1.B). ECAR has modified the definition of "Most severe single contingency".

Using the proposed Std 1300 language from the multiple documents and regional definitions mean that almost all ABC's generating facilities fall under the rules of Standard 1300.

Is it NERC's intent that all generating stations should be subject to the rules of Standard 1300? If this is not NERC's intent, then the proposed language needs to be changed.

ABC recommends that all of the rules for identifying the critical bulk electric system assets and the critical cyber assets should be identified in one document, rather than using multiple documents subject to regional interpretations as used in Std 1300 version 1. Recommendation: On page 9, eliminate reference to NERC Policy 1.B in (iii) (A) and replace with this language: "…greater than or equal to 80% of the most severe single contingency loss."

ABC seeks clarification from NERC of the term "Most severe single contingency". Please use the following example:

Utility owns approximately 600 MW of a total 1300 MW generation site all in ECAR

Same utility owns 100 % of a 635 MW generation site

Which of the above should be identified as the largest "single contingency"? If the 635 MW site is used, generating units, which ABC does not consider critical, will be included in the list of "critical cyber assets."

ABC recommends that a good use for the FAQ's would be to provide additional examples, including some examples using how the requirements apply to jointly owned units (JOU's).

Page 9: Either fully explain or eliminate (iii) Generation (B) "…generating resources that when summed meet the criteria…"

Page 10: ABC believes the level of documentation and administrative control required by proposed Standard 1300 is extensive and imposes a significant operating cost on participants. Once again, this section contains requirements without any documented evidence that the expense to implement will enhance security or that there is a relevant threat, which will be mitigated by this level of documentation. Parts of the section are redundant to other requirements. ABC has designated two company officers that are responsible for the Cyber Security Policy and implementation. "Critical Bulk Electric system Asset and Critical Cyber Asset List Approval section," requires a properly dated record of senior management officer's approval of the list of critical bulk electric system assets. ABC recommends that requirements such as this be deleted unless evidence is shown which indicates direct security benefit. Recommendation: Eliminate Requirement (a) (3) " …A sr. management officer must approve the list of…" and also eliminate corresponding "Compliance Monitoring Process" (i) (3) (iv) page 11. The senior officers are responsible for implementation of the program and should not be required to sign off on each section of the document as each section is updated.

In the October 18 Webcast, NERC slides indicated a "3 step" approach to identifying the critical cyber assets. Standard 1300 lists (#1) Identify the Critical Bulk Electric System Assets and (#2) Identify Critical Cyber Assets. ABC seeks clarification from NERC regarding the three (3) steps referred to in the Webcast.

1303 – Personnel & Training

Page 13 "Awareness Program": Once again, this section contains requirements without any documented evidence that such requirements will enhance security. Requiring both training program and awareness program seems redundant and burdensome. ABC recommends that the awareness in inherent in training and is part of the training requirements. We recommend that the separate "Awareness" section be deleted.

Page 14 Access Changes:
By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1301 & 1306)
Need clarification & consistency from NERC on exactly WHAT the access change requirements are.
- 1301 states: "Responsible entities shall… ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."
- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)… and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.
- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who…are not allowed access…(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.
- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations…24 hours.

Regarding requirements for updating access records, ABC recommends:
1. The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat…Routine administrative changes …should be handled within three business days after occurrence."
2. The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.
3. If the item is used to identify non-compliance, all references throughout the document should reflect the revised requirements.

Page 14: Background Screening. The entire section on background screening, as written in Standard 1300, is problematic. For example:
- "…A minimum of Social Security Number verification…" Language as written will deny access to anyone except U.S. citizens. ABC recommends that the language requiring a social security number be deleted unless it is NERC's intent that only U.S. citizens and no one else is granted electronic or physical access.

NERC showed insight when, in their Responses to comments submitted during the balloting of the Urgent Action Cyber Security Standard 1200, NERC wrote: "…organizations are NOT required to conduct background investigations of existing employees given the fact that they have had the opportunity to observe and evaluate the behavior and work performance of those employees after they have been employed for a period of time." ABC again recognizes that Standard 1300 is a different standard from Standard 1200; however, the logic that provided the foundation for the previous NERC comment is sound. If the company has had an opportunity to observe the long service employee, the background screen requirement should be relaxed.

ABC recommends one of the following to replace proposed Standard 1300 language:
A. The requirement should include background screening for all individuals (employees and vendors) who seek approval for new permanent access to critical cyber assets.

Background screening on existing employees, previously approved for access, is appropriate if there is cause to suspect the individual of suspicious behavior.

Requiring the screening of all personnel every 5 years should be deleted.

B. If the above proposed language is not acceptable as an alternative by NERC, then ABC recommends language be inserted indicating that background screening requirements will be evaluated by the company involved, and the policy toward such screenings will be documented by that company. Company will be free to document policies such as: At Company's discretion, long service employees, which the Company has observed, may be grandfathered and background checks will not be done on these employees. Company will not be found in non-compliance for such a policy.

Page 13: Language states that a "higher level of background screening" should be conducted on personnel with access. ABC's background screening for new hires complies with the NERC requirements and other legal requirements. ABC does not agree that multiple levels of background screening are required. ABC recommends that the reference to multiple levels of background screening be deleted.

Page 13: Records: " …background screening of all personnel having access to critical cyber assets shall be provided for authorized inspection upon request." ABC does not agree that the background screen information obtained on all its employees will be provided to NERC inspectors. In the 10/18 Webcast NERC stated that it is not their intent that the contents of the background screening be provided to the inspectors. Recommendation: Improve language so that it is clear that contents of background screen need not be divulged to inspectors.

Page 15 (i) Standard 1300 language implies that background check lists & verifications are kept by operations groups responsible for the cyber security implementation. Such records will continue to be maintained by the Human Resource Department at ABC.

Page 13: Background screening: Proposed language states: "…contractors and service vendors, shall be subject to background screen prior to being granted unrestricted access to critical assets." Is it NERC's intention that they be granted unrestricted access after completing a background screen as stated in 1300?

1304 – Electronic Perimeter

Page 17 (a) (1) Electronic Security perimeter: Proposed language states "Communication links …are NOT part of the secured perimeter…However, end points of the communication links… are considered access points to the perimeter. Where there are non critical assets within the defined perimeter these non-critical assets must comply with the requirements…" Language is contradictory and confusing. Proposed language makes the asset and the end point critical assets and within the perimeter, but language excludes the communication line between them. The next sentence implies the communication line needs to be treated as though it is part of the perimeter. ABC seeks clarification.

Page 18: (b) (1) Electronic Security Perimeter:
ABC seeks clarification regarding from NERC regarding Frame Relay Access Devices (FRAD's) and modems connected to cyber assets. Are these considered "access points to the electronic security perimeter"?

If the FRAD's are considered 'within the perimeter' with the resulting requirements extending to the FRAD's, this is an excessive and unnecessary level of detail and will prove costly and burdensome without proven corresponding benefit.

Page 18: Measures (3): Monitoring Electronic Access Controls: Wording of this section, particularly the last sentence, is very confusing and needs clarification regarding exact requirements for documentation and for implementation of monitoring the access controls.
P. 19 (e) (3) Electronic Access Controls: Page 19 identifies a non-compliance item if "…not all transactions documented have records." ABC seeks clarification. If a transaction is documented, by definition, doesn't that mean the transaction has a record?
Page 17 Electronic Access Controls: "…non critical cyber assets (within the perimeter) must comply with the requirements of this standard." Different departments within the organization will handle different functions. Current language implies one rigid process to apply to both critical assets and non-critical assets, which may exist within the perimeter. Recommend that this be changed to: non-critical cyber assets within the perimeter must utilize similar electronic access controls.
1305 – Physical Perimeter

While ABC acknowledges that controls may be required, it does not seem appropriate for NERC to dictate the controls to be implemented. Example: Implement CCTV or Alarm System.

ABC's interpretation of current draft language in Section 1302 will result in almost all ABC generating plants being subject to these rules. Section 1305 then seeks to name the controls, which must be implemented at each asset location. No mention to a review of costs associated with such sweeping changes is even mentioned in any of the language. ABC believes it is appropriate to address the costs and corresponding benefits before moving forward with such a sweeping and costly initiative. ABC recommends that participants and NERC develop an estimate of the proposed cost to the industry before finalizing these requirements.

Generating plants control rooms may be manned 24 hours a day seven days a week. ABC seeks clarification and evidence of the need for the many controls, such as CCTV, which are specified in the document in these cases where facilities are manned.

Page 24 (6) Maintenance and testing of security systems to be retained for 1 yr. This involves corp. wide – Equipment Maintenance area. This is one more example of the costs, which must be considered before moving forward. These types of requirements are very costly to large organization because they impose enterprise wide requirements. Maintenance records on the security installation equipment will not be kept in Electric Operations areas. Requirements will need to be coordinated across groups responsible for equipment maintenance.

1306 – System Security management

While the list of physical controls to be implemented in the proposed section 1305 language represents a huge, solid, and obvious cost burden, requirements in section 1306 represent a less obvious but huge cost burden as well.

Once again, there is no evidence presented that there is a relevant threat, which will be mitigated, if these types of controls/documentation requirements are implemented. Also, once again, there is no indication if the idea of associated costs was even contemplated prior to writing the language requiring the controls/documentation.

ABC requests that evidence needs to be presented showing (1) a relevant threat will be mitigated if the controls outlined in this section are implemented (2) costs and benefits associated with requirements have been identified.

ABC is concerned that if money and resources are required for documentation requirements that yield no real enhancement to security, then less money and resources will be available for security measures that could truly yield benefit. Recommendation: Either significantly lessen requirements or eliminate many of the following.

Page 28: Archive backup information for a prolonged period of time and then test it annually to ensure it is recoverable. A definition of 'information' and 'archival information' should be provided. Archived information looses its value in time and may become irrelevant. Is NERC dictating records retention policy? What is the consequence if this does not occur? Requires extra work, but what is the point? Need better understanding of costs vs. benefits.

Page 28: Create Operating Status Monitoring tools. This section indicates the tools gauge 'performance.' Standard 1300 language contains no statement as to what these performance-monitoring tools are trying to gauge nor are any performance goals indicated. This would be costly to implement with no defined benefit or even goals for the tools. Requires extra work, but what is the point?

Page 28: Create Operating Status Monitoring tools: Language in the section implies that performance documentation is to be kept for every asset. This is not reasonable.

Page 27: Retention of system Logs: "All critical cyber security assets must generate an audit trail for all security related system events." In the case of local RTU's this is probably not possible.

Page 26: Test Procedure language as written is overly burdensome. Language implies that EVERYTHING needs to be tested. It is not realistic that EVERY minor change is documented in formal testing. FAQ's seem to conflict with Std. 1300 proposed language. Recommendation: Modify Standard 1300 language to imply levels similar to NERC's recent Standard 1300 FAQ posting.

Page 27: Testing "…provide a controlled environment for modifying ALL hardware and software for critical cyber assets." Since the Energy Management System is by nature a critical cyber asset, the language implies that EVERYTHING must be modified in a separate controlled environment. Current language is burdensome and not practical. Recommendation: Indicate a reasonable level for testing within the controlled environment. Use levels similar to those identified in NERC's recent Standard 1300 FAQ posting.

Page: 27 Test Procedure Measures: Language states, " …Critical cyber assets were tested for potential security vulnerabilities prior to be rolled into production…" It is unclear what 'potential vulnerabilities' are to be tested or how the tester is to know about them. Recommendation: Explain clearly or delete the reference.

Page 29: Integrity software: ABC is pursuing a course of isolating the Energy Management System from the corporate network. This path of isolation reduces threat from email, Internet use, etc. The language requires anti-virus versions be kept immediately up to date. In practice, this

conflicts with the work to isolate the EMS and presents un-necessary requirements since the EMS will be isolated from the source of the viruses.

