

**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
<input type="checkbox"/> ERCOT	<input type="checkbox"/>	1 - Transmission Owners
<input type="checkbox"/> ECAR	<input checked="" type="checkbox"/>	2 - RTOs, ISOs, Regional Reliability Councils
<input type="checkbox"/> FRCC	<input type="checkbox"/>	3 - Load-serving Entities
<input type="checkbox"/> MAAC	<input type="checkbox"/>	4 - Transmission-dependent Utilities
<input type="checkbox"/> MAIN	<input type="checkbox"/>	5 - Electric Generators
<input type="checkbox"/> MAPP	<input type="checkbox"/>	6 - Electricity Brokers, Aggregators, and Marketers
<input type="checkbox"/> NPCC	<input type="checkbox"/>	7 - Large Electricity End Users
<input type="checkbox"/> SERC	<input type="checkbox"/>	8 - Small Electricity End Users
<input type="checkbox"/> SPP	<input type="checkbox"/>	9 - Federal, State, Provincial Regulatory or other Government Entities
<input type="checkbox"/> WECC		
<input type="checkbox"/> NA - Not Applicable		

Comment Form – Draft 1 of Cyber Security Standard (1300)

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.

<p>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.</p> <p>DEFINITIONS</p> <p>Cyber Assets: Those systems (including hardware, software, and data) and communication networks (including hardware, software, and data) associated with bulk electric system assets.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Responsible Entity: The organization performing the reliability function, as identified in the Reliability Function table of the Standard Authorization Request for this standard.</p> <p>Incident: Any physical or cyber event that:</p> <ul style="list-style-type: none"> • 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. <p>Security Incident: Any malicious or suspicious activities which are known to cause, or could have resulted in, an incident.</p>	<p style="text-align: center;">Comments</p> <p>General:</p> <p>Identification of the compliance administration/monitor is not clear. Believed to be the RROs. This could be made clearer in the standard?</p> <p>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.</p> <p>Incident: Delete second bullet. Because the first bullet sufficiently covers any incidents. “Attempt” dilutes the definition and could cause excessive reporting.</p> <p>Any malicious or suspicious activity which is known to have caused or could have resulted in an incident.</p>
--	---

<p>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 <i>Balancing Authority</i>, <i>Interchange Authority</i>, <i>Reliability Authority</i>, <i>Purchasing/Selling Entity</i>, and <i>Transmission Service Provider</i> refer to the entities performing these functions as defined in the Functional Model.</p>	
<p>1301 Security Management Controls</p>	
<p>(a) Requirements</p>	
<p>(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.</p>	
<p>(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.</p>	<p>Disaster recovery plans should be specifically identified.</p>
<p>(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.</p>	<p>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.</p> <p>The word “entity” should be “organization”</p>
<p>(iii) Protection Responsible entities must identify the information access limitations related to critical cyber assets based on classification level.</p>	<p>“as defined by the individual organizations” should be included after classification level, to read – “...classification level as defined by the individual organizations.”</p>

Comment Form – Draft 1 of Cyber Security Standard (1300)

<p>(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.</p>	<p>Where is 1.2?</p>
<p>(b) Measures</p>	
<p>(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.</p>	<p>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.</p>
<p>(d) Compliance Monitoring Process</p>	
<p>(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.</p>	<p>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.</p>

Comment Form – Draft 1 of Cyber Security Standard (1300)

<p>(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.</p>	
<p>1302 Critical Cyber Assets</p>	
<p>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.</p>	
<p>(a) Requirements</p>	
<p>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.</p>	<p>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.</p>
<p>(1) Critical Bulk Electric System Assets</p>	
<p>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:</p>	<p>Replace “electric grid” with “bulk electric system” for consistency.</p>

<p>(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.</p>	
<p>(2) Critical Cyber Assets</p>	
<p>(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.</p>	<p>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.</p>

Comment Form – Draft 1 of Cyber Security Standard (1300)

