

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:		
Organization:		
Telephone:		
Email:		
NERC Region		Registered Ballot Body Segment
<input type="checkbox"/> ERCOT	<input type="checkbox"/>	1 - Transmission Owners
<input type="checkbox"/> ECAR	<input 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"/>	
<input type="checkbox"/> NA - Not Applicable	<input type="checkbox"/>	

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.

[No comments on these definitions.](#)

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?

Yes

No

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

Comment Form — Proposed Critical Infrastructure Protection Standards

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

Yes

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 attached comments in document titled Cyber Security Standards CIP 002-009 Table ISORTOCOUNCIL.doc.

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?

Yes

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 attached comments in document titled Cyber Security Standards CIP 002-009 Table ISORTOCOUNCIL.doc.

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

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

Yes

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 attached comments in document titled Cyber Security Standards CIP 002-009 Table ISORTOCOUNCIL.doc.

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?

Yes

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 attached comments in document titled Cyber Security Standards CIP 002-009 Table ISORTOCOUNCIL.doc.

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?

Yes

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 attached comments in document titled Cyber Security Standards CIP 002-009 Table ISORTOCOUNCIL.doc.

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

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

Yes

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 attached comments in document titled Cyber Security Standards CIP 002-009 Table ISORTOCOUNCIL.doc.

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?

Yes

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 attached comments in document titled Cyber Security Standards CIP 002-009 Table ISORTOCOUNCIL.doc.

CIP-009-1 — Cyber Security — Recovery Plans

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

Yes

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 attached comments in document titled Cyber Security Standards CIP 002-009 Table ISORTOCOUNCIL.doc.

Comment Form — Proposed Critical Infrastructure Protection Standards

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

Yes

No

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

Please see attached comments in document titled Cyber Security Implementation Plan Final Table ISORTOCOUNCIL.doc.