Page 27: Security Patch Management: ABC seeks clarification of " …upgrades to critical cyber assets." If this language includes every upgrade, it is costly and over-burdensome without resulting security benefit.

Page 27: Created formalized change control & configuration management process: Entire section creates un-necessary and redundant requirements that are included in the Test Procedures requirements section of 1306.

Section 1306 Security Patch Management section presents additional problems for power plant control systems. For example,

Security Patch Management language (page 27) requires timely installation of applicable security patches and operating system upgrades.

Patches and upgrades (at the power plant) at ABC can only be applied during an outage of the control system.

ABC seeks clarification from NERC as to how all of Section 1306, including Security Patch Management, applies to power plant control systems. Will plants be expected to create more outages to keep up with requirements?

Page 28 (2) Account Management: "review access permissions within 5 working days. For involuntary terminations, …no more than 24 hours". By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 & 1301)

Need clarification & consistency from NERC on exactly WHAT the access change requirements are.

- 1301 states: "Responsible entities shall… ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."
- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)… and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.
- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who…are not allowed access…(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.
- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations…24 hours.

ABC recommends:

- The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat…Routine administrative changes …should be handled within three business days after occurrence."
- The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.
- If the requirement is used in the non-compliance section, then the non-compliance section should be consistent with revised requirements.

1307 & 1308- Response & Recovery Plans

Page 34:
1300 Language seems to imply NERC expects multiple plans to be created for Cyber Security. " …recovery plans associated with control centers will differ from those associated with power plants and substations." This level of detail may become too onerous. ABC seeks clarification from NERC if multiple plans are required. Once again, this will involve time, money and resources to create documentation at an un-precedented detail level with no indication that such a measure will increase real security.

If entities strictly follow the language proposed for 1307, they will be forced to create un-necessary documentation for very brief interruptions and for events, which were not malicious and did not create a disruption. NERC definitions provided the following:
NERC defines an "incident" as ANY physical or cyber event that disrupts or could lead to a disruption of the critical cyber assets.
Same section defines a "cyber security incident" as malicious or suspicious activities, which cause or may cause an incident.
Definition section does NOT include a definition of a "reportable incident"

The language of the entire 1307 section is written to apply to both incidents and cyber security incidents.
Once again, as we have seen in other sections, companies that attempt to follow these requirements will create costly levels of detail and documentation (for every incident which either creates a slight disruption or could lead to a disruption) with no proven direct benefit to security. Here are some examples:
Page 32 states, "…retain records of incidents and cyber security incidents for 3 calendar years." This includes but is not limited to:
o System and application log files
o Video and or physical access records
o Investigations and analysis performed
o Records of any action taken including recovery actions
o Records of all reportable incidents and subsequent reports
…make all records and documentation available for inspection."
Recommendation: Re-work the language so that it is clear at what level this degree of detailed documentation needs to be retained.

Page 34 (a) (3) "…update the recovery plans within 30 days of a system or procedural change and post the recovery plan contact information." This language is problematic in 2 areas:
1. It is not realistic to expect that the plan will be updated within 30 days of each procedural or system change.
2. ABC does not "post" contact information. NERC does not specify what type of "posting" they require. Further this requirement is contradictory to other NERC cyber security requirements. ABC regards emergency plans and contact information as critical cyber asset information. Information is treated as such.
ABC recommends that plans be updated annually and that contact information should be treated consistent with other information related to critical cyber assets.

Additional Comments on Format
- The numbering sequence is not accurate throughout the document, making it difficult to follow in some sections. Recommendation: A different consistent numbering system should be used or, at the least, the entire document should be reviewed for appropriate numbering. Examples include but are not limited to:
o See Page 9 (a) Requirements then Page 10 (g) Measures. Where are items (b), (c), (d), (e), & (f)?
o Page 13: All of Section 1303 need review
- Typing mistakes need to be corrected. Example: Page 15 "…doesn't not cover one of the …"

FAQ's Recently Posted by NERC

In addition to inserting requirements regarding separation of duties noted above, question 3 on page 9 of the FAQ document seeks to limit the definition of RTU's, that use a non-routable protocol. Standard 1300 implies that non-routable protocols are excluded. However, the answer to question 3 tightens the definition of what is excluded by adding additional requirements that may not apply to all non-routable protocols: "…have a master/slave synchronous polling method that cannot be used to access anything on the EMS and they use SBO command…" As noted above, it is not appropriate to introduce additional restrictions to the Standard language via the FAQ posting process.

ABC Implementation Timeline

After the Standard 1300 language and requirements are finalized, ABC estimates:

o 1.5 to 2 years to evaluate standard impact and what is to be included in compliance.
o This is dependent upon how much guidance is given by NERC in regards to specifics for equipment and facilities to be included.

o 3.5 to 4 years to implement and become compliant.

o Total of 5 to 6 years from acceptance of the standard until compliance is reached.
of the standard until compliance is reached.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Ray Morella	
Organization:	FirstEnergy Corp	
Telephone:	330.384.5686	
Email:	morellar@firstenergycorp.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☒ ECAR ☐ FRCC ☐ MAAC ☐ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☒	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☐	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

Definition for Bulk Electric System Asset is not consistent with it's intent. This is a highlevel component that is really facility based and should be reflected as "Bulk Electric System Facility".

There is definition or criteria stated for the Risk Assessment. There should be three definative levels for the risk assessment starting at the top with Bulk Electric System Facility, then Critical Cyber Assets (System Functions) and Cyber Assets. This should be spelled out in the standard and not added as a FAQ.

Applicability: Should contain a disclaimer that the NUKES are not included, currently if you want that information you have to go to the SAR.

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
See response to question 3

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

Definitions: Bulk Definitions need to be clear and consistent from one NERC document to the next if a true “consensus” throughout the industry is desired by NERC prior to balloting.

By placing additional security restrictions/costs on routable (IP) technology, NERC will (in effect) slow the migration from older technologies to more flexible future technologies involving (IP).

During the Standard 1200 process, the NERC Responses to the Ballot Comments provided a different definition than the language contained in Standard 1200 in some cases. Example: Standard 1200 clearly stated an “isolated” test environment was required. NERC Responses clearly stated that an “isolated” test environment was NOT required. This led to mis-understandings about what the real requirements were. Although the Standard 1300 process is young, there appears to be too much reliance on the FAQ’s to embellish the requirements. Documents, such as the FAQ’s, should be used to provide examples. The intent of the requirements should be fully explained in the Standard 1300 language, not the FAQ’s.

ABC is concerned that requirements, such as excessive documentation, will mean that resources are utilized to comply with requirements that do not truly enhance actual security.

ABC believes that some estimate of the costs vs. the benefit of the requirements must be understood before moving toward implementation.

General Question

If a company goes through the process and finds that it has NO critical cyber assets, does that company have any additional obligations under Standard 1300? If so, please explain.

Definitions Section

Page 1
The definition of "Cyber Assets" (on page 1 of the draft) is vague and leaves room for interpretation, and how it is interpreted could have drastic impact. The term "cyber" in the heading implies computerized equipment, particularly that which can be networked together via electronic communications, however the definition does not specifically state that. ABC seeks clarification from NERC regarding "non-computer" devices such as protective relays, solid-state transducers, etc. that are not networked nor communicated to in any way.

Definitions section needs to clearly define “routable protocol” in the definitions including what is a routable protocol and what is not a routable protocol. While the definition may be familiar to many, this concept is key to identifying the critical cyber assets, yet no definition is provided.

Definitions section also needs to define “dial up accessible” for same reasons noted above.

1301 Security Management Controls Section

Page 3: Several sections of 1301 will require coordination at executive level across business units throughout corporations. These types of sweeping administrative documentation requirements will prove extremely time consuming and, therefore, expensive to implement under the proposed 1300 language. Some are already inherent in the organization charts, operating procedures, and job descriptions of the corporation. Standard 1300, as proposed, will simply create redundant corporate documentation in these cases because (while documentation may exist) it may not be in a format readily available for Standard 1300 audit review. If no relevant threat information exists or the costs and benefits do not warrant implementation, ABC recommends section such as those listed below be eliminated or modified.

Governance section, which requires entities to document structure for decision making at executive level.
o The Cyber Security Policy section of 1301 requires that senior management acknowledge responsibility for cyber security. Therefore the 'decision making' at the executive level is covered in the Policy section, making the governance section un-necessary.

Roles & Responsibilities requiring participants to "maintain in its policy the defined roles & responsibilities…"
o If The Roles & Responsibilities section is not deleted entirely, then at least delete the second paragraph: 'The responsible entity shall also define the roles and responsibilities of critical cyber asset owners, custodians, and users…identified and classified in section 1.2'. From the existing numbering system used, it is not clear what "1.2" refers to.

Page 4: "Authorization to Place into Production," part of Section 1301, requires entities to "identify the controls for testing…and document that a system has passed testing criteria." ABC agrees that a testing procedure is required. However 1301 language as proposed requires redundant documentation over and above requirements as spelled out on p. 26 and 28 in the "Test Procedures" part of Section 1306. Section 1306, "Test Procedures" (p. 28) states "…change control documentation shall include records of test procedures, results of acceptance of successful completion…documentation shall verify that all changes to critical cyber assets were successfully tested…prior to being rolled into production…" Recommendation: Section 1301 authorization to Place into Production section (for the most part) is redundant to Section 1306 Test Procedures. If the following sentence was added to Section 1306, Test Procedures, then all of "Authorization to Place into Production" section could be eliminated. "Responsible entities shall designate approving authority that will formally authorize that a system has passed testing criteria." Appropriate references to associated non-compliance items would also have to be eliminated.

NERC's recently published FAQ's on Standard 1300 actually adds additional issues. Standard 1300 calls for "…entities to...identify controls…designate approving authorities that will formally authorize and document that a system has passed testing criteria….approving authority shall be responsible for verifying that a system meet minimum security configurations standards." There is nothing in the Standard 1300 which states the approving party cannot be an operator, programmer, or owner of the system. Yet in the FAQ for Standard 1300, NERC states " …assign accountability to someone other than the operator, programmer, or owner of the systems to ensure that …" testing has been completed. It appears that NERC is adding yet more requirements, ie., (separation of duties,) through the use of FAQ posting. ABC recommends that if requirements are not spelled out in the Standard language, additional requirements (such as this type of separation of duties) should not be introduced via the FAQ publications.

Page 4: Access Changes: By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 & 1306)
Need clarification & consistency from NERC on exactly WHAT the access change requirements are.
- 1301 states: "Responsible entities shall… ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."
- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)… and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.
- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who…are not allowed access…(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.
- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations…24 hours.

Further on the subject of Access requirements, commentors stated that the 24-hour access limitation for updating records was un-duly severe in the Standard 1200 comments. NERC Responses to Cyber Security Standard 1200 Ballot Comments 6-11-03 posted to the NERC website provided the following:

"NERC acknowledges the validity of these comments and will address them more fully in the final standard... we will expect that a system will be in place to periodically update access authorization lists on at least a quarterly basis. That protocol will also ensure that access be suspended as soon as possible and no later than 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems. Routine administrative changes resulting from retirements, resignations, leaves, etc. should be handled within the normal course of business but not in excess of three business days after occurrence…."

While ABC acknowledges that Standard 1300 is a different standard from 1200, we wish to remind NERC of the statement that they will address objections to the excessively stringent 24 hour access update requirement in the 'final standard." Since objections have not been addressed, NERC still needs to do this.

Regarding requirements for updating access records, ABC recommends:
(1) The requirement should be stated as recommended by NERC above 'Access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat…Routine administrative changes …should be handled within three business days after occurrence."
(2) The requirement should only be defined in one section of the document rather than currently proposed language which includes multiple conflicting requirements within the same Standard.
(3) If the item is used to identify non-compliance, all references throughout the document should reflect the revised requirements.

