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**
☐ **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: 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**	**SERC**	**9**
David A. Wright	**Public Service Commission of SC**	**SERC**	**9**
Randy Mitchell	**Public Service Commission of SC**	**SERC**	**9**
Elizabeth B. Fleming	**Public Service Commission of SC**	**SERC**	**9**
G. O'Neal Hamilton	**Public Service Commission of SC**	**SERC**	**9**
Mignon L. Clyburn	**Public Service Commission of SC**	**SERC**	**9**
C. Robert Moseley	**Public Service Commission of SC**	**SERC**	**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.

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.

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.

However, the PSCSC reiterates its view that the approach in all the standards being reviewed appears to be compliance-based rather than performance-based. Is the objective having a plan and procedures on hand, or a reliable system? The PSCSC maintains that the real objective is reliability, and not readily available plans and procedures. The real measure of success is effective implementation of the plans and procedures such that reliability is not compromised.

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.

However, the PSCSC reiterates its view that the approach in all the standards being reviewed appears to be compliance-based rather than performance-based. Is the objective having a plan and procedures on hand, or a reliable system? The PSCSC maintains that the real objective is reliability, and not readily available plans and procedures. The real measure of success is effective implementation of the plans and procedures such that reliability is not compromised.

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.

However, the PSCSC reiterates its view that the approach in all the standards being reviewed appears to be compliance-based rather than performance-based. Is the objective having a plan and procedures on hand, or a reliable system? The PSCSC maintains that the real objective is reliability, and not readily available plans and procedures. The real measure of success is effective implementation of the plans and procedures such that reliability is not compromised.

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.

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 rather than within 24 hours as proposed.

The PSCSC reiterates its view that the approach in all the standards being reviewed appears to be compliance-based rather than performance-based. Is the objective having a plan and procedures on hand, or a reliable system? The PSCSC maintains that the real objective is reliability, and not readily available plans and procedures. The real measure of success is effective implementation of the plans and procedures such that reliability is not compromised.

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.

However, the PSCSC reiterates its view that the approach in all the standards being reviewed appears to be compliance-based rather than performance-based. Is the objective having a plan and procedures on hand, or a reliable system? The PSCSC maintains that the real objective is reliability, and not readily available plans and procedures. The real measure of success is effective implementation of the plans and procedures such that reliability is not compromised.

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.

However, the PSCSC reiterates its view that the approach in all the standards being reviewed appears to be compliance-based rather than performance-based. Is the objective having a plan and procedures on hand, or a reliable system? The PSCSC maintains that the real objective is reliability, and not readily available plans and procedures. The real measure of success is effective implementation of the plans and procedures such that reliability is not compromised.

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.

However, the PSCSC reiterates its view that the approach in all the standards being reviewed appears to be compliance-based rather than performance-based. Is the objective having a plan and procedures on hand, or a reliable system? The PSCSC maintains that the real objective is reliability, and not readily available plans and procedures. The real measure of success is effective implementation of the plans and procedures such that reliability is not compromised.

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.

However, the PSCSC reiterates its view that the approach in all the standards being reviewed appears to be compliance-based rather than performance-based. Is the objective having a plan and procedures on hand, or a reliable system? The PSCSC maintains that the real objective is reliability, and not readily available plans and procedures. The real measure of success is effective implementation of the plans and procedures such that reliability is not compromised.

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.

However, the PSCSC reiterates its view that the approach in all the standards being reviewed appears to be compliance-based rather than performance-based. Is the objective having a plan and procedures on hand, or a reliable system? The PSCSC maintains that the real objective is reliability, and not readily available plans and procedures. The real measure of success is effective implementation of the plans and procedures such that reliability is not compromised.

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.

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:	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.

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.

None.

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.

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.

This new standard imposes a significant overhead on smaller utilities and control areas that can not be justified by loss of those systems to the interconnected grid. The purpose statement indicates the critical assets should adversely impact the reliable operation of the critical bulk electric system assets. The standard should exempt any electric utility or control area with less than 1% connected load (estimated peak) or less than 1% of generation resources in the interconnection to which they are synchronized. As an example, the Eastern Interconnection is approximately 605,000 MW, so any "Responsible Entity" with less than approximately 6050 MW in the Eastern Interconnection would be exempt.

Under section R2.1 - The Cyber Asset uses a routable protocol - describe intent of this section to more accurately depict the threat the standard is protecting against. Routable protocols can be secured, and non-routable protocols can be hacked, tapped, spoofed, etc.

Unders section C. Measures, M4 - Does the “or” mean that we can choose one method or the other, or that both methods must be followed?

Unders section C. Measures, M4 - What is meant by a “modification” of a critical cyber asset?

Under section C. Measures, M6 - does the senior management officer need to approve "modifications" (as used in M4) to critical cyber assets?

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.

Under section R2.1 - A few SCADA vendors exist that provide systems across the globe. SCADA systems are used around the world and the majority of the documentation that will be classified by this document is readily available to "the bad guy".

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.

Under section M4.6 - Delete the requirement for update screenings every five years and require the update screenings for cause only.

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.

Under section R1. - What constitutes a secure gateway across the electronic security perimeter? If a firewall can be used and an entitity uses a firewall in conjuction with a routable protocol, does this conflict with requirements in CIP-002-1, R2.1

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.

Under section M5 - Manual logging - what constitutes human observation or remote verification?

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.

Requirement R1 states to test for known security vulnerablilities. This means we must have the malicious software to run the test and the expertise. This is not practical nor logical. If Microsoft puts out a patch for a known vulnerability, we should not have to test using the malicious software. What if the problem is for a vulnerability and the malicious software hasn't been developed yet - are we suppose to develop the malicious software to use for testing? We should test our critical cyber asset to make sure their patch doesn't fail ot corrupt the system, but we shouldn't have to test the malicious software.

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.

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.

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.

