

COMMENT FORM
DRAFT 2 OF PROPOSED CRITICAL INFRASTRUCTURE PROTECTION
STANDARDS
CIP-002-1 — CIP-009-1

Please use this form to submit comments on draft 2 of the Cyber Security Standards CIP-002-1 through CIP-009-1 as well as the definitions listed in Draft 2 of these standards. Comments must be submitted by **February 17, 2005**. 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 Mark Ladrow at mark.ladrow@nerc.net or (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:	Independent Electricity System Operator
Telephone:	905.855.6258
Email:	peter.henderson@ieso.ca
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 — Proposed Critical Infrastructure Protection Standards

Posted for comments is Draft 2 of the NERC Cyber Security Standards CIP-002-1 through CIP-009-1. While reviewing the comments to draft one of Standard 1300 the drafting team was advised that NERC was implementing a new numbering scheme and format devised for NERC Reliability Standards. This new format does not accommodate sections within a standard. Therefore, the drafting team divided Standard 1300 into eight separate standards corresponding to the eight sections of Standard 1300. The table below shows the relationship between the sections of Standard 1300 and the new, separate standards.

Old Section #	Topic	New Std #
1301	Security Management Controls	CIP-003-1
1302	Critical Cyber Assets	CIP-002-1
1303	Personnel and Training	CIP-004-1
1304	Electronic Security	CIP-005-1
1305	Physical Security	CIP-006-1
1306	Systems Security Management	CIP-007-1
1307	Incident Reporting and Response Planning	CIP-008-1
1308	Recovery Plans	CIP-009-1

When completed, Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP-006-1, CIP-007-1, CIP-008-1, and CIP-009-1 will be presented to the NERC registered ballot body for approval. If approved, these standards, as a package, will replace the urgent action cyber security standard (1200) approved by the industry in June 2003 and the definitions proposed in these standards will be added to the NERC Reliability Standards Glossary of Terms.

Cyber Security Standards Definitions

These draft standards contain a set of proposed definitions (repeated in each standard). Rather than soliciting comments on the definitions eight times, please provide your input regarding these definitions on this form. The definitions have been refined based on input received during the comment period for draft 1 of Standard 1300.

Question 1: After reviewing the definitions within these standards, please identify those with which you do not agree and please suggest alternative wording.

The definition of Critical Asset should be revised. The failure of virtually any facility, system or piece of equipment will cause some definable detrimental impact on the reliability or operability of the electric grid. The phrase, would have a detrimental impact on the reliability or operability of the electric grid should be revised to read, would have a significant impact on the reliability or operability of the electric grid.

CIP-002-1 — Cyber Security — Critical Cyber Assets

Question 2: Does this draft of the standard clearly communicate that, in order to identify critical cyber assets, one must use an appropriate assessment methodology applied to a particular entity's circumstances?

No

If no, please identify revisions necessary to make this clear.

Question 3: Do you believe Standard CIP-002-1 is ready to go to ballot?

No

If no, please describe the revision necessary to achieve a standard that you feel is ready to ballot. Please be specific regarding the revisions needed.

Please see specific comments in attached.

General Comments:

1)The group of standards still looks inconsistent in a number of areas:

- a)There are a number of instances where a requirement is established in one standard which covers the same ground as requirements in another standard, and where contradictory requirements result;
- b)The numbering of sections remains inconsistent;
- c)The time periods prescribed for activities such as document review and document revision are still inconsistent across the CIP 002 to 009 group of standards.
- d)It is clear that a professional technical writer has not looked at these standards to make it clear and homogenous.

These inconsistencies have caused much time to be wasted by review teams which is regrettable considering it could have been easily solved.

2)If an entity is found not to have properly identified its critical infrastructure in 002, will this, ipso facto, mean being assessed as non-compliant in the other remaining standards (since all other standards are built on the assumption that the entities' lists of critical cyber assets are definitive?

3)The set of standards does not clearly require a security and governance program if it is determined that there are no critical assets. The standards must require that a program exist regardless of whether critical assets exist. The standard should state that the entity must perform an annual review to reconfirm its position on cyber assets. As such, the order of 002 and 003 should be reversed.

4)Most references to unattended facilities do not seem to bear relevance on security measures to critical cyber assets. The requirement for making a distinction between attended and unattended assets should be reviewed.

Furthermore, if this distinction is deemed necessary, definitions should be provided for the term unattended. It is not clear whether a facility that is continuously monitored, or a facility that is manned frequently, but not continuously, is unattended.

5)Throughout these standards there are numerous instances where requirements are effectively first established in the Measures and/or Levels of Non-Compliance sections of the text. This is inappropriate. If a condition needs to be met to be fully compliant, that condition should be identified in the Requirements section. In particular, it should not be necessary to read descriptions of non-compliance to infer the requirements for full compliance.

6)In several of the draft standards, there are instances where levels of non-compliance are described in such a way that entities could simultaneously satisfy the conditions of more than one

Comment Form — Proposed Critical Infrastructure Protection Standards

level of non-compliance. Levels of non-compliance should be described as a set of mutually exclusive conditions in order to avoid confusion and inappropriate certification.

7) Requirements related to authorizing, controlling, monitoring, and auditing electronic and physical access to critical cyber assets are specified in several different standards. This is confusing at best, and has resulted in both duplication and contradiction. All requirements pertaining to access control should be specified in one standard for better consistency and clarity.