Page 3: (a) (2) (i) "The responsible entity shall identify "all" information, regardless of media type, related to critical cyber assets." It is impossible to certify that ALL information is identified and protected. ABC recommends that the word "all" should be deleted and language changed to: "The responsible entity shall identify information related to critical cyber assets."

Page 3: ABC seeks guidance from NERC regarding the minimum levels of 'protection' to be afforded this information.

Page 7: Levels of non-compliance, particularly for Level four are excessive. There are eleven (11) different items identified that can trigger a non-compliance item. This is far too many non-compliance triggers, and too burdensome. Recommendation: If the sections on Governance and Roles & Responsibilities are omitted as suggested above, then these items will also be omitted from Levels of Non-compliance, making the document manageable: Level 2 delete (iii); Level 3 delete (iv); Level 4 delete (iv), (v), (vi), (viii). If Governance and Roles & Responsibilities sections remain part of the document, then NERC should select 2 to 4 items from the list of 11 Level 4 triggers that will provide an indication of compliance and delete the remainder.

Page 7 (4) (xi) The item which seeks a violation if one access change is not accomplished within 24 hours needs to be either eliminated or else modified to reflect the above recommendation that a violation is only warranted if the access is not suspended in 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems.
1302 – Critical cyber assets
Page 10: Critical Cyber Assets: "…the cyber asset supports a critical bulk electric system asset." Examples: Environmental and performance software supports generation assets but is not critical to continuation of power. In the 10/18 Webcast, NERC used the word "control" rather than "supports". ABC recommends that the word "supports" be changed to reflect the intent that the cyber asset is essential to continued operation of the critical bulk electric system asset, i.e., loss of that cyber assets causes loss of the critical bulk electric system asset.
Page 10: "Critical Cyber Assets", as defined on page 10 of the draft, narrows the definition to cyber assets that "support critical bulk electric system assets" AND "uses a routable protocol" or "is dial-up accessible". Because a proper understanding of what constitutes a critical cyber asset, ABC has several questions and seeks clarification from NERC on protocols in use throughout the organization today as well as protocol proposed for the next generation of communication from remote locations to ABC's Energy Management System.
ABC interprets Standard 1300 to exclude devices such as remote terminal units that communicate over dedicated point to point communication circuits. An example of this would include RTU's communicating via Landis & Gyr 8979 RTU protocol over 4-wire dedicated Bell 3002 circuits. ABC seeks clarification on the following:

ABC currently uses a "non-routable" protocol (e.g. ABC's current Landis & Gyr 8979 RTU protocol) that are communicated using PVCs (private virtual circuits) over a frame relay network. ABC seeks clarification on routable protocol reference and how NERC believes it applies here.

ABC needs clarification on 'routable protocol' reference and how requirements apply to proposed use of "DNP over IP" using frame relay.

ABC seeks clarification of the 'dial up accessible' reference regarding DNP.

Is an electronic relay interpreted by NERC to be a computerized cyber asset?

If a relay is constructed to allow remote data retrieval but prohibit any configuration changes, is it excluded from the requirements?

Page 9 Generation: Proposed Standard 1300 references other documents (Policy 1) that are open to interpretation by Regional Councils. Rather than spelling out the rules for generation that needs to be considered a Critical Bulk Electric System Assets, Standard 1300 refers to another document (Policy 1.B). ECAR has modified the definition of "Most severe single contingency".

Using the proposed Std 1300 language from the multiple documents and regional definitions mean that almost all ABC's generating facilities fall under the rules of Standard 1300.

Is it NERC's intent that all generating stations should be subject to the rules of Standard 1300? If this is not NERC's intent, then the proposed language needs to be changed.

ABC recommends that all of the rules for identifying the critical bulk electric system assets and the critical cyber assets should be identified in one document, rather than using multiple documents subject to regional interpretations as used in Std 1300 version 1. Recommendation: On page 9, eliminate reference to NERC Policy 1.B in (iii) (A) and replace with this language: "…greater than or equal to 80% of the most severe single contingency loss."

ABC seeks clarification from NERC of the term "Most severe single contingency". Please use the following example:

Utility owns approximately 600 MW of a total 1300 MW generation site all in ECAR

Same utility owns 100 % of a 635 MW generation site

Which of the above should be identified as the largest "single contingency"? If the 635 MW site is used, generating units, which ABC does not consider critical, will be included in the list of "critical cyber assets."

ABC recommends that a good use for the FAQ's would be to provide additional examples, including some examples using how the requirements apply to jointly owned units (JOU's).

Page 9: Either fully explain or eliminate (iii) Generation (B) "…generating resources that when summed meet the criteria…"

Page 10: ABC believes the level of documentation and administrative control required by proposed Standard 1300 is extensive and imposes a significant operating cost on participants. Once again, this section contains requirements without any documented evidence that the expense to implement will enhance security or that there is a relevant threat, which will be mitigated by this level of documentation. Parts of the section are redundant to other requirements. ABC has designated two company officers that are responsible for the Cyber Security Policy and implementation. "Critical Bulk Electric system Asset and Critical Cyber Asset List Approval section," requires a properly dated record of senior management officer's approval of the list of critical bulk electric system assets. ABC recommends that requirements such as this be deleted unless evidence is shown which indicates direct security benefit. Recommendation: Eliminate Requirement (a) (3) " …A sr. management officer must approve the list of…" and also eliminate corresponding "Compliance Monitoring Process" (i) (3) (iv) page 11. The senior officers are responsible for implementation of the program and should not be required to sign off on each section of the document as each section is updated.

In the October 18 Webcast, NERC slides indicated a "3 step" approach to identifying the critical cyber assets. Standard 1300 lists (#1) Identify the Critical Bulk Electric System Assets and (#2) Identify Critical Cyber Assets. ABC seeks clarification from NERC regarding the three (3) steps referred to in the Webcast.

1303 – Personnel & Training

Page 13 "Awareness Program": Once again, this section contains requirements without any documented evidence that such requirements will enhance security. Requiring both training program and awareness program seems redundant and burdensome. ABC recommends that the awareness in inherent in training and is part of the training requirements. We recommend that the separate "Awareness" section be deleted.

Page 14 Access Changes:
By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1301 & 1306)
Need clarification & consistency from NERC on exactly WHAT the access change requirements are.
- 1301 states: "Responsible entities shall… ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."
- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)… and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.
- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who…are not allowed access…(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.
- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations…24 hours.

Regarding requirements for updating access records, ABC recommends:
1. The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat…Routine administrative changes …should be handled within three business days after occurrence."
2. The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.
3. If the item is used to identify non-compliance, all references throughout the document should reflect the revised requirements.

Page 14: Background Screening. The entire section on background screening, as written in Standard 1300, is problematic. For example:
- "…A minimum of Social Security Number verification…" Language as written will deny access to anyone except U.S. citizens. ABC recommends that the language requiring a social security number be deleted unless it is NERC's intent that only U.S. citizens and no one else is granted electronic or physical access.

NERC showed insight when, in their Responses to comments submitted during the balloting of the Urgent Action Cyber Security Standard 1200, NERC wrote: "…organizations are NOT required to conduct background investigations of existing employees given the fact that they have had the opportunity to observe and evaluate the behavior and work performance of those employees after they have been employed for a period of time." ABC again recognizes that Standard 1300 is a different standard from Standard 1200; however, the logic that provided the foundation for the previous NERC comment is sound. If the company has had an opportunity to observe the long service employee, the background screen requirement should be relaxed.

ABC recommends one of the following to replace proposed Standard 1300 language:
A. The requirement should include background screening for all individuals (employees and vendors) who seek approval for new permanent access to critical cyber assets.

Background screening on existing employees, previously approved for access, is appropriate if there is cause to suspect the individual of suspicious behavior.

Requiring the screening of all personnel every 5 years should be deleted.

B. If the above proposed language is not acceptable as an alternative by NERC, then ABC recommends language be inserted indicating that background screening requirements will be evaluated by the company involved, and the policy toward such screenings will be documented by that company. Company will be free to document policies such as: At Company's discretion, long service employees, which the Company has observed, may be grandfathered and background checks will not be done on these employees. Company will not be found in non-compliance for such a policy.

Page 13: Language states that a "higher level of background screening" should be conducted on personnel with access. ABC's background screening for new hires complies with the NERC requirements and other legal requirements. ABC does not agree that multiple levels of background screening are required. ABC recommends that the reference to multiple levels of background screening be deleted.

Page 13: Records: " …background screening of all personnel having access to critical cyber assets shall be provided for authorized inspection upon request." ABC does not agree that the background screen information obtained on all its employees will be provided to NERC inspectors. In the 10/18 Webcast NERC stated that it is not their intent that the contents of the background screening be provided to the inspectors. Recommendation: Improve language so that it is clear that contents of background screen need not be divulged to inspectors.

Page 15 (i) Standard 1300 language implies that background check lists & verifications are kept by operations groups responsible for the cyber security implementation. Such records will continue to be maintained by the Human Resource Department at ABC.

Page 13: Background screening: Proposed language states: "…contractors and service vendors, shall be subject to background screen prior to being granted unrestricted access to critical assets." Is it NERC's intention that they be granted unrestricted access after completing a background screen as stated in 1300?

1304 – Electronic Perimeter

Page 17 (a) (1) Electronic Security perimeter: Proposed language states "Communication links …are NOT part of the secured perimeter…However, end points of the communication links… are considered access points to the perimeter. Where there are non critical assets within the defined perimeter these non-critical assets must comply with the requirements…" Language is contradictory and confusing. Proposed language makes the asset and the end point critical assets and within the perimeter, but language excludes the communication line between them. The next sentence implies the communication line needs to be treated as though it is part of the perimeter. ABC seeks clarification.

Page 18: (b) (1) Electronic Security Perimeter:
ABC seeks clarification regarding from NERC regarding Frame Relay Access Devices (FRAD's) and modems connected to cyber assets. Are these considered "access points to the electronic security perimeter"?

If the FRAD's are considered 'within the perimeter' with the resulting requirements extending to the FRAD's, this is an excessive and unnecessary level of detail and will prove costly and burdensome without proven corresponding benefit.

Page 18: Measures (3): Monitoring Electronic Access Controls: Wording of this section, particularly the last sentence, is very confusing and needs clarification regarding exact requirements for documentation and for implementation of monitoring the access controls.
P. 19 (e) (3) Electronic Access Controls: Page 19 identifies a non-compliance item if "…not all transactions documented have records." ABC seeks clarification. If a transaction is documented, by definition, doesn't that mean the transaction has a record?
Page 17 Electronic Access Controls: "…non critical cyber assets (within the perimeter) must comply with the requirements of this standard." Different departments within the organization will handle different functions. Current language implies one rigid process to apply to both critical assets and non-critical assets, which may exist within the perimeter. Recommend that this be changed to: non-critical cyber assets within the perimeter must utilize similar electronic access controls.
1305 – Physical Perimeter

While ABC acknowledges that controls may be required, it does not seem appropriate for NERC to dictate the controls to be implemented. Example: Implement CCTV or Alarm System.

ABC's interpretation of current draft language in Section 1302 will result in almost all ABC generating plants being subject to these rules. Section 1305 then seeks to name the controls, which must be implemented at each asset location. No mention to a review of costs associated with such sweeping changes is even mentioned in any of the language. ABC believes it is appropriate to address the costs and corresponding benefits before moving forward with such a sweeping and costly initiative. ABC recommends that participants and NERC develop an estimate of the proposed cost to the industry before finalizing these requirements.

Generating plants control rooms may be manned 24 hours a day seven days a week. ABC seeks clarification and evidence of the need for the many controls, such as CCTV, which are specified in the document in these cases where facilities are manned.