The implementation schedule is too aggressive. Delay implementation at least one year or please consider an intial implementation of a much smaller scope to include control centers (CIP-002-1, R1.1.1 and R1.1.2), with full implementation over several years of other critical assets (CIP-002-1, R1.1.3 through R1.1.9).

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:	Todd Thompson	
Organization:	Southwest Power Pool	
Telephone:	(501) 614-3286	
Email:	tthompson@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.

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 the 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.

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

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

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

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

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

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

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

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

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

Implementation Plan
for Cyber Security Standards
CIP-002-1 through CIP-009-1

The intent of the proposed NERC cyber security standard is to ensure that all entities responsible for the reliability of the bulk electric systems of North America identify and protect critical cyber assets that control or could impact the reliability of the bulk electric systems. This implementation plan is based on the following assumptions; Cyber Security Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP006-1, CIP-007-1, CIP-008-1, and CIP-009-1 are approved by the ballot body and the NERC Board of Trustees no later than September 1, 2005. The NERC Functional Model is implemented in concert with the passage of the Version 0 standards. Entities have registered to the NERC Functional Model. Cyber Security Standards CIP-002-1 through CIP-009-1 become effective October 1, 2005. To provide time for responsible entities to examine their policies and procedures, to assemble the necessary documentation, and to meet the requirements of these standards, compliance assessment will begin starting in 2006. Implementation Schedule Beginning with the first quarter of 2006, NERC and its Regions will develop self-certification forms as part of their compliance and enforcement programs. The Regions will distribute these forms to the applicable functional entities within their respective Regions. Regions may ask other entities to provide self-certification forms if they believe they are performing one of the	The following is the position of the ISO/RTO Council Members: Since the standard will not become official before October 1, 2005, it is not realistic to expect an acceptable level of auditable compliance in Q1 2006. • NERC CIP 002-009 is much deeper and wider than NERC 1200 and will require a significant compliance effort. • 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 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. Change 2006 to 2007 (and successive columns) and change from auditably to substantially compliant. A good requirement would be to require a corporate implementation plan for compliance 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: The entity must identify the dates when the document retention processes must begin to be compliant with

functions identified in the standard. In such cases, the completion of a self-certification form by those other entities will be voluntary. All applicable entities will complete and submit the appropriate Regional self-certification forms, indicating their compliance, or degree of non-compliance, to the requirements of these standards. These self-certification forms will be submitted to the appropriate NERC Regional Reliability Council, which will hold the individual responses as confidential. It will be the responsibility of the Regional Compliance Manager to summarize the results of the self-certification and provide that summary to the NERC Compliance Program. Responsibility for compliance with these standards remains with the "Responsible Entity". The following table identifies when entities must be Auditably Compliant (AC) or Substantially Compliant (SC) with a requirement. Auditably Compliant means the entity meets the full intent of the requirement and can prove compliance to an auditor. The intent of the proposed NERC cyber security standard is to ensure that all entities responsible for the reliability of the bulk electric systems of North America identify and protect critical cyber assets that control or could impact the reliability of the bulk electric systems. This implementation plan is based on the following assumptions; Cyber Security Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP006-1, CIP-007-1, CIP-008-1, and CIP-009-1 are approved by the ballot body and the NERC Board of Trustees no later than September 1, 2005. The NERC Functional Model is implemented in concert with the passage of	the standard.

the Version 0 standards. Entities have registered to the NERC Functional Model. Cyber Security Standards CIP-002-1 through CIP-009-1 become effective October 1, 2005. To provide time for responsible entities to examine their policies and procedures, to assemble the necessary documentation, and to meet the requirements of these standards, compliance assessment will begin starting in 2006. Implementation Schedule Beginning with the first quarter of 2006, NERC and its Regions will develop self-certification forms as part of their compliance and enforcement programs. The Regions will distribute these forms to the applicable functional entities within their respective Regions. Regions may ask` other entities to provide self-certification forms if they believe they are performing one of the functions identified in the standard. In such cases, the completion of a self-certification form by those other entities will be voluntary. All applicable entities will complete and submit the appropriate Regional self-certification forms, indicating their compliance, or degree of non-compliance, to the requirements of these standards. These self-certification forms will be submitted to the appropriate NERC Regional Reliability Council, which will hold the individual responses as confidential. It will be the responsibility of the Regional Compliance Manager to summarize the results of the self-certification and provide that summary to the NERC Compliance Program. Responsibility for compliance with these standards remains with the “Responsible Entity”. The following table identifies when entities	

must be Auditably Compliant (AC) or Substantially Compliant (SC) with a requirement. Auditably Compliant means the entity meets the full intent of the requirement and can prove compliance to an auditor. Substantially Compliant means an entity has begun the process to become compliant with a requirement, but is not yet Auditably Compliant. The table has two sections for each standard. The first section defines the implementation schedule for Balancing Authorities (BA) and Reliability Coordinators (RC). The second section defines the implementation schedule for Interchange Authorities (IA), Transmission Providers (TP), Transmission Owners (TO), Transmission Operators (TOP), Generation Owners (GO), Generation Operators (GOP) and Load Serving Entities (LSE).	