<p>(3) A senior management officer must approve the list of critical bulk electric system assets and the list of critical cyber assets.</p>	<p>The terms “senior management” and “officer” have legal meaning in companies. This should be clarified further.</p>
<p>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.</p>	
<p>(a) Requirements</p>	
<p>(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.</p>	<p>Using “escorted access” and “unescorted access” is better terminology than “unrestricted access” and is a better terminology to reinforce and enforce.</p>
<p>(l) Measures</p>	
<p>(4) Background Screening The responsible entity shall:</p>	
<p>(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.</p>	<p>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.</p>
<p>(o) Levels of Noncompliance</p>	
<p>(1) Level One</p>	

<p>(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.</p>	<p>(ii): This needs to align more closely with the previous benchmark of “24 hours” and escalate based on this benchmark.</p>
<p>1305 Physical Security</p>	
<p>(b) Measures</p>	
<p>(3) Physical Access Controls: The responsible entity shall implement one or more of the following physical access methods.</p> <ul style="list-style-type: none"> • 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). <p>Other Authentication</p> <ul style="list-style-type: none"> • Devices - Biometric, keypad, token, or other devices that are used to control access to the cyber asset through personnel authentication. <p>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.</p>	<p>“man trap” should be “Man-trap”</p>
<p>1306 Systems Security Management</p>	

Comment Form – Draft 1 of Cyber Security Standard (1300)

<p>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.</p>	
<p>(a) Requirements</p>	
<p>(3) Security Patch Management</p>	
<p>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.</p>	<p>The word ‘timely’ does not adequately reflect the risk management approach that should be used in applying patches.</p>
<p>(b) Measures</p>	
<p>(2) Account and Password Management</p>	
<p>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.</p>	<p>It is not reasonable to expect a manager to sit at a terminal or otherwise review all access permissions. Management must “ensure” the review.</p>
<p>(11) Back-up and Recovery</p>	
<p>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.</p>	<p>The company must identify in its policy a minimum retention period satisfactory to reconstruct a critical cyber asset.</p>
<p>(e) Levels of Noncompliance</p>	
<p>(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.</p>	<p>(i) and (ii): More clarity is required around these specific reviews.</p>

<p>(3) Level three:</p> <p>(i) Documents(s) exist, but more than three of the items specified are not covered.</p> <p>(ii) Test Procedures: Document(s) exist, but documentation verifying that changes to critical cyber assets were not tested in scope with the change.</p> <p>(iii) Password Management:</p> <p>A) Document(s) exist, but documentation verifying accounts and passwords comply with the policy does not exist and/or</p> <p>B) 5.3.3.2 Quarterly audits were not performed.</p> <p>(iv) Security Patch Management: Document exists, but records of security patch installations are incomplete.</p> <p>(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.</p> <p>(vi) Identification of Vulnerabilities and Responses:</p> <p>A) Document exists, but annual vulnerability assessment was not completed and/or</p> <p>B) Documentation verifying that the entity is taking appropriate actions to remediate potential vulnerabilities does not exist.</p> <p>(vii) Retention of Logs (operator, application, intrusion detection): A gap in the logs of greater than 7 days exists.</p> <p>(viii) Disabling Unused Network Services/Ports: Documents(s) exist, but a record of regular audits does not exist.</p> <p>(ix) Change Control and Configuration Management: N/A</p> <p>(x) Operating Status Monitoring Tools: N/A</p> <p>(xi) Backup and Recovery: Document exists, but record of annual restoration verification exercise does not exist.</p>	<p>(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.</p>
<p>1307 Incident Response Planning</p>	
<p>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.</p>	
<p>(a) Requirements</p>	

<p>(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:</p> <p>(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.</p> <p>(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.</p> <p>(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).</p>	<p>Some of the reviewers were not clear on what ESISAC meant. Should be spelled out.</p>
<p>1308 Recovery Plans</p> <p>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.</p> <p>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.</p> <p>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</p>	<p>This introduction is repetitive and redundant. It could be shortened to one paragraph and still be effective.</p>

Comment Form – Draft 1 of Cyber Security Standard (1300)

<p>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.</p>	
<p>(a) Requirements</p>	
<p>(1) The responsible entity shall create recovery plans for critical cyber assets and exercise its recovery plans at least annually.</p> <p>(2) The responsible entity shall specify the appropriate response to events of varying duration and severity that would trigger its recovery plans.</p> <p>(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.</p> <p>(4) The responsible entity shall develop training on its recovery plans that will be included in the security training and education program.</p>	<p>(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.</p>