Page 24 (6) Maintenance and testing of security systems to be retained for 1 yr. This involves corp. wide – Equipment Maintenance area. This is one more example of the costs, which must be considered before moving forward. These types of requirements are very costly to large organization because they impose enterprise wide requirements. Maintenance records on the security installation equipment will not be kept in Electric Operations areas. Requirements will need to be coordinated across groups responsible for equipment maintenance.

1306 – System Security management

While the list of physical controls to be implemented in the proposed section 1305 language represents a huge, solid, and obvious cost burden, requirements in section 1306 represent a less obvious but huge cost burden as well.

Once again, there is no evidence presented that there is a relevant threat, which will be mitigated, if these types of controls/documentation requirements are implemented. Also, once again, there is no indication if the idea of associated costs was even contemplated prior to writing the language requiring the controls/documentation.

ABC requests that evidence needs to be presented showing (1) a relevant threat will be mitigated if the controls outlined in this section are implemented (2) costs and benefits associated with requirements have been identified.

ABC is concerned that if money and resources are required for documentation requirements that yield no real enhancement to security, then less money and resources will be available for security measures that could truly yield benefit. Recommendation: Either significantly lessen requirements or eliminate many of the following.

Page 28: Archive backup information for a prolonged period of time and then test it annually to ensure it is recoverable. A definition of 'information' and 'archival information' should be provided. Archived information looses its value in time and may become irrelevant. Is NERC dictating records retention policy? What is the consequence if this does not occur? Requires extra work, but what is the point? Need better understanding of costs vs. benefits.

Page 28: Create Operating Status Monitoring tools. This section indicates the tools gauge 'performance.' Standard 1300 language contains no statement as to what these performance-monitoring tools are trying to gauge nor are any performance goals indicated. This would be costly to implement with no defined benefit or even goals for the tools. Requires extra work, but what is the point?

Page 28: Create Operating Status Monitoring tools: Language in the section implies that performance documentation is to be kept for every asset. This is not reasonable.

Page 27: Retention of system Logs: "All critical cyber security assets must generate an audit trail for all security related system events." In the case of local RTU's this is probably not possible.

Page 26: Test Procedure language as written is overly burdensome. Language implies that EVERYTHING needs to be tested. It is not realistic that EVERY minor change is documented in formal testing. FAQ's seem to conflict with Std. 1300 proposed language. Recommendation: Modify Standard 1300 language to imply levels similar to NERC's recent Standard 1300 FAQ posting.

Page 27: Testing "…provide a controlled environment for modifying ALL hardware and software for critical cyber assets." Since the Energy Management System is by nature a critical cyber asset, the language implies that EVERYTHING must be modified in a separate controlled environment. Current language is burdensome and not practical. Recommendation: Indicate a reasonable level for testing within the controlled environment. Use levels similar to those identified in NERC's recent Standard 1300 FAQ posting.

Page: 27 Test Procedure Measures: Language states, " …Critical cyber assets were tested for potential security vulnerabilities prior to be rolled into production…" It is unclear what 'potential vulnerabilities' are to be tested or how the tester is to know about them. Recommendation: Explain clearly or delete the reference.

Page 29: Integrity software: ABC is pursuing a course of isolating the Energy Management System from the corporate network. This path of isolation reduces threat from email, Internet use, etc. The language requires anti-virus versions be kept immediately up to date. In practice, this

conflicts with the work to isolate the EMS and presents un-necessary requirements since the EMS will be isolated from the source of the viruses.

Page 27: Security Patch Management: ABC seeks clarification of " …upgrades to critical cyber assets." If this language includes every upgrade, it is costly and over-burdensome without resulting security benefit.

Page 27: Created formalized change control & configuration management process: Entire section creates un-necessary and redundant requirements that are included in the Test Procedures requirements section of 1306.

Section 1306 Security Patch Management section presents additional problems for power plant control systems. For example,

Security Patch Management language (page 27) requires timely installation of applicable security patches and operating system upgrades.

Patches and upgrades (at the power plant) at ABC can only be applied during an outage of the control system.

ABC seeks clarification from NERC as to how all of Section 1306, including Security Patch Management, applies to power plant control systems. Will plants be expected to create more outages to keep up with requirements?

Page 28 (2) Account Management: "review access permissions within 5 working days. For involuntary terminations, …no more than 24 hours". By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 & 1301)

Need clarification & consistency from NERC on exactly WHAT the access change requirements are.

- 1301 states: "Responsible entities shall… ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."
- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)… and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.
- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who…are not allowed access…(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.
- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations…24 hours.

ABC recommends:

- The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat…Routine administrative changes …should be handled within three business days after occurrence."
- The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.
- If the requirement is used in the non-compliance section, then the non-compliance section should be consistent with revised requirements.

1307 & 1308- Response & Recovery Plans

Page 34:
1300 Language seems to imply NERC expects multiple plans to be created for Cyber Security. " …recovery plans associated with control centers will differ from those associated with power plants and substations." This level of detail may become too onerous. ABC seeks clarification from NERC if multiple plans are required. Once again, this will involve time, money and resources to create documentation at an un-precedented detail level with no indication that such a measure will increase real security.

If entities strictly follow the language proposed for 1307, they will be forced to create un-necessary documentation for very brief interruptions and for events, which were not malicious and did not create a disruption. NERC definitions provided the following:
NERC defines an "incident" as ANY physical or cyber event that disrupts or could lead to a disruption of the critical cyber assets.
Same section defines a "cyber security incident" as malicious or suspicious activities, which cause or may cause an incident.
Definition section does NOT include a definition of a "reportable incident"

The language of the entire 1307 section is written to apply to both incidents and cyber security incidents.
Once again, as we have seen in other sections, companies that attempt to follow these requirements will create costly levels of detail and documentation (for every incident which either creates a slight disruption or could lead to a disruption) with no proven direct benefit to security. Here are some examples:
Page 32 states, "…retain records of incidents and cyber security incidents for 3 calendar years." This includes but is not limited to:
o System and application log files
o Video and or physical access records
o Investigations and analysis performed
o Records of any action taken including recovery actions
o Records of all reportable incidents and subsequent reports
…make all records and documentation available for inspection."
Recommendation: Re-work the language so that it is clear at what level this degree of detailed documentation needs to be retained.

Page 34 (a) (3) "…update the recovery plans within 30 days of a system or procedural change and post the recovery plan contact information." This language is problematic in 2 areas:
1. It is not realistic to expect that the plan will be updated within 30 days of each procedural or system change.
2. ABC does not "post" contact information. NERC does not specify what type of "posting" they require. Further this requirement is contradictory to other NERC cyber security requirements. ABC regards emergency plans and contact information as critical cyber asset information. Information is treated as such.
ABC recommends that plans be updated annually and that contact information should be treated consistent with other information related to critical cyber assets.

Additional Comments on Format
- The numbering sequence is not accurate throughout the document, making it difficult to follow in some sections. Recommendation: A different consistent numbering system should be used or, at the least, the entire document should be reviewed for appropriate numbering. Examples include but are not limited to:
o See Page 9 (a) Requirements then Page 10 (g) Measures. Where are items (b), (c), (d), (e), & (f)?
o Page 13: All of Section 1303 need review
- Typing mistakes need to be corrected. Example: Page 15 "…doesn't not cover one of the …"

FAQ's Recently Posted by NERC

In addition to inserting requirements regarding separation of duties noted above, question 3 on page 9 of the FAQ document seeks to limit the definition of RTU's, that use a non-routable protocol. Standard 1300 implies that non-routable protocols are excluded. However, the answer to question 3 tightens the definition of what is excluded by adding additional requirements that may not apply to all non-routable protocols: "…have a master/slave synchronous polling method that cannot be used to access anything on the EMS and they use SBO command…" As noted above, it is not appropriate to introduce additional restrictions to the Standard language via the FAQ posting process.

ABC Implementation Timeline

After the Standard 1300 language and requirements are finalized, ABC estimates:

o 1.5 to 2 years to evaluate standard impact and what is to be included in compliance.
o This is dependent upon how much guidance is given by NERC in regards to specifics for equipment and facilities to be included.

o 3.5 to 4 years to implement and become compliant.

o Total of 5 to 6 years from acceptance of the standard until compliance is reached.
of the standard until compliance is reached.

From: DeGraffenried, Chris [mailto:Chris.DeGraffenried@nypa.gov]
Posted At: Wednesday, November 03, 2004 12:26 PM
Posted To: Standards
Conversation: Version 0 Comments - NPCCREV4CyberSecSTrd1300_NYPACommentForm.doc
Subject: Version 0 Comments - NPCCREV4CyberSecSTrd1300_NYPACommentForm.doc

See attached Word file.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name: Christopher L. de Graffenried		
Organization: NYPA		
Telephone: (914) 390-8134		
Email: degraffenried.c@nypa.gov		
NERC Region		**Registered Ballot Body Segment**
ERCOT **ECAR** **FRCC** **MAAC** **MAIN** **MAPP** **NPCC** **SERC** **SPP** **WECC** **NA - Not Applicable**		1 - Transmission Owners
		2 - RTOs, ISOs, Regional Reliability Councils
		3 - Load-serving Entities
		4 - Transmission-dependent Utilities
		5 - Electric Generators
		6 - Electricity Brokers, Aggregators, and Marketers
		7 - Large Electricity End Users
		8 - Small Electricity End Users
		9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

*** If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.**

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for

posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

Yes

No

Comments

NPCC's participating members recommend that the definition of Critical Cyber Assets be;

"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).

NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.

NPCC's participating members recommend changing the Incident definition from

"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."

to

"Incident: Any physical or cyber event that:

disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."

Question 2: Do you believe this standard is ready to go to ballot?

Yes

No

If No, what are the most significant issues the drafting team must reconsider?
NPCC's participating members feel there is much redrafting to be done to the standard and that the following items may be considered "show stoppers" by some.

Standard 1300 is based on what the critical BES assets are, which is defined in 1302.a.1. Per question 1, NPCC's participating members do not agree with that definition and have made suggestions as to what the Drafting Team may do to address the issue.

NPCC's participating members also believe the need to change the Incident definition, to the one shown in Question 1 is important.

As previously discussed and commented on in various forums, NPCC supports the NERC decision to move away from monetary sanctions.

NPCC's participating members have also expressed concern over the incremental administrative tasks and documentation requirements to be compliant with this standard and hopes the Standard Drafting Team will consider this during the development of the associated "Implementation Plan".

Throughout the document, the compliance levels should be updated to measure the proposed revisions suggested below. NPCC has made some recommendations in this regard.

There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected and recognized with consideration of this Standard.

The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to gauge the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. It is NPCC's hope that this will be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.

NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk and have made recommendations later in the form that will make this Section acceptable.

The references within the standard made to other portions of Standard 1300 are not correct. Without clear references, NPCC cannot determine if the document is acceptable or not. For example, 1301.a.3 says "as identified and classified in section 1.2." Where is this section? Each one of these incorrect references must be corrected.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
Correct references as covered in question 2.

Request clarification on what "information" is protected in 1301.a.2.

Change 1301.a.2 from;

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

to

"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets." (NPCC's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)

Change 1301.a.2.i from;

"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."

to

"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well." (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)

Change 1301.a.3 from;

"....entity's implementation of..."

to

"...entity's implementation and adherence of..."(NPCC's participating members believe it is important to stress that not only is it important to implement this Standard but to adhere to it as well.

The "24 hours" in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.

Change 1301.a.5.iv from;

"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."

to

"Responsible entities shall define procedures to ensure that modification,

suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven calendar days for all other users of a change in user access status. All access revocations/changes must be authorized and documented." (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)

change 1301.b.5.i from;

"5 days"

to

"7 calendar days" (NPCC's participating members believe that the 5 days may be not be sufficient time especially when considering holiday seasons)

1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency in the reference for retention of audit records.