Compliance Schedule for Standards CIP-002-1 through CIP-009-1

	1st Qtr		1st Qtr 2007		2008 & Beyond	
Requi	Contr	Other Facilit	Control	Other Facilit	Control	Other Facilities
Standard CIP-002-1 – Critical Cyber Assets BA & RC						
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
Standard CIP-002-1 – Critical Cyber Assets IA, TP, TO, TOP, GO, GOP, LSE						
F	SC	SC	AC	AC	AC	AC
F	SC	SC	AC	AC	AC	AC
F	SC	SC	AC	AC	AC	AC
F	SC	SC	AC	AC	AC	AC
Standard CIP-003-1 – Security Management Controls						
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC

Standard CIP-003-1 – Security Management Controls						
F	SC	SC	AC	AC	AC	AC
F	SC	SC	AC	AC	AC	AC
F	SC	SC	AC	AC	AC	AC
F	SC	SC	AC	AC	AC	AC
F	SC	SC	AC	AC	AC	AC
Standard CIP-004-1 – Personnel & Training BA & RC						
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC

	1st Qtr 2006		1st Qtr 2007		2008 & Beyond	
Requirement	Control	Other Facilities	Control	Other Facilities	Control	Other Facilities
R4	SC	SC	SC	SC	AC	AC
Standard CIP-004-1 – Personnel & Training IA, TP, TO, TOP, GO, GOP, LSE						
R1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	SC	SC	AC	AC
Standard CIP-005-1 – Electronic Security BA & RC						
R1	AC	SC	AC	AC	AC	AC
R2	AC	SC	AC	AC	AC	AC
R3	AC	SC	AC	AC	AC	AC
R4	AC	SC	AC	AC	AC	AC
R5	AC	SC	AC	AC	AC	AC
R6	AC	SC	AC	AC	AC	AC
Standard CIP-005-1 – Electronic Security IA, TP, TO, TOP, GO, GOP, LSE						
R1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	AC	AC	AC	AC
R5	SC	SC	AC	AC	AC	AC
R6	SC	SC	AC	AC	AC	AC
Standard CIP-006-1 – Physical Security BA & RC						
R1	AC	SC	AC	AC	AC	AC
R2	AC	SC	AC	AC	AC	AC
R3	AC	SC	AC	AC	AC	AC
R4	AC	SC	AC	AC	AC	AC
R5	AC	SC	AC	AC	AC	AC
R6	AC	SC	AC	AC	AC	AC
Standard CIP-006-1 – Physical Security IA, TP, TO, TOP, GO, GOP, LSE						
R1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	AC	AC	AC	AC
R5	SC	SC	AC	AC	AC	AC
R6	SC	SC	AC	AC	AC	AC
Standard CIP-007-1 – Systems Security Management						

	1st Qtr 2006		1st Qtr 2007		2008 & Beyond	
COMM	Control	Other Facilit	Control	Other Facilit	Control	Other Facilit
R4	AC	SC	AC	AC	AC	AC
R5	AC	SC	AC	AC	AC	AC
Standard CIP-009-1 – Recovery Plans IA, TP, TO, TOP, GO, GOP, LSE						
1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	AC	AC	AC	AC
R5	SC	SC	AC	AC	AC	AC

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAC approves Standard 1300 SAR, draft 1 posting (July 1, 2003)
2. SAC approves Standard 1300 SAR, draft 2 posting (December 1, 2003) 3. SAC appoints Standard 1300 Drafting Team (June 23, 2004) 4. Drafting Team posts draft 1 for comment (September 15, 2004)
5. Drafting Team posts draft 2 of Standard CIP–002–1 (Draft 1, Std 1300, section 1302) (January 17, 2005)

Description of Current Draft:

The current draft reformats Standard 1300, section 1302 into the new NERC Standards format and is to be posted for a 30-day posting period for public review and comment. This draft includes revisions based on public comments received during the posting of Draft 1.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Review comments to draft 2 and revise as needed	February 17, 2005 –March 15, 2005
2. Post Draft 3 for 45-day public comment period	March 15, 2005– April 30, 2005
3. Post Final Draft for 30-day public review, solicit Ballot Body	June 1–30, 2005
4. First ballot of Standard CIP–002–1	July 1–10, 2005
5. Respond to comments, post for recirculation ballot	July 21–31, 2005
6. 30-day posting before board adoption	August 1–31, 2005
7. Board adopts Standard CIP–002–1	September 1, 2005
8. Effective date	October 1, 2005

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data associated with bulk electric system assets.

Critical Asset: 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.

Cyber 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.

Electronic Security Perimeter: 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.

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.

Critical Cyber Assets: Those Cyber Assets essential to the reliable operation of Critical Assets.

Introduction 1. Title: Cyber Security — Critical Cyber Assets 2. Number: CIP–002–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. Business and operational demands for managing and maintaining 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 Responsible Entities identify and protect critical Cyber Assets that support the reliable operation of the bulk electric system. The Critical Assets are identified by the application of a risk-based assessment procedure on the operation of the interconnected bulk electric system. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service provider 4.5.Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. 5. (Proposed) Effective Date: October 1, 2005 Requirements R1.1. Responsible Entities shall identify their Critical Assets using their preferred risk-based assessment. A list	

of Critical Assets is then the basis to identify a list of associated critical Cyber Assets that must be protected by this standard. R1.2. Critical Assets: The Responsible Entity shall identify its Critical Assets. For the purpose of this standard the list of Critical Assets consists of those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a detrimental impact on the reliability or operability of the electric grid and critical operating functions and tasks affecting the interconnected bulk electric system such as, but not limited to: monitoring and control, load and frequency control, emergency actions, contingency analysis, special protection systems, power plant control, substation control and real-time information exchange. Those Critical Assets include the following: R1.3. Control centers and backup control centers performing the functions of a Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generation Owner, Generation Operator and Load Serving Entities. R1.4. Systems, equipment and facilities critical to operating functions and tasks supporting control centers and backup control centers such as telemetering, monitoring and control, automatic generation control, real-time power system modeling and real-time inter-utility data exchange. R1.5. Transmission substations associated with elements monitored as Interconnection Reliability Operating Limits (IROL) R1.6. Generating resources under control of a common system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. R1.7. Generation control centers having control of generating resources that when summed meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. R1.8. Systems, equipment and facilities critical to System Restoration, including Blackstart generators and substations associated with transmission lines used for initial system restoration. R1.9. Systems, equipment and facilities critical to automatic load shedding under control of a common system capable of load shedding 300 MW or greater. R1.10. Special Protection Systems whose misoperation can negatively affect elements associated with an IROL.	

