

**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	
<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 checked="" 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

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.