1301.d.3.iv, request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor

1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii to ensure the protection of the identity/personal information of the affected individuals

Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor

1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.

1301.e.2.iii, change from;

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

to

"An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or" (NPCC believes it was the drafting team's itent to deploy the system rather than promote which has a different connotation associated with it,)

Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change "Executive Management" to "Senior Management" for consistency and clarity.

1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).

NPCC Participating Members believe that the concept of the Bulk Electric System and association "definitions" may not be appropriate to capture the intent of the standard. NPCC suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.

Replace the 1302 preamble and 1302.a.1 and 1302.a.2 as shown below, with;

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 which support the reliable operation of the bulk electric system.

The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.

(a) Requirements
Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.

(1) Critical Bulk Electric System Operating Functions and Tasks

The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:

* monitoring and control
* load and frequency control
* emergency actions
* contingency analysis
* arming of special protection systems
* power plant control
* substation control
* real-time information exchange

(2) Critical Cyber Assets

(i) In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:

A) The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.

B) The consequences of the Operating Function or Task being compromised (i.e. "highjacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.

C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.

D) Known risks associated with particular technologies

Change 1302.g.1 from;

"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."

to

"1 Critical Bulk Electric System Operating Functions and Tasks
(i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."

Change 1302.g.2.i from;

"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."

to

"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure." (NPCC believes the use of the word additional is of no value as used here and recommends removal).

Change 1302.g.5 from;

"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"

to

"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval" (NPCC believes that it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations of operations is lost.)

Change 1302.g.5.i from;

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

to

"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."

Change 1302;
"critical bulk electric system assets"

to

"critical bulk electric system operating functions and tasks"

1303, NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for the NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk.

The FAQ describes supervised access, 1303 does not touch upon this topic.

Change 1303.a.4 from "unrestricted access" to "authorized access".

Change 1303.a.4 title to "Personnel Risk Assessment."

Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."

Change 1303.a.2 from;

"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."

to

"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"

1303.a.4 from;

"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."

to

"Personnel Risk Assessment: There must be a documented company personnel risk assessment process."

Add to 1303 Measures.2, a training measures for disaster recovery (1308) and incident response planning (1307).

The numbering of 1303 starting with Measures needs correction.

1303 Measures 4.i, request clarification. Does this include third party personnel?

Change 1303.Measures.4.i from;

"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)."

to

"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 respective security perimeter(s)." (NPCC believes there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)

Change 1303.Measures.4.ii from;

"two business days"

to

"seven calendar days", per earlier comments and to keep consistent with FERC Order.

1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days", per earlier comments

1303.Measure.4., remove;

Subsections iv, v and vi.

and replace with

"There must be a documented company personnel risk assessment process." NPCC's participating members feel these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities."

1303.Compliance Monitoring Process.2, NPCC's participating members do not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria
is not applied, or" to "Personnel risk assement program is practiced, but not properly documented, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"

Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".

Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."

Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii

From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.

Change 1304 a.2 Electronic Access Controls:
to
"The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" 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)."

Change 1304 a.3 Monitoring Electronic Access Control:
to
"The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."

Change 1304 a.4 from;

"The responsible entity shall ensure that all documentation reflect current configurations and processes."

to

The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.

1304.a.4 Remove -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. (This is a measure and should be removed here)

Compliance Monitoring Process;
Change 1304.d.3 from;

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

to

"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"

Level of non compliance
"Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.

1305 Physical Security;

Eliminate the bulleted items in the Preamble to Section 1305-they appear in the Requirement section.

Replace 1305 a.1 with;
"Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.

* The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),
* The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and
* The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."

Change the following - (a) Requirements;
"(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."

to

"(3) Physical Access Controls: The responsible entity shall implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.
(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.
(5) (We recommend deleting this bullet as the intent is captured in bullet "4").
(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."

Change Measures;

"(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."

to

"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility." (NPCC believes the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)

In 1306.a.1, last paragraph, modify the second sentence to read as follows;

"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."

1306.a.2.ii change "pooding" and "puffing" to "putting" (it appears a pdf translation problem as some documents the group printed have it and others did not)

1306.a.2.ii remove "Generic" from the title

1306.a.2.iii, use "at least annually" instead of "at least semi-annually"

Change 1306.a.3 from;
"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."

to

"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets." (NPCC believes that it upgrades are a subset of the applicable security patches.)

Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."

Change 1306.a.4 from;

"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."

to

"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."

1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).

Change 1306.a.6 from

"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."

to

"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three calendar years in an exportable format, for possible use in further event analysis."

1306.a.7 Remove "Configuration Management" from the title

1303.a.8 Remove the word "inherent" it is not clear what is meant by it.

1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.

1306, remove 1306.a.11 since 1308 addresses back-up and recovery.

1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.

1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days".

1306.b.3, remove;

"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."

and change

"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."

to

"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."

1306 b.3 first sentence-eliminate the word "management".

1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.

1306.b.4 third sentence Change
"..so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."

to

"..mitigate risk of malicious software".

1306.b.4 Remove the second sentence.

1306.b.4 Replace the fourth sentence with;

"Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."

1306.b.5 remove the first sentence.
Based on the common use of third parties for outsourcing of this associated work of vulnerabilty assessment, it is not reasonable to maintain the information called for in sentence one.

Change 1306.b.6 from;

"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."

to

"Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis."

1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"

Remove 1306.b.11, since 1306.a.11 was removed.

1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."

1306.d.3.iii, change "system log files" to "audit trails"

1306.e.2, change "the monthly/quarterly reviews" to "the reviews"

1306.e.2.ii.C, change "anti-virus" to "malicious"

1306, the Compliance levels should be updated to match the above measures.

1307, spell out and provide clarification on the acronyms throughout.

Change 1307, from;

"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."

to

"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."

1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;

"Incident and Cyber Security Incident Reporting"

to

"Security Incident Reporting".

and also Change from;

"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

to

"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis & Warning (IAW) Program's Standard Operating Procedure (SOP)."

Refer to our definition of a "security incident", change 1307.b.5 from;

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

to

"The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements."

Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."

to

"The responsible entity shall retain records of security incidents for three calendar years."

Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."

to

"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."

1307.d.1 there is a 90 day reference that does not appear in the measures.

In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.

Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Version 0 Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:		
Organization:		
Telephone:		
Email:		
NERC Region		**Registered Ballot Body Segment**
☐ **ERCOT**	☐	1 - Transmission Owners
☐ **ECAR**	☐	2 - RTOs, ISOs, Regional Reliability Councils
☐ **FRCC**	☐	3 - Load-serving Entities
☐ **MAAC**	☐	4 - Transmission-dependent Utilities
☐ **MAIN**	☐	5 - Electric Generators
☐ **MAPP**	☐	6 - Electricity Brokers, Aggregators, and Marketers
☐ **NPCC**	☐	7 - Large Electricity End Users
☐ **SERC**	☐	8 - Small Electricity End Users
☐ **SPP**	☐	9 - Federal, State, Provincial Regulatory or other Government Entities
☐ **WECC**		
☐ **NA - Not Applicable**		

Group Comments (Complete this page if comments are from a group.)

Group Name: NERC Compliand and Certification Managers Committee

Lead Contact: **Mark Kuras**

Contact Organization: **MAAC**

Contact Segment: **2**

Contact Telephone: **610-666-8924**

Contact Email: **kuras@pjm.com**

Additional Member Name	Additional Member Organization	Region*	Segment*
Robert L. Dintelman	**WECC**	**WECC**	**2**
Ronald W. Ciesiel	**SPP**	**SPP**	**2**
Raymond Palmieri	**ECAR**	**ECAR**	**2**
Mark R. Henry	**ERCOT**	**ERCOT**	**2**
Linda Campbell	**FRCC**	**FRCC**	**2**
Joseph D. Willson	**MAAC**	**MAAC**	**2**
Norbert D. Mizwicki	**MAIN**	**MAIN**	**2**
Robert W. Millard	**MAIN**	**MAIN**	**2**
Sheldon L. Berg	**MAPP**	**MAPP**	**2**
William J. Head	**MAPP**	**MAPP**	**2**
Steve Rueckert	**WECC**	**WECC**	**2**
Michael A. DeLaura	**NERC**	**NERC**	**2**
David W. Hilt	**NERC**	**NERC**	**2**

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☒ Yes

☐ No

Comments

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
Entity-level deviation and or exception from the Standard requirements should not be allowed. The only differences allowed in the Standards Process Manual are Regional Differences. This would set a precidence that could make compliance monitoring very difficult or even impossible. Also, Distribution Providers should be subject to the requirements of the Standard and Load Serving Entities should not be subject to the requirements of the Standard.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
Some formatting needs to be considered. References to other section of the standard does not seem to line up with the actual numbering. For example a reference may say 1302.1.1. The actual numbering scheme is 1302(a)(1)(i). I would suggest using a decimal type numbering scheme like the reference.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	Benjamin T. Church, CISSP	
Organization:	Burns & McDonnell Engineering	
Telephone:	562-499-9304	
Email:	bchurch@burnsmcd.com	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT ☐ ECAR ☐ FRCC ☐ MAAC ☒ MAIN ☐ MAPP ☐ NPCC ☐ SERC ☐ SPP ☐ WECC ☐ NA - Not Applicable	☐	1 - Transmission Owners
	☐	2 - RTOs, ISOs, Regional Reliability Councils
	☐	3 - Load-serving Entities
	☐	4 - Transmission-dependent Utilities
	☐	5 - Electric Generators
	☐	6 - Electricity Brokers, Aggregators, and Marketers
	☐	7 - Large Electricity End Users
	☒	8 - Small Electricity End Users
	☐	9 - Federal, State, Provincial Regulatory or other Government Entities

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☒ Yes

☐ No

Comments

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
1. Implementation should be created and presented, at least in draft, form before the 1300 is balloted. The Implementation plan may place greater restrictions than previously considered for certain elements of 1300, given its rather ambigious language.

2. Greater clarification should be provided to the concept of Governance.

3. See Comments provided below for Question 3.

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments

1301 Security Management Controls

1301(a)(2) Information Protection
Also refer to the FAQ Section 1301 Question 3. Phrase (…information pertaining to or used by critical cyber assets) would require that the creation of an information protection strategy be applied to data used in EMS functions or any other Critical Cyber Asset and not simply data about Critical Cyber Assets.

Utilities would be required to undergo a very complicated process of classifying nearly all data at work within the responsible entity. Technical controls may not be available to enforce the classification system proposed in particular with respect to EMS platform vendors. Also, include the term Data Classification Model, as that is what is required by the information protection section and referenced in the FAQ.

1301 (a)(3) Roles & Responsibilities
This section should integrate better with the April 2004 Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations from the U.S.-Canada Power System Outage Task Force and include in the 1300 Cyber Security Standard the requirement to build a security functions which adhere to Recommendation 43. Designation of a member of Senior Management should be aligned with this recommendation. 1300 should mandate the creation of position or set of functions to be known as Chief or Cyber Security Officer with integrated responsibilities for both corporate IT as well as security for a utility's information systems (a.k.a. Critical Cyber Assets).

1301(a)(4) Governance
The governance section should also follow Recommendation #43 in terms of establishing relationships that enable executive direction of security environment. It may be more effective to integrate Governance and Roles & Responsibility sections. More detail and/or direction should be provided. Is NERC recommending or requiring the use of a control structure such as COBIT? In many cases controls include use of best practices, would adoption of ISO 17799 be sufficient under the Governance section?

The clarification provided in the FAQ Section 1300 Question 5 actually confuses the matter further. The description provided blurs the lines between standard information security program functions and traditional corporate / internal audit. Perhaps, by integrating 1301(1)(3) and 1301(a)(4) and labeling it Information Security Program and embedding some control language, and then pointing out specific interfaces to traditional audit functions, more of the Blackout recommendations could be adopted and clarity achieved.