R1.11. Additional Critical Assets: The Responsible Entity shall utilize a risk-based assessment to identify any additional Critical Assets. The risk-based assessment documentation must include a description of the assessment including the determining criteria and evaluation procedure. R1.12. The Responsible Entity shall identify the critical Cyber Assets associated with each Critical Asset listed in section R1. For the purpose of this standard, Critical Cyber Assets will be limited to those Cyber Assets having the following characteristics: R1.13. The Cyber Asset uses a routable protocol, or R1.14. The Cyber Asset is dial-up accessible. R1.15. Dial-up accessible Critical Cyber Assets which do not use a routable protocol require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter R1.16. Any other Cyber Asset within the same Electronic Security Perimeter as identified Critical Cyber Assets must be protected to ensure the security of the Critical Cyber Assets. R1.17. A member of senior management must approve the list of Critical Assets and the list of Critical Cyber Assets. C. Measures M1. The Responsible Entity shall maintain its approved list of Critical Assets as identified in R1. M2. The Responsible Entity shall maintain documentation depicting the risk-based assessment used to identify its Critical Assets in R1. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure. M3. The Responsible Entity shall maintain its approved list of Critical Cyber Assets as identified under Requirement R2 and all other Cyber Assets as identified under Requirement R3. M4. The Responsible Entity shall review, and as necessary, update the documentation referenced in M1, M2, and M3 at least annually, or within 30 calendar days of the addition of, removal of, or modification to any Critical Asset or critical Cyber Asset. M5. A signed and dated record of the senior management officer's approval of the list of Critical Assets must be maintained. M6. A signed and dated record of the senior management officer's approval of the list of Critical Cyber Assets must be maintained.	

D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe Verify annually that necessary updates were made within 30 calendar days of asset additions, deletions or modifications. The performance-reset period shall be one (1) calendar year. The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. 1.3. Data Retention The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.3.1 Documentation of the approved list of Critical Assets, 1.3.2. Documentation depicting the risk-based methodology used to identify its Critical Assets. The document or set of documents shall include a description of the methodology including the determining criteria and evaluation procedure. 1.3.3. Documentation of approved list of Critical Cyber Assets, and 1.3.4 Documentation of the senior management official's approval of both the Critical Asset list and the critical Cyber Asset list. 1.4 Additional Compliance Information: Not Specified Levels of Non-Compliance Level 1: The required documents exist, but have been updated with known changes within thirty (30) calendar days. Level 2: The required documents exist, but have not been approved, updated or reviewed in the last calendar year. Level 3: One or more document(s) missing. Level 4: No Documents exist. E. Regional Differences 1. None Version History	

Introduction 1. Title: Cyber Security Management controls 2. Number: CIP–003–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. 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. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2.balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. 5. (Proposed) Effective Date: October 1, 2005 B. Requirements R1. 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 controls. R2. The Responsible Entity shall document and implement a program for the protection of critical information associated with Critical Cyber Assets R1. The Responsible Entity shall identify all information, regardless of media type, related to the entities Critical Cyber Assets whose compromise could	

impact the reliability and/or availability of the bulk electric system for which the entity is responsible. This includes 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.	The last sentence in "this" R1 should be deleted as it is redundant.
R2. The Responsible Entity shall categorize information related to Critical Cyber Assets to aid personnel with access to this information in determining what information can be disclosed to unauthorized personnel; as well as the relative sensitivity of information that should not be disclosed outside of the entity without proper authorization. R3. Responsible Entities must identify the information access controls related to Critical Cyber Assets based on classification level as defined by the individual entity. R3. The Responsible Entity shall assign a member of senior management with responsibility for leading and managing the entity's implementation and adherence of the cyber security standard. This person, or their designated delegate, must authorize any deviation or exception from the requirements of this standard. Any such deviation or exception and its authorization must be documented.	The words "from the requirements of this standard" should be replaced by "from the requirements of the NERC CIP series of standards".
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 categorized in Requirement R2 of this standard. R4. 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. This governance process must include: R4. 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 prior to the system being promoted to operate in a production environment.	This sentence is redundant and should be deleted: Roles and responsibilities shall also be defined for the access, use, and handling of critical information as identified and categorized in Requirement R2 of this standard.

R5. 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.	"and ultimately ensure the overall integrity of the Critical Cyber Assets." is superfluous.
R5. The Responsible Entity shall institute and document a process for management of access to information associated with Critical Cyber Assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible.	This instance of R5 is redundant and should be deleted as it is stated in R2.
R6. 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.	
R7. 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.	
R8. Responsible Entities shall define and document procedures to ensure that modification, suspension, or termination of user access to Critical Cyber Assets is accomplished in a time frame that ensures Critical Cyber Assets are not put at significant risk. All access revocations/changes must be authorized and documented.	
C. Measures	
M1. The Responsible Entity shall maintain its written cyber security policy stating the entity's commitment to protect Critical Cyber Assets.	
M2. The Responsible Entity shall review the cyber security policy as often as determined by the entity with a minimum review period not to exceed three years.	
M3. The Responsible Entity shall maintain documentation of any deviations or exemptions authorized by the current senior management official responsible for the cyber security program.	
M4. 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.	
M5. The Responsible Entity shall review the information security protection program at least	Remove sections M5 & M6 because they are scope creep and are covered in M7

annually. M6. The Responsible Entity shall perform an assessment of the information security protection program to ensure compliance with the documented processes at least annually. M7. The Responsible Entity shall document the procedures used to secure the information that has been identified as critical cyber information according to the categorization level assigned to that information. M8. The Responsible Entity shall assess the critical cyber information identification and categorization procedures to ensure compliance with the documented processes at least annually. M9. The Responsible Entity shall maintain in its policy the defined roles and responsibilities for the handling of critical cyber information. M10. The current senior management official responsible for the cyber security program shall be identified by name, title, business phone, business address, and date of designation. M11. Changes to the current senior management official must be documented within 30 calendar days of the effective date. M12. The Responsible Entity shall review the roles and responsibilities of Critical Cyber Asset owners, custodians, and users at least annually. M13. 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. M13.1. The Responsible Entity shall have a defined process that maintains a current list of designated personnel responsible for authorizing systems suitable for the production environment. M13.2. 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. M14. The Responsible Entity shall have a defined process that maintains a current list of designated personnel responsible to authorize access to Critical Cyber Assets to reflect any change in status that affects the designated personnel's ability to authorize access to those Critical Cyber Assets.	Suggest "procedures" in M7 and M8 be changed to "controls". M 10 is too prescriptive. Name, Title and Date of Designation are adequate here. Maintaining the other information is too onerous and does not provide any value. M13.1 is a duplicate of M 12 M13.2 – There is not a requirement for Change Management in this standard. This text should be moved to the requirements section. M14 – This statement is redundant - to reflect any change in status that affects the designated personnel's ability to authorize access to those