8) As a general rule, the frequency at which entities are required to review and update documentation should not be arbitrarily prescribed in these standards. Rather, the review frequency should be determined and documented by those entities based on risk management considerations. An appropriate Measure for such a requirement would be the presence or absence of a documented review frequency, with compliance being demonstrated by document review/update being performed at that defined frequency.

9) In a number of places, these standards are very prescriptive and appear to be inconsistent with, or at least appear not to contemplate, the application of a risk based approach to meeting an overall goal. Because of the high degree of specificity, some requirements may not be applicable to all Responsible Entities, and the intent of other requirements may be fully satisfied without meeting the requirement as worded. In situations where the intent of the requirement (or the purpose of the standard) can be satisfied without meeting the specific wording of one or more requirements, entities should be permitted to claim full compliance provided they document their rationale for doing so.

10) In a number of Standards, the text of the Data Retention portion of the Standard (under Compliance) contradicts the text in the subsequent Additional Compliance Information Section of the same Standard.

Comment Form — Proposed Critical Infrastructure Protection Standards

CIP-003-1 — Cyber Security — Security Management Controls

Question 4: Do you believe Standard CIP-003-1 is ready to go to ballot?

No

If no, please describe the revision necessary to achieve a standard that you feel is ready to ballot. Please be specific regarding the revisions needed.

Please see comments in Question 3 above and Specific comments in attached.

Comment Form — Proposed Critical Infrastructure Protection Standards

CIP-004-1 — Cyber Security — Personnel and Training

Question 5: Do you believe Standard CIP-004-1 is ready to go to ballot?

No

If no, please describe the revision necessary to achieve a standard that you feel is ready to ballot. Please be specific regarding the revisions needed.

Please see comments in Question 3 above and Specific comments in attached

Comment Form — Proposed Critical Infrastructure Protection Standards

CIP-005-1 — Cyber Security — Electronic Security

Question 6: Do you believe Standard CIP-005-1 is ready to go to ballot?

No

If no, please describe the revision necessary to achieve a standard that you feel is ready to ballot. Please be specific regarding the revisions needed.

[Please see comments in Question 3 above and Specific comments in attached](#)

Comment Form — Proposed Critical Infrastructure Protection Standards

CIP-006-1 — Cyber Security — Physical Security

Question 7: Do you believe Standard CIP-006-1 is ready to go to ballot?

No

If no, please describe the revision necessary to achieve a standard that you feel is ready to ballot. Please be specific regarding the revisions needed.

Please see comments in Question 3 above and Specific comments in attached

CIP-007-1 — Cyber Security — Systems Security Management

Question 8: Do you believe Standard CIP-007-1 is ready to go to ballot?

No

If no, please describe the revision necessary to achieve a standard that you feel is ready to ballot. Please be specific regarding the revisions needed.

Please see comments in Question 3 above and Specific comments in attached

Comment Form — Proposed Critical Infrastructure Protection Standards

CIP-008-1 — Cyber Security — Incident Reporting and Response Planning

Question 9: Do you believe Standard CIP-008-1 is ready to go to ballot?

No

If no, please describe the revision necessary to achieve a standard that you feel is ready to ballot. Please be specific regarding the revisions needed.

Please see comments in Question 3 above and Specific comments in attached

Comment Form — Proposed Critical Infrastructure Protection Standards

CIP-009-1 — Cyber Security — Recovery Plans

Question 10: Do you believe Standard CIP-009-1 is ready to go to ballot?

No

If no, please describe the revision necessary to achieve a standard that you feel is ready to ballot. Please be specific regarding the revisions needed.

Please see comments in Question 3 above and Specific comments in attached

Question 11: Does draft 1 of the Implementation Plan for the Cyber Security Standards allow enough time for compliance?

No

If no, please identify specific requirements by standard and by functional entity that should change and identify the appropriate compliance time frame.

Since the standard will not become official before October 1, 2005, it is unrealistic to expect an acceptable level of auditable compliance in Q1 2006 for the following reasons:

- NERC CIP 002 through CIP-009 establish much deeper and wider requirements than NERC 1200 and will require a significant compliance effort even from those already in full compliance with NERC 1200.
- No budgeting can typically be done until the standards are confirmed and solidified.
- Most budgets are confirmed four or five months prior to the fiscal target year.

Since NERC 1200 standards are in place and companies typically use cyber security standards as good business practices, a gap in the effective dates of the standards would have little to no impact and should be acceptable in view of the development of this new and major standard.

The implementation plan should recognize typical corporate fiscal planning processes.

The Implementation Plan should be revised as follows:

Change the year 2006 to 2007 in the first group of columns, and make corresponding changes to the year in subsequent columns by adding one year. In the first column, for control centers (in the year 2007 after having made the change noted previously) change AC (auditably compliant) to SC (substantially compliant) in all instances.

A good requirement would be to require that a corporate implementation plan for reaching auditable compliance be submitted by Q2 2006. It should be accompanied by a statement that the entity will remain compliant with NERC 1200 during that period on a self-certification basis.

Recommendation: Throughout these standards, a requirement is established to be able to provide up to three years of records for examination on request of an auditor. The wording of the standards or of the implementation plan should contemplate that entities may legitimately not have fully 3 years of records to submit until 3 years after they are required to come into Auditable Compliance. It may be suitable to require entities to identify the dates when the document retention processes will be deemed to begin as part of the implementation plan suggested above.