Members of the security team should sit on key support committees or otherwise have oversight functions over processes such as Production Control (i.e. 1301(a)(6)), Change Control, Technology Selection, etc.

1301(a)(6) Authorization to Place into Production

Integrate with 1301(a)(4) and further define that part of the security control structure is an oversight function for placing systems into production. Otherwise move into section 1306.

1301(b)(5)(i) Change (within five days of a change) to (within 24 hours). If the control / management environment that was required in 1301(a)(4) is in place, the list of designated personnel authorized to grant access should be able to be updated within 24 hours.

1302 Critical Cyber Assets

1302(a) Critical Bulk Electric System Assets
One or a list of available and preferred Risk Assessment methodologies should be provided. Otherwise, NERC should recommend if not require the use of Department of Energy's Vulnerability Assessment Methodology: Electric Power Infrastructure available through the ESISAC. Otherwise more direction or decision flows such as those provided in 1302(a)(1) should be provided.

1301(a)(1)(i) Control Center
Should Control Centers be included in the section on Bulk Electric System Assets? Do Control Centers rely on cyber assets interfacing with Bulk Electric Systems Assets rather than act as a Bulk Electric System Asset themselves? Perhaps section 1302(2) should be expanded to provide for a more complete list of Cyber Assets, in particular those that interface within a Control Center, and the criteria for selecting Critical Cyber Assets.

1302 Security Management
1302(a)(1)(vii) Additional Critical Bulk Electric System Assets
Unless a consistent Risk Assessment methodology is applied then utilities may use this category to very broadly or too narrowly define CCAs. Given that more specific criteria is given in 1302(a)(1)(i-vi) perhaps either expand to better define (additional) or note the specific methodology to be utilized.

1302(2) Critical Cyber Assets

Utilizing the term routable protocol as a criteria for determining criticality represents a logical break. Criticality is a measurement of value to a utility in relation to its ability to support Critical Bulk Electric System Assets. The use of a routable communications protocol may represent elevated risk through inherent vulnerabilities in protocols such as TCP/IP, but is not a metric for criticality.

The definition of criticality is formed by simply those information systems which act in a primary support capacity for the identified Critical Bulk Electric System Assets. Otherwise, a matrix similar to the one provided for Critical Bulk Electric System Assets should be developed.

1302(2)(C) Dial-up Accessible
Too narrow of a definition given the variety of communication methods. Perhaps it should read as just non-routable protocol.

1302(3) Senior Management Approval

Is this the same person as the Senior Management in charge of the Cyber Security Policies in 1301(a)(3), if so how would a security management person be qualified to approve a list of Critical Bulk Electric System Assets? Assuming that the reference is to the same person, then given the

expertise necessary to approve a list of Critical Bulk Electric System assets, the de facto choice would be someone with a VP or equivalent title in Engineering and most likely not truly a security person. This then puts added pressure on the Governance section in 1301(a)(4).

1303 Personnel & Training

1303(b)(2) Training
Align with Blackout Recommendation 37. Training should be required for all IT personnel who have support missions for CCAs. IT support personnel should receive training of a like-kind that EMS support personnel receive. This should apply to IT personnel supporting CCAs other than the EMS as well.

1304 Electronic Security
At some point there should be a requirement to encrypt data used by CCAs.

1304(a)(2) Electronic Access Controls
What if the system being accessed does not have the ability to display banners? Consider a user accessing the EMS through a dedicated workstation. Unless the EMS vendor has programmed the capacity for a banner pop-up at log-on, no such banner will occur while engaged in the username / password Electronic Access Control at the application level. The requirement to have (…an appropriate use banner upon interactive access attempts) assumes a network environment which may not be in place.

Recommended language: An appropriate use banner must be physically mounted on the information device used to access the Critical Cyber Asset or otherwise represented electronically during interactive access attempts.

1304(a)(2) Electronic Access Controls
The phrase (..shall implement strong procedural or technical measures to ensure authenticity of the access party…) requires clarification and/or direction. While the FAQ in Section 1304 Question 5 attempts to clarify what is meant by strong authentication the concept is still too broad. If two-factor authentication, a known best practice, is ultimately required then it should be stated as such. If the typical control of username / password is not sufficient then alternatives should be presented and recommended.

In many cases vendors of CCAs may not be able to support the requirement of strong authentication in any form as most employ username / password as the solitary control. Therefore additional authentication, perhaps at the network level, maybe required.

1304(b)(1) Electronic Security Perimeter
Even though the FAQ in Section 1304 Question 4 indicates that firewalls are not required to form an ESP, perhaps greater clarity as to what constitutes (adequate controls) may be provided. Some form of additional perimeter control should be required and specified such as firewalls. Otherwise, a much better definition of (adequate control) should be provided. Loose definitions may allow utilities to sacrifice technology upgrades in the face of the rising cost of security.

1304(b)(2) Electronic Access Controls
If firewalls are not required, language should be included that stipulates that the same control which provided the ESP should not be included in providing Electronic Access Controls (EAC).

For example, if ACLs are employed on core switches to build an ESP, then they would be disqualified from providing security as an EAC.

1306 System Security Management
A requirement should be added to stipulate that the system management functions described in section 1306 should be performed by appropriate system or network administrators / engineers / analysts (i.e. IT Support personnel) and not by actual users of the CCAs. This is in-line with developing a governance model referenced in Blackout Recommendation 34.

1306(a) Requirements
Additional requirement should be added that requires that all IT Support procedures be documented if not already required by other requirements within this section. This is in-line with Blackout Recommendation 33. Likewise users / operators / analysts interacting with CCAs, other than IT Support personnel, should also have clearly documented processes and procedures.

1306(a)(2)(ii) Generic Account Management
Add to the requirement that in the event a generic account is technically required, the process / procedures performed under the generic account should be documented and a manual log of use should be kept and reviewed as electronic access logs will not be available for sufficient auditing.

The phrase (technically supported) should be clarified. The FAQ in Section 1306 Question 6 Paragraph 2 does not supply any additional clarification. The verbiage as presented in section 1306(a)(2)(ii) may be used to apply not to technical requirements, such as those required operations under a generic account mandated by the software itself, but rather as a matter of operational requirements. Meaning, that EMS users / operators / analysts may state that their current mode of operations requires the use of generic accounts even though the underlying software supports individual accounts.

Note, in Paragraph 1 in discussion of (direct logins as root / administrator), this should be changed to reflect the same verbiage as generic accounts. No one other than a system administrator, and not an actual user, should ever log on as root or administrator unless there are technical requirements that prevent use of individual system accounts. Also it should be noted that as a matter of separation of duties system administrators should not be actual application users, regardless of the level of knowledge of these users.

1307 Incident Response Planning

1307(a)(3) Requirements
Add to requirement a language aligning actions with the overall governance structure stipulated in 1301. Furthermore, require a specific type of incident response team structure one with a centralized Incident Coordinator / Manager preferably someone from the information security team.

The Incident Coordinator / Manager working with both IT and users/operators/analysts of CCAs should create an incident definition matrix. Therefore, the party ultimately responsible for declaring that a set of events properly constitute an Electronic Security Incident (ESI), and as such would be reportable to the ESISAC as part of the IAW SOP, would be the Incident Coordinator / Manager.

COMMENT FORM
Draft 1 of Proposed Cyber Security Standard (1300)

This form is to be used to submit comments on Draft 1 of the Cyber Security Standard (1300). Comments must be submitted by **November 1, 2004**. You may submit the completed form by emailing it to: sarcomm@nerc.com with the words "Cyber Security Standard Comments" in the subject line. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net on 609-452-8060.

ALL DATA ON THIS FORM WILL BE TRANSFERRED AUTOMATICALLY TO A DATABASE.

DO: **Do** enter text only, with no formatting or styles added.
Do use punctuation and capitalization as needed (except quotations).
Do use more than one form if responses do not fit in the spaces provided.
Do submit any formatted text or markups in a separate WORD file.

DO NOT: **Do not** insert tabs or paragraph returns in any data field.
Do not use numbering or bullets in any data field.
Do not use quotation marks in any data field.
Do not submit a response in an unprotected copy of this form.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:	John Currier(seg 5), Ron Donahey(seg3), Jose Quintas(seg 6), Paul Davis (seg 1)	
Organization:	Tampa Electric Company	
Telephone:	813-225-5287 Paul McClay	
Email:	PFMCCLAY@TECOENERGY.COM	
NERC Region		**Registered Ballot Body Segment**
☐ ERCOT	☒	1 - Transmission Owners
☐ ECAR	☐	2 - RTOs, ISOs, Regional Reliability Councils
☒ FRCC	☒	3 - Load-serving Entities
☐ MAAC	☐	4 - Transmission-dependent Utilities
☐ MAIN	☒	5 - Electric Generators
☐ MAPP	☒	6 - Electricity Brokers, Aggregators, and Marketers
☐ NPCC	☐	7 - Large Electricity End Users
☐ SERC	☐	8 - Small Electricity End Users
☐ SPP	☐	9 - Federal, State, Provincial Regulatory or other Government Entities
☐ WECC		
☐ NA - Not Applicable		

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact Email:

Additional Member Name	Additional Member Organization	Region*	Segment*

* If more than one Region or Segment applies, indicate the best fit for the purpose of these comments. Regional acronyms and segment numbers are shown on prior page.

Background Information:

Posted for comments is Draft 1 of the NERC Cyber Security Standard (1300). This draft does not include an implementation plan. An implementation plan will be developed at a later date for posting with a subsequent draft of this standard. The drafting team recognizes that this standard is an expansion of the Urgent Action Cyber Security Standard (1200) and will require an implementation plan that takes into account time needed by applicable entities to attain compliance with this standard. However, until the industry can reach consensus on the requirements and measures of this standard, drafting an implementation plan is not realistic.

Also posted for reference is a Frequently Asked Questions (FAQ) document. The intent of the FAQ is to provide examples (as suggested in comments to 1200 and the 1300 Standard Authorization Request) to help clarify the concepts addressed in this proposed standard.

When completed, Standard 1300 will be presented to the NERC registered ballot body for approval. If approved, the standard will replace the Urgent Action Cyber Security Standard (1200) approved by the industry in June 2003.

In developing Draft 1 of this standard, the drafting team reviewed and considered all comments submitted during the development of the urgent action cyber security standard and those submitted in response to Standard Authorization Request for this standard.

Question 1: Do you agree with the definitions included in Standard 1300?

☐ Yes

☒ No

Comments

SEE ATTACHED GENERAL & SPECIFIC COMMENTS…

Question 2: Do you believe this standard is ready to go to ballot?

☐ Yes

☒ No

If No, what are the most significant issues the drafting team must reconsider?
SEE ATTACHED GENERAL & SPECIFIC COMMENTS…

Question 3: Please enter any additional comments you have regarding Standard 1300 below.

Comments
SEE ATTACHED GENERAL & SPECIFIC COMMENTS…

"ATTACHED TAMPA ELECTRIC
GENERAL and SPECIFIC COMMENTS"
(as referenced in the file:
"Standard 1300 Comment Form from TEC")

Comments of the Tampa Electric Company
on
Proposed Draft NERC Standard 1300, Cyber Security

General Comments

Overall this standard is an improvement over the existing 1200 standard, especially with the inclusion of the FAQ document to assist with interpretation. However, where compliance is concerned, an organization must comply with the standard as written, and to our knowledge external documentation, such as the FAQ, is not a part of the standard. We feel that considerable work still exists to improve the wording to further clarify the standard, so that it can stand alone without the need of a FAQ for clarification.