M15. The list of designated personnel responsible to authorize access to Critical Cyber Assets shall identify each designated person by name, title, business phone, business address, date of designation, and list of systems/applications they are responsible to authorize access for. The list of authorizers shall be reviewed for accuracy at least annually. M16. 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. M17. The Responsible Entity shall ensure that any authorized change in user access to Critical Cyber Assets is documented. Documentation shall be reviewed at least annually to ensure compliance with entities' documented access control processes. M18. The Responsible Entity shall review user access rights to confirm access is still required at least annually. D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.3.1 Written cyber security policy; 1.3.2 The name, title, business address, and business phone number of the current designated senior management official and the date of his or her designation. 1.3.3 Documentation of justification for any deviations or exemptions. 1.3.4 Documented review results of this standard and mitigation strategies for the information security protection program. Review results will be kept for a minimum of 3 years. 1.3.5 The list of approving authorities for access to critical cyber information assets. 1.3.6 The name(s) of the designated approving authority(s) responsible for authorizing systems suitable	Critical Cyber Assets. M15 – same comment as M10 M17 and M18 should be deleted. This measure duplicates measures 4.1 and 4.2 of CIP 004. 1.3.4 – if this is required, it should be moved to a requirements section.

for production. 1.4. Additional Compliance Information: Not specified 2. Levels of Non Compliance 2.1 Level 1: 2.1.1 A current senior management official was not designated for less than 30 calendar days during a calendar year; or 2.1.2 A written cyber security policy exists but has not been reviewed in the last calendar year, or 2.1.3 Deviations from requirements or written cyber security policy are not documented within 30 calendar days of the deviation, or exception, or 2.1.4 An information security protection program exists but has not been reviewed in the last calendar year, or 2.1.5 Processes to protect information associated with Critical Cyber Assets have not been reviewed in the last calendar year. 2.2. Level 2: 2.2.1 A current senior management official was not designated for 30 or more calendar days, but less than 60 calendar days during a calendar year, or 2.2.2 Access to critical cyber information has not been assessed within the last calendar year, or 2.2.3 An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or 2.2.4 The list of designated personnel responsible to authorize access to critical cyber information has not been kept current and has not been reviewed within the last calendar year. 2.3. Level 3: 2.3.1 A current senior management official was not designated for 60 or more calendar days, but less than 90 calendar days during a calendar year, or 2.3.2 Deviations to policy are not documented or authorized by the current senior management official or delegate responsible for the cyber security program, or 2.3.3 Roles and/or responsibilities are not clearly and distinctly defined, or 2.3.4 Controls for the testing and assessment of new or replacement systems and software patches/changes have not been identified or the list of designated approving authorities is not maintained and up to date. .4. Level 4: 2.4.1 A current senior management official was not designated for more than 90 calendar days during a calendar year; or 2.4.2 No cyber security policy exists, or	

2.4.3 No information security program exists, or 2.4.4 Roles and responsibilities have not been defined, or 2.4.5 Executive management has not been engaged in the cyber security program, or 2.4.6 No corporate governance program exists, or 2.4.7 Access authorizations have not been reviewed within the last calendar year, or 2.4.8 There is no authorizing authority to validate systems that are to be promoted to production, or 2.4.9 The list of designated personnel responsible to authorize access to logical or physical Critical Cyber Assets does not exist or, 2.4.10 Access revocations/changes are not authorized and/or documented. E. Regional Differences 1. None Version History	

Personnel & Training

Introduction 1. Title: Cyber Security — Personnel & Training 2. Number: CIP–004–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. Personnel having authorized 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. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 5.(Proposed) Effective Date: October 1, 2005 B. Requirements Responsible Entity shall comply with the following requirements of this standard R1. Awareness — The Responsible Entity shall	

develop, maintain and document its security awareness program to ensure personnel subject to the standard receive on-going reinforcement in sound security practices. R2. Training — The Responsible Entity shall develop and maintain a company specific cyber security-training program that will be reviewed annually. This program will ensure that all personnel having authorized 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. R3. Records — The Responsible Entity shall prepare and maintain records to document training, awareness reinforcement, and background screening of all personnel having authorized access to Critical Cyber Assets and shall be provided for authorized inspection upon request. R4. Personnel Risk Assessment — The Responsible Entity shall subject all personnel having access to Critical Cyber Assets, including contractors and service vendors, to a documented company personnel risk assessment process prior to being granted authorized access to Critical Assets. C. Measures M1. 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: M1.1 Direct communications (e.g., emails, memos, computer based training, etc.); M1.2 Security reminders (e.g., posters, intranet, brochures, etc.); M1.3 Management support (e.g., presentations, all-hands meetings, etc.). M2. Training — The Responsible Entity shall develop and maintain a company-specific cyber security annual training program that includes, at a minimum, the following required items: M2.1 The cyber security policy; M2.2 Physical and elctronic access controls to Critical Cyber Assets; M2.3 The proper release of Critical Cyber Assetn	