The standard lacks an impact analysis (NERC & market participant cost of implementation, timing, etc.). We will have to submit to the FPSC/FERC for cost recovery of the costs to implement these standards. As such NERC should include an impact analysis of implementing the new standard. We normally view the NERC standards as Regulatory requirements since compliance is essentially, mandatory. In any other venue (Nationally, Regionally or Locally) approval of a Regulatory rule is done in consideration of both an impact analysis and the public record of comments of the proposed rule. It is certainly done at FERC and it should be done in the NERC process.

In addition, we have noted inconsistency and redundancy across sections of the standard, and inconsistency in some sections between requirements, measures and compliance. Often the measure is no more that a restatement of the requirement; other times it lists the requirements, where the requirement itself is vague. Non-compliance levels seem to be related to the requirements at times and at times are related to the measures. Backward references to which section of the standard non-compliance refers to might be helpful. For example in 1303, lists of personnel with access are not mentioned in the requirements, but appear in the measures. Periodic background screening would be a requirement, and having documentation of such background screening would be the measure. We would suggest a thorough review of requirements versus measures versus non-compliance.

The first item of the compliance monitoring process for all sections of the standards says, "and investigations upon complaint" please clarify - "upon complaint" - of who?

These comments and suggestions were developed based on many hours of discussion with Tampa Electric employees both in operating areas of the company and IT. Both the standard and FAQ should be reviewed to ensure that references correspond to the proper locations within the standard document. We do not feel this standard is ready to be distributed for balloting.

Definitions

~~With the expansion of scope to include generation and substation assets the definition of Physical Security Perimeter should be modified to include generation control rooms and substation control houses. (I'm not sure this paragraph and the one below are consistent nor what we'd like to see)~~

The definition of critical cyber assets should be reworded to clearly indicate that it includes only those facilities that would impact the ability to operate the bulk electric system. Where there are plant and transmission facilities that can be operated without the associated cyber assets, those cyber assets should not be considered "critical" cyber assets.

The definition of physical security boundaries should not be assumed to be a room. It should take into account that a cage or cabinet (which provides physical security and may be inside a computer room or other room) may be the boundary inside which critical cyber assets are stored.

Definition of security incident should be more specific. Any network scan or probe could be interpreted as an activity that "could have resulted" in an incident and these occur too frequently across the industry to have a manageable process if **all** were reported. We recommend dropping the phrase "or could have resulted" from this definition.

Add definitions in this section for Deviations, Exemptions, and Exceptions clearly stating the difference between these terms (if there is any) and how they apply to compliance reporting, i.e. are you fully compliant if you have an exemption from a standard? If all terms are intended to convey the same thing, use only one term in all subsequent sections. For instance, in section 1301 the use of the terms "exception, deviation and exemption" is inconsistent and what they are deviations to/from (requirements or policy) varies:

Requirements (a) (1) (3) **– "**deviations or exceptions from the requirements of this standard"
Measures (b) (1) – says "maintain documentation of" (iii) / "review all" (iv) "deviations or exemptions"
Compliance Monitoring Process (d) (3) (iii) - documentation of justification of deviations or exemptions
Levels of non-compliance – (e) (1) (iii) and (e) (3) (ii) "deviations to policy "

Section 1301 Security Mangement Controls

(a) (2) (i) Identification - "all information related to critical cyber assets" seems a bit broad. In (5) (i) you limit the information that the "access process" needs to deal with to "that information whose compromise could impact. reliability and/or availability…". We would like the wording of (a) (2) (i) to be similar:

> The responsible entity shall identify all 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, regardless of media type.

(a)(2)(iii) – Information Classification
Under generally accepted security best practices, an information classification program typically entails the classification of information into multiple categories (public, internal, confidential, top secret, etc), with separate handling procedures for security, retention, destruction etc. A program such as this can be very resource intensive and overly burdensome, which we do not feel should be the intent of this standard. This standard seems to be addressing only the protection aspect of such a program, and all information related to critical cyber assets (whose compromise would impact reliability, etc.) would likely fall into a single category as it relates to the protection of information. The intent of the standard should be to identify and protect such information, and we recommend that the use of a classification system or some other means to protect the information should be left up to the individual organization. Measures (b) (2) (iii) and (iv) would go away if this is changed.

(a)(3) – The terms, deviation and exception (used in paragraph 1), are unclear in the standard and in the FAQ. Is a deviation where an organization has implemented a compensating control when unable to meet the specific requirements of the standard, or when an organization has opted not to meet the requirements in the standard and accepts the risk related to this omission? If an organization has a deviation by using compensating controls, they might be considered in compliance, but if they have opted not to follow the standard and accept the risk, they might be considered non-compliant. This needs to be clarified, perhaps in the definitions, and made very clear when a deviation, exception, or exemption is acceptable from a compliance standpoint. See comment in the definitions section above.

(a) (4) Governance – This seems to be redundant.~~.~~ The senior management official named in (a) (3) has the responsibility to lead the implementation and the policy (a) (1) to manage governance. While the FAQ is helpful in what the senior management official might do, the standard is not and should not be prescriptive for how this is done. The governance requirement doesn't seem to add any value. Recommend deleting this statement and the associated measure (b) (4).

(a) (5) (ii) Not sure if the sentence, "all access authorizations must be documented", is saying you need to "document who may authorize access" (which would be redundant, since a list is a document) or that the accesses the authorizer permits need to be

documented, in which case this sentence seems to belong better in (a) (5) (i) as a requirement of the process.

(a) (5) (iv) Suggest wording change to indicate 24 hours applies only to "unfriendly terminations" not all changes. 3-5 days seems to be more appropriate for "friendly separations" and transfers.

(a) (6) Authorization to Place into Production – this paragraph starts with the requirement to identify controls for testing and "assessment" (whatever that means) of new or replacement systems… The 1301 section is called security management controls – testing of new systems doesn't seem to fit in this section unless you are specifically referring to testing of security for new or replacement systems only. Please clarify the wording.

This section also states that an approving authority must authorize and document that a system has passed "testing criteria". And ends with "the approving authority shall verify system meets minimal security configuration standards". What testing criteria does this refer to? Are they the controls for testing or something different? Is the intent of this section to ensure the system meets minimum **security** standards, that functionality is tested, that there are testing controls or all of the above? The test procedures referred to in 1306 are clearly for testing information security; are these same procedures? The intent in this section is unclear. Section (a) (6) should be reworded to clarify.

(**b) (1)** Cyber Security Policy Measures
The measures refer to deviations, yet the requirements do not cover deviations in the policy section (a) (1) but rather in the roles and responsibilities (a) (3) section. Are we to document deviations and exceptions to the organization's policy or to the cyber standard requirements? The requirements and measures should address deviations in the same sections.

(b) (2) Information Protection Measures – In **(i) and (ii)** delete the word "security" here or add to the requirements section- it was not used there. What is the difference between "reviewing" **(i)** the program annually and "assessing **(ii)** the program for compliance annually? Do you really need two measures here? How is "measure" **(iii)** different than the requirement to "document and implement a process.."

(b) (5) (iii) Appears to be a requirement versus a measure. Suggest moving to (a) (5) (ii)

(b) (6) (iii) What needs to be on the list appears to be a requirement versus a measure. Suggest moving to the requirements. It indicates changes to this list need to be documented in 48 hours; 5 days (such as for (b) (5) (i)) seems more reasonable and consistent.

(d) (3) (iv) Compliance monitoring process **–** This section is the first time use of the phrase "Audit and mitigation strategies" and "Audit results" appears. If this is referring to documentation of the information protection program review (or assessment if those

are different), then wording needs to be consistent. Also refers here to "information protection security program" – see comment related to (b) (2) above.

(e) (1)– Level 1 Non compliance –
(**iii)** Suggest you change "deviations to policy" to "deviations from requirements"

(iv) and **(v)** - refers here to "information protection security program" and separates review and assessment – see comments related to **(b) (2)**

(vi) seems redundant to the above.. Are the processes different than the "program"?

(e) (2) (iii) – "formal process to validate and promote systems to production" - this "formal process" is not specified in the requirements (a) (6) – only that you identify controls and have an approving authority. Same for **(e) (3) (iv)**

(e) (4) (xi) "Access revocations and change not accomplished within 24 hours." 3-5 days seems to be more appropriate for "friendly separations" and transfers. See comment on (a) (5) (iv).

1302 Critical Cyber Assets

(a) (1) (ii) The standard is referring to a term (IROL) that is not currently an approved term within the NERC operating policies. Is it the drafting team's assumption that this definition will be a part of the NERC policy by the time this standard is implemented, or will this definition and related definitions from the FAQ be included in the definitions for this standard?

(a) (1) (iii) (A) Reportable Disturbance criteria
Within a generating station, each unit may be controlled by separate non-connected distributed control systems but may be under the control of a common automated generation control (AGC) system from an energy control center. Does AGC qualify as a common system controlling generating resources for the purposes of this standard? If so, does the AGC need to be routable (TCP/IP) to make these resources qualify as critical cyber assets? We feel this should be clarified in the standard.

(a) (2) (i) **(A)** Critical Cyber Assets:
Revise From: The cyber asset supports a critical bulk electric system asset, and"
To: The cyber asset affects the reliability and operation of a critical bulk electric system asset, and"

Add to: **1302 (a) (2) (i)** as new item:
An isolated routable network (i..e closed IP network) located in a secure area that is not connected to a modem and~~or~~ has no~~any~~ other means of external access ~~by routable protocols shall be considered as a non-routable network. An isolated network that meets these requirements~~ shall be considered a non-critical cyber asset. As a note, in the

conference call of October 18th, Larry Bugh agreed with the person who suggested this. (See Question 5f in the summary of Q&A) ~~(Paul – this is a generation comment I don't understand… but have put here for your review; it conflicts with E)~~

(a) (2) (i) E) – the reference (1302.1.2.1) doesn't exist. Similar references that don't point to anything in this document appears in **1302 (g) (1) (i), (g) (3) (i), (g)(4)** (i).

(a) (2) (i) E) – refers to other cyber assets in same electronic security perimeter needing to be "protected" but section 1302 only addresses making lists. Should other cyber assets in the perimeter be on the lists? Why? The protection of those assets should be covered elsewhere, **if they need to be protected at all**. If they don't impact the running of critical bulk electric facilities, why do they need to be protected?

1303 Personnel & Training

Many of the measures within this section appear to be more like requirements than measures. For example, lists of personnel with access are not mentioned in the requirements, but appear in the measures. Periodic background screening would be a requirement, and having documentation of such background screening could be the measure. We would suggest a thorough review of this section.

Another example - The requirements and compliance sections indicate that records shall be kept on background screening, but the measures states records shall be kept for training.

It is unrealistic to track, do background screening, and train all personnel who ever walk by critical cyber assets. We recommend the following changes:
First paragraph – change "personnel having access" to personnel having "unescorted or unsupervised access"
(a) (2) Training – Change "All personnel having access to critical…" to "All personnel having unescorted or unsupervised access to critical"

(a) (3) Records – Change "of all personnel having access to critical…" to "of all personnel having unescorted or unsupervised access to critical.. "

(a) (4) Suggest changing wording from All personnel with access to critical cyber….being granted unrestricted access…." to "All personnel having unescorted or unsupervised access to critical cyber…… being granted ~~unrestricted~~ access"

(a) (4) Background Screening
The requirement for background screening will become particularly onerous and costly for many organizations. For example, in some areas of a generating station it is not possible to establish a discrete physical security perimeter around every critical cyber asset. During periods of construction/maintenance at a generating station, hundreds of contract laborers may be present and the requirement to background screen these personnel would significantly impact the cost and time required to complete construction

efforts. How should an organization address this issue and stay in compliance with the standard?

Note on the related FAQ - The FAQ for this section seems to be out of synch with the numbering in the standard.

(l) Measures (think this should have been **(b))**
(l) (2) – Training should be given based on the roles assigned to individuals not one-size-fits-all training for all personnel. For instance, not all personnel with access to cyber assets require training in recovery plans for cyber assets.

(l) (3) (i) Suggest changing wording from "all personnel with access to critical cyber" to "all personnel having unescorted or unsupervised access to critical cyber"

(l) (4) (i) Suggest changing wording from "all personnel with access to critical cyber" to "all personnel having unescorted or unsupervised access to critical cyber"

(l) (4) (ii) Background Screening- reference to 1303.2.4.1 – section doesn't exist. "Substantive change" is an un-defined term

(l) (4) (iii) Background Screening
It is unclear why measures (i, ii, iii) for the personnel list, update of the list, and access revocation is covered under background screening. Is this stating that access must only be removed for anyone whose change in status occurs as a result of the background screening? If this is not the case, we believe that 24 hours (note non-compliance states 2 days) is an unreasonable expectation for access revocation, except in the case where the individual represents a potential threat to the organization. In most large organizations transfers, changes in responsibilities and routine employee separation cannot be communicated to personnel responsible for physical and cyber access management within this timeframe, not to mention situations where the personnel may work for a 3rd party contracting firm. We recommend that at least 3 business days be allowed for routine personnel movement access changes.

(l) (4) (iv)
Suggest changing "being granted access" to "being granted unescorted or unsupervised access" it is not reasonable to have background checks on every vendor ever in a computer room. Social security number verification should not be a requirement as it eliminates foreign nationals.

(l) (4) (v) The Q&A indicates that **"**adverse employment actions" are related to the background screening, but this is not apparent in the way it is worded. Suggest making it more clear. Perhaps "adverse employment actions resulting from background screening results"….

(l) (4) (vi) This requirement for update screening of personnel every 5 years is onerous and extremely costly. In addition, it indicates lack of trust of our valued long term

employees and should be removed or changed to indicate criteria should be established within the background screening procedures for what might trigger the need for an update screening.

(m) – (p) is mis "numbered" – should be (c), (d), etc.
references in (n) (2) don't exists

(n) (2) The requirement exists to keep records on the background screening for the duration of employee employment. Does this mean the responsible entity must keep records on background screening for both employees and contract personnel? The FAQ indicates that the responsible entity must only ensure that background screening is performed for those third parties, in which case the responsible entity would not have those records. There appears to be inconsistency here. Many of our vendors have already indicated they will perform background checks, but will not provide records about their employees to us.

(n) (2) (i) bullet 3 – what checklist are you referring to??

(o) (1) (iii) – Should say Background "screening" not "investigation". (also in (o) (2) (v))

"Consistent selection criteria is not applied" – what is this referring to? Selection criteria is not mentioned in the requirements or the measures.

1304 Electronic Security

The opening paragraph of this section introduces a concept of assigning security levels to electronic perimeters; however, this does not follow through the remainder of the document. We recommend this be stricken as it does not add value to the standard.

(a) (1) Electronic security perimeter
It is unclear from the wording in this section what is meant by the terms "access point" and "end point". The following wording might make this section more clear (the term "access point" is also a candidate for the definitions section):

…..The responsible entity shall identify the electronic security perimeter(s) surrounding its critical cyber assets and all access points (firewalls, routers, modems, etc) into the perimeter(s). Omit the sentence, "Communication links connecting discrete electronic perimeters are not considered part of the security perimeter." Omit sentence, "Where there are also non-critical cyber assets….. " These previous sentences do not have anything to do with the perimeter.

(a) (2) Electronic access control
The FAQ (for 1304) Q3 refers to dial-in modems that have "proper access control and logging". The fragment (paragraph 2) needs to be finished, not sure what this is supposed to be saying. However, t~~T~~he requirements for dial-in modems need to be better defined. We know of no dial back modems that are designed for the substation environment (e.g.

must be DC powered and capable of handling severe electrical surge). We have tried to use office style modems (Hayes, US Robotics, etc.) in substation withll no success. The more rugged modems do not have any security features. We rely on password protection in the data switch, but they have no logging capability. How would this be addressed?

Also, if we are allowing access into the electronic security perimeter through a router, what do we need to do at the router to implement "strong procedural or technical measures to ensure authenticity"? A router or firewall will typically filter access based upon IP address, and a firewall can enforce session authentication (login) before access to the perimeter is allowed. The FAQ for this section (question 5) seems to imply that two factor authentication is required, which is not practical in many situations, and certainly not possible with many of the devices, such as modems which are in the field today.

What is an "interactive access attempt" and how does it differ from an "access attempt"?

"appropriate use banner" – please define.. If what I think it is, not all systems are technically capable of presenting such a banner.

(b) (4) references to 1304.2… refer to sections that don't exist.. check the numbering.

(d) (2) Eliminate exceptions in the sentence, "keep document revisions ~~and exceptions~~ and other security" – requirements don't mention exceptions. Change "other audit records such as access records" to "other access logs"

(e) The levels of noncompliance seem to be inconsistent. Level one is gap in logs for less than 7 days, but level 2 is no monitoring for 1 device for less than 1 day. It would appear that missing logs for 7 days is worse than not monitoring for less than 1 day, yet is a lower level of non-compliance.

1305 Physical Security

It is not clear why "different security levels **shall** be assigned" and what difference the security levels would make in implementing the requirements in this standard. The Q&A in this section #4 indicates the organization **may** establish higher levels. Seems like it should be optional – shall doesn't sound optional.

(a) Requirements
(a) (1) Requirement #1 appears to be in the wrong location (should be last since it references the above requirements?).

(a) (2) Can the nearest "4 wall boundaries" be defined as a cage or a locked cabinet ? If not consider changing this to "It is defined as the nearest physical boundary that can be physically secured…"
Securing a substation control house to provide a physical security perimeter is a problem. Many people need access to the control house for routine work. However, there may only

be one or two racks of equipment that are defined as a "Critical Cyber Asset". We need to secure those assets (RTU, router, etc) without causing unnecessary hindrances to routine substation operation.

Complying with these requirements as written will also be very difficult, costly and **dangerous** for our generating stations. The control rooms are centers of activity with the operations personnel monitoring and approving all activities occurring on-site. On most days this includes hundreds of contractors that must come to the control room to get HEC tagging, Hot Work or Confined Space Entry Permits approved The short term nature of the most contractor employees is such that maintaining lists and background screening of all is nearly impossible. If we create another area for this activity, then operations may not be able to monitor what all is taking place **causing operational and safety issues that may impact reliability**. Creating another area for this activity would also require the stations to hire additional employees to cover this location 24/7 (5 people per station).

(a) (5) recommend changing "technical and procedural mechanisms" to "technical **or** procedural mechanisms"

(b) Measures
(b) (1) Recommend changing "physical security methods" to "physical access controls" and moving this measure to the bottom of the measures.

(b) (4) Add "Human monitoring or observation: to the monitoring methods

Based on our previous suggestions re "escorted access", it is our understanding that:~~Add as Section **(b) (7): (Paul this is another one that really doesn't make sense to include from Generation)**~~

"By virtue of a r~~R~~oom~~s~~ containing critical cyber asset(s) being~~that are~~ staffed at all times, 24 hours per day, 7 days per week, personnel who enter these rooms are given~~are~~ "escorted" or "restricted" access as long as there is a formal shift handoff between authorized personnel and the room is capable of being secured in case of an emergency evacuation. . Thus personnel entering these rooms are exempted from the~~se~~ requirements for background checking, training, and logging physical access. ~~as long as there is a formal shift handoff between authorized personnel and the room is capable of being secured in case of an emergency evacuation." Maybe if we could be more specific about what they are exempted from it would make sense.. if they have escorted access because there are people in the room and the other changes in 1303 are accepted, we don't need to keep a log of supervised/escorted personnel that enters the room. That seems to me to be the only requirement they might be exempted from?~~
Is this a correct interpretation?

(d) (2) keep document revisions ~~and exceptions~~ and other security – requirements don't mention exceptions.

(d) (3) (ii) – Documents for ~~configuration~~, processes, etc. Configuration not mentioned in the requirements.

(e) The levels of non-compliance within this section and those within section 1304 should be more consistent with each other. This section specifies 1 week at level 1, one month at level 2 and 90 days at level 3, while 1304 is one week, less than one day, and less than one week at the same levels. Also the numbered references don't exist in the document.

(e) (1,2,3) (ii) Log retention is required for 90 days, but the non-compliance sections addresses gaps over a 1 year period. If the logs are retained for only 90 days how can you evaluate over a 1 year period?

1306 Systems Security Management

Change first sentence to: "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 that could affect critical cyber asset(s)."

(a) (1) modify sentence 2 to be more clear; Suggestion: Significant changes include security patches, firmware, cumulative service packs, and new release, upgrades, or versions of ~~to~~ operating systems, …….. …

(**a) (1)** delete the sentence "Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment." While this may be a good practice when available, this is not always technically possible. Some systems are so old, there is no way to recreate another similar environment. Also delete, the corresponding wording in the measure (b) (1)

(a) (2) (ii) Generic Account Management
Revise the last sentence to: "Where individual accounts are not supported or practical in order to maintain critical bulk electric system asset reliability, 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."

(a) (5) Delete controlled penetration testing- Controlled penetration testing should not be a requirement. These penetration tests (on older generation systems particularly) can cause system outages affecting the reliability of generating units and impacting the very thing we are trying to protect. Each utility should determine wh~~ich~~at are the best methods of identifying vulnerabilities.

(a) (9) This section indicates we shall "secure dial-up-modem connections, but lists no requirements for how to secure dial-up modems."

(b) (3) and (4) keeping the records related to monthly reviews on the inventory document, may not be the best place to maintain this information. Each utility should be able to determine where this information is retained.

(b) (4) Suggest changing last sentence for clarity to – Where integrity software is not available for a particular computer platform or where other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from viruses or ~~and~~ other malicious software, this must also be documented.

(b) (7) The documentation shall verify that ~~all~~ the responsible entity….

(b) (8 & 9) – "against the policy and documented configuration" - what "policy" are you referring to here? And both indicate we need to take "appropriate actions to secure" – who decides what is "appropriate?"

(b) (11) modify the end of 1st sentence to **– "…** retention schedule of all critical cyber assets' information backup data and tapes."

(d) (2) and (3) numbered references don't exist in document

1307 Incident Response Planning

(a) (4) The requirements section indicates that "the responsible entity shall report **all** incidents to the ESISAC in accordance with the Indications, Analysis and Warning Program (IAW) Standard Operating Procedures." The ESISAC program does not require all incidents be reported. Along with the suggested change in the security incident definition (see definitions section), we suggest changing this to "The responsible entity shall report to the ESISAC **security incidents meeting the reporting criteria** in accordance with the Indications, Analysis and Warning Program (IAW) Standard Operating Procedures."

Numbering is messed up – you have 2 (b) sections.

(d) (3) (ii) There may well be no cyber incidents reported to ESISAC, if none have occurred.. Suggest changing to "One or more cyber incidents meeting the **reporting criteri**a in accordance with the Indications, Analysis and Warning Program (IAW) Standard Operating Procedures were not reported to the ESISAC."

1308 Recovery Plans

The standard's purpose is Cyber Assets protection. In paragraph 1, we suggest changing "must establish recovery plans" to "must establish critical cyber asset recovery plans."

The language of paragraph 3 section appears to be expanding the scope well beyond the recovery of the cyber assets. Suggest removing the entire paragraph. This standard does not deal with recovering substations, generating plants, nor control center facilities.

(a) (3) "and post its recovery plan contact information" – post where?? For who? And why?

(a) (4) delete "that will be included in the security training and education program" and replace with "that will be provided to personnel with a role in the recovery"

(b) (2) change to "and adjust, if warranted, its response"

(d) (3) numbered references are incorrect

(e) (3) does not address "the types of events that are necessary**" –** this is very vague, please be more specific about what you mean.