formation; M2.4 Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident. M3. Records — The Responsible Entity shall develop and maintain records to adequately document compliance with this standard. M3.1 The Responsible Entity shall maintain documentation of all personnel who have access to Critical Cyber Assets and the date of completion of their training. M3.2 The Responsible Entity shall maintain documentation that it has reviewed and updated its training program annually. M4. Personnel Risk Assessment — The Responsible Entity shall: M4.1 Maintain a list of all authorized personnel with access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets within the security perimeter(s). M4.2 Review the document referred to in measure M4.1 of this standard quarterly, and update the listing within seven calendar days of any substantive change of personnel. M4.3 Physical and electronic access revocation must be completed within 24 hours for any personnel terminated for cause and seven calendar days for any personnel who have a change in status where they are not allowed access to Critical Cyber Assets (e.g., resignation, suspension, transfer, requiring escorted access, etc.). M4.4 The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel prior to being granted authorized 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 identity verification (e.g., Social Security Number verification in the U.S.) 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. M4.5 The Responsible Entity shall ensure that adverse employment actions are consistent with the Responsible Entity's legal and human resources practices for hiring and retention of employees or	M2.4 – this is a new requirement and there is no matching requirement in this standard. M4.1, 4.2, 4.3 are redundant as they are covered in CIP 003.

contractors. M4.6 The Responsible Entity shall conduct update screenings at least every five years or for cause. D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years, and personnel risk assessment documents for the duration of employee employment. Contractor and service vendor records will be maintained for the duration of their engagement. 1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 Document(s) for compliance, training, awareness and screening; 1.4.2 Records of changes to access authorization lists verifying that changes were made within prescribed time frames; 1.4.3 Supporting documentation (e.g., checklists, access request/authorization documents); 1.4.4 Verification that quarterly and annual security awareness have been conducted; 1.4.5 Verification that personnel risk assessments are being conducted 2. Levels on Non-Compliance 2.1.1 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 2.1.2 One instance of personnel termination (employee, contractor or service provider) in which the access control list was not updated within 24 hours for cause or seven calendar days for other personnel changes; or 2.1.3 Personnel risk assessment program exists, but	M4.6 – this should refer to risk assessment as in R4 rather than screenings.

not properly documented, or 2.1.4 Training program exists, but records of training either do not exist or reveal some key personnel were not trained as required; or 2.1.5 Awareness program exists, but not applied consistently or with the minimum of quarterly reinforcement. 2.2. Level 2: 2.2.1 Access control document(s) exist, but have not been updated or reviewed for more than six months but less than 12 months; or 2.2.2 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 seven calendar days or 24 hours if termination for cause; or 2.2.3 Training program exists, but doesn't not cover one of the specific items identified, or 2.2.4 Awareness program does not exist or is not implemented, or 2.2.5 Personnel risk assessment program exists, but is not consistently applied. 2.3. Level 3: 2.3.1 Access control list exists, but does not include service vendors; and contractors or 2.3.2 More than five instances of personnel termination (employee, contractor or service vendor) in which the access control list was not updated within seven business days or 24 hours if termination for cause; or 2.3.3 A personnel risk assessment program does not exist; or 2.3.4 Training documents exist, but do not cover two or more of the specified items. .4. Level 4: 2.4.1 Access control rights list does not exist; or 2.4.2 No training program exists addressing Critical Cyber Assets E. Regional Defences: None Version History:	2.3.1 – Please include a matching requirement or delete this paragraph.

Introduction 1. Title: Cyber Security — Electronic Security 2. Number: CIP–005–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. 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. Applicability When used in within the text of this standard, “Responsible Entity” shall mean 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities.	

Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1 5. (Proposed) Effective Date: October 1, 2005 B. Requirements	
R1. 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 nonCritical Cyber Assets within the defined Electronic Security Perimeter, these non-Critical Cyber Assets must comply with the requirements of this standard.	R1 – delete the first sentence. Repeating the term Electronic Security Perimeters is redundant. The rest of the paragraph is helpful but should not be contained in a requirements statement. Could be moved to the Electronic Security Perimeter definition or to an FAQ.
R2. Disabling unused Network Ports/Services: The Responsible Entity shall enable only those ports/services required for normal and emergency operations of Critical Cyber Assets. All other ports/services, including those used for testing purposes, must be disabled prior to production usage.	
R3. The Responsible Entity shall secure dial-up modem connections. Where remote activation of dial-up connectivity via SCADA activated relays from the security or control center is technically feasible, dial-up equipment at unattended facilities shall be physically deactivated when not in approved use and remotely activated upon approval of activation. In all other cases, the Responsible Entity shall implement procedural or technical measures to ensure authenticity of the accessing device and/or application.	R3 – attended or unattended is irrelevant to security in this paragraph.
R4. Electronic Access Controls — The Responsible Entity shall implement the organizational, technical and procedural controls to permit or deny logical access at all	

electronic access points to the Electronic Security Perimeter(s) and the Critical Cyber Assets within the Electronic Security Perimeter(s). R4.1. These Electronic Security Perimeter access controls shall implement an access control model, which denies access by default unless explicit access permissions are specified. R4.2. 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. These strong procedural or technical measures shall include at least one of the following measures: Two-factor authentication Digital certificates Out-of-band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication One time use passwords In dial-up access, automatic number identification (ANI) to augment static user id and password authentication In dial-up access, call back to augment static user id and password authentication R4.3. Where technically feasible, electronic access control devices shall display an appropriate use banner upon interactive access attempts. R5. 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. R6. Documentation Review and Maintenance - The Responsible Entity shall ensure that all documentation by this standard reflect current configurations and processes. The entity shall conduct a review of these documents at least every 90 calendar days to ensure accuracy and shall update all documents within 30 calendar days following the implementation of changes. C. Measures M1. Electronic Security Perimeter — The Responsible	R4 – The phrase “and the Critical Cyber Assets within the Electronic Security Perimeter(s).” is confusing given that this standard refers to Electronic Security Perimeter. R4.2 – Did y’all mean “remote access” or really “external interactive logical access”? Please clarify. R4.2 – Suggest that indicating “Strong procedural or technical controls” is all that is required. R4.2 – this is too prescriptive for a standard. Would be better as a guideline because technology changes so rapidly. R4.3 – should be removed. This is not a security measure but a legal support measure. R5 – Monitoring authorized access should be replaced with logging authorized access. R6. We could find no requirements for the creation of any documents in the requirements section of this standard.

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 entity shall ensure that all systems hosting Critical Cyber Assets have been identified and are within the Electronic Security Perimeter(s) documented.	M1 establishes a new requirement to document interconnected critical cyber assets within the security perimeter which is not reflected in the requirements.
M2. Disabling unused Network Ports/Services: The Responsible Entity shall disable unused ports and services, and maintain documentation of status/configuration of all ports and services available on Critical Cyber Assets. M3. Dial-up Modems: M3.1 The Responsible Entity shall maintain a documented policy for securing dial-up modem connections to Critical Cyber Assets, and a record of an annual audit of all dial-up modem connections and ports against the policy and documented configuration. M3.2 The documentation shall verify that the Responsible Entity has taken the appropriate actions to secure dial-up access to all Critical Cyber Assets. M4. Electronic Access Controls M4.1 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). M4.2 For each control, the document or set of documents shall identify and describe, at a minimum, M1.4.2 The access request and authorization process implemented for that control, M2.4.2 The authentication methods used, and M3.4.2 A periodic review process for authorization rights, in accordance with management policies and controls defined in Standard CIP–003–1, and ongoing supporting documentation (e.g. access request and authorization documents, review checklists) verifying that these have been implemented. M5. Monitoring Electronic Access Control — The Responsible Entity shall maintain a document or set of documents to identify and describe: M5.1 Organizational, technical and procedural controls, including tools and procedures, for monitoring electronic (logical) access.	M2, M3.1 and M3.2 establish new requirements which are not covered in the requirements section.
M5.2 Supporting documents, including access records and logs, to verify that the tools and procedures are	M5.2 – this appears to be the same as CIP 007, R 7/M6.

functioning and being used as designed. M5.3 Processes, procedures and technical controls implemented to review 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. Documents that record these reviews shall be identified. M6. Documentation Review and Maintenance: — The Responsible Entity shall review the documents referenced in this standard at least annually and shall update these documents within 30 calendar days of the modification of the network or controls. D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep document revisions and security incident related data (such as unauthorized access reports) for three (3) 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 calendar days. The compliance monitor shall keep audit records for three years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years, and personnel risk assessment documents for the duration of employee employment. Contractor and service vendor records will be maintained for the duration of their engagement. 1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 Document(s) for configuration, processes, tools and procedures as described in this standard; 1.4.2 Records of electronic access to Critical Cyber Assets (e.g. access logs, intrusion detection logs) 1.4.3 Supporting documentation (e.g. checklists, access request/authorization documents) 1.4.4 Verification that necessary updates were made at least annually or within 90 calendar days of a modification 2. Levels of Non-Compliance 2.1 Level 1:	M6 contradicts R6 of this standard. 1.2 there is an inconsistency with CIP 007 R 7.1. 1.4.4 – Not consistent with requirements or measures.

2.1.1 Document(s) exist, but have not been updated with known changes within the 90calendar day period and/or, 2.1.2 Access to any Critical Cyber Asset was unmonitored for a period that does not exceed 24 hours. 2.2. Level 2: 2.2.1 Document(s) exist, but have not been updated or reviewed in the last 12 months and/or, 2.2.2 Monitoring is in place, but a gap in the access records exists for one calendar day or more but for less than seven calendar days. 2.3. Level 3: 2.3.1 Electronic Security Perimeter: Document exists, but no verification that all critical assets are within the perimeter(s) described or, 2.3.2 Disabling Unused Network Ports/Services: Documents(s) exist, but a record of regular audits does not exist. 2.3.3 Electronic Access Controls: 2.3.3.1 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 2.3.3.2 Required documents exist, but records for some transactions are missing. 2.3.4 Electronic Access Monitoring: 2.3.4.1 Access not monitored to any Critical Cyber Asset for one week or more; or 2.3.4.2 Access records reveal access by personnel not approved on the access control list. 2.4. Level 4: 2.4.1 No document or no monitoring of access exists E. Regional Differences 1: None Version History	2.1.2 – This is not a realistic requirement as it deals mainly with the reliability/availability of systems. A better measure would be to verify that the monitoring processes are in place or the failure of a monitoring process was corrected within 24 hours. 2.3.2 – The word audit is a new requirement and has specific connotations. The word regular is un-measurable. A better expression would “record of [time period] validations or assessments”. 2.3.3 – Delete this section because it is not measurable.

A. Introduction

1. Title: Cyber Security — Physical Security 2. Number: CIP–006–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. 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) (nearest six-wall boundary) within which these Cyber Assets reside.	Delete (nearest six-wall boundary) as this is already covered in the definition above or move it to the definition.
4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 5. (Proposed) Effective Date: October 1, 2005 Requirements R1. Security Plan: The Responsible Entity shall document its implementation of the following requirements in its physical security plan. R1.1. The identification of the Physical Security Perimeters(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). R1.2. The implementation of the necessary measures to control access at all access points of these perimeter(s) and the Critical Assets within them. R1.3. Implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the Critical Cyber Assets. R2. 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) following an industry or government, generally accepted, risk assessment procedure. R3. 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. R4. Logging physical access: The Responsible Entity shall implement the technical and procedural mechanisms for logging physical access. R5. Maintenance and testing: The Responsible Entity shall implement a 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.	
R6. Documents for configuration, processes, tools, and procedures: The Responsible Entity shall maintain the specified documentation concerning its implementation of its Physical Security Plan. C. Measures	R6 – Duplicates R1.
M1. Documentation Review and Maintenance: The Responsible Entity shall review and update its physical security plan at least annually or within 90 days of modification to the perimeter or physical security methods.	M1 – 90 days is not found in the requirements section.
M2. 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).	
M3. Physical Access Controls: The Responsible Entity shall implement one or more of the following	M3 – this is too prescriptive and does not respect changing technologies. The words “or

physical access methods: Card Key: A means of electronic access where the access rights of the cardholder 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 Enclosure: A cage/safe/cabinet system that controls physical access to the Critical Cyber Asset (for environments where the nearest six-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 all physical access point through the Physical Security Perimeter. The documentation shall identify and describe, at a minimum, the access request, authorization, and revocation process implemented for that control, and a periodic review process for verifying authorization rights, in accordance with management policies and controls defined in Standard CIP–003–1, and on-going supporting documentation. M4. 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 or point of facility access.	equivalent" would make this section better. The term "Security Officers" is confusing and should be changed to "Security Personnel". M4. This is redundant. These requirements are referred to in R1 and M1.

Alarm Systems	A system that indicates a door or gate has been opened without authorization. These alarms must report back to a central monitoring station. Examples include card key alarm systems, 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 describe processes to review records for unauthorized access. The Responsible Entity shall have a process for creating unauthorized access reports.

M5. 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 or remote verification
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.

M6. Maintenance and testing of physical security systems: 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.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep document revisions and other security event-related data including unauthorized access reports for three calendar years. The Responsible Entity shall keep audit records for 90 days. The compliance monitor shall keep audit records for three years. The performance-reset period shall be one (1) calendar year.	
1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years.	1.3 If the documents referred to are video records, then this is excessive, unless the documents relate to a significant security incident.
1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 The Physical Security Plan 1.4.2 Document(s) for configuration, processes, tools, and procedures as described in this standard. 1.4.3 Records of physical access to Critical Cyber Assets (e.g., manual access logs, automated access logs). 1.4.4 Supporting documentation (e.g., checklists, access request/authorization documents) 1.4.5 Verification that necessary updates were made at least annually or within 90 days of a modification.	
2. Levels of Non-Compliance 2.1. Level 1: 2.1.1 Document(s) exist, but have not been updated or reviewed within the last 90 days and/or 2.1.2 Access control, monitoring and logging exists, but aggregate interruptions in system availability over a calendar year exist for more than seven days, but less than 1 month.	2.1.1 Not consistent with M1.
2.2. Level 2: 2.2.1 Document(s) exist, but have not been updated or reviewed in the last 6 months and/or 2.2.2 Access control, monitoring and logging exists, but aggregate interruptions in system availability over a calendar year exist for more than one month, but less than three months.	2.2.1 Requires more stringent compliance than level 1 compliance.
2.3. Level 3: 2.3.1 Document(s) exist, but have not been updated or reviewed in the last 12 months and/or 2.3.2 Access control, monitoring and logging exists, but aggregate interruptions in system availability	

over a calendar year exist for more than three months. 2.4. Level 4: 2.4.1 No access control, or no monitoring, or no logging of access exists. E. Regional Differences 1. None Version History	

1. Title: Cyber Security — Systems Security Management 2. Number: CIP–007–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. A System Security Management Program is necessary to minimize or prevent the risk of failure or compromise from misuse or malicious cyber activity. 4. Applicability When used within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. While there are significant differences between attended and unattended facilities that contain Critical Cyber Assets, the requirements below will apply to both unless specifically differentiated. R1. Test Procedures — Attended Facilities: The Responsible Entity shall use documented information security test procedures to augment functional test and acceptance procedures for all new systems and significant changes to existing	This standard is a prime example of the need for a technical writer's review of the standards. It is much more prescriptive than the rest and demonstrates the lack of homogeneity across the standards. R1 – Delete. This requirement is well covered in CIP 003, R4 and R5

critical cyber security assets. The Responsible Entity shall ensure that significant changes include but are not limited to security patches, cumulative service packs, new releases, 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 non-production environment. All testing shall be performed in a manner that precludes adversely affecting the production system and operation. The Responsible Entity shall document full detail of the test environment. The Responsible Entity shall verify that all changes to Critical Cyber Assets were successfully tested for known security vulnerabilities prior to being rolled into production, on a controlled non-production system.	
R2. Test Procedures – Unattended Facilities: The Responsible Entity shall not store test documentation, security procedures, and acceptance procedures at an unattended facility but at another secured attended facility. The Responsible Entity shall conduct security test procedures for Critical Cyber Assets at the unattended facility on a controlled non-production environment located at another secure attended facility.	R2 – Delete. This requirement is well covered in CIP 003, R4 and R5
R3. Account and Password Management: The Responsible Entity shall 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 shall establish, implement, and document end user account (administrator, system, and individual) management that include but are not limited to: R3.1. Strong Passwords: In the absence of more sophisticated authentication methods that are stronger than passwords and don't require a password, (e.g., multi-factor access controls, certificates, or bio-metric), the Responsible Entity shall use accounts that have a strong password. For example, a password consisting of a combination of	R3 – use "account management" instead of "establish an account password management program" R3 – "by compromised account passwords" should be struck as unnecessary. R3 – "that include but are not limited to:" should say "that must meet at a minimum:

alpha, numeric, and special characters with a minimum of six characters to the extent allowed by the existing technology. Passwords shall be changed periodically per a risk-based frequency to reduce the risk of password cracking. R3.2. Generic Account Management – Attended: The Responsible Entity shall have a process for managing factory default accounts, e.g., administrator or guest. The process shall include the removal, disabling, or renaming of these accounts where possible. For those accounts that must remain, passwords shall be changed prior to putting any system into service. Where technically supported, individual accounts shall be used (in contrast to a group account). Where individual accounts are not supported, the Responsible Entity shall 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 (automated or manual), and steps for securing the account in the event of staff changes, e.g., change in assignment or exit. R3.3. Generic Account Management – Unattended: For unattended facilities, the Responsible Entity shall ensure the physical access to Cyber Assets by approved users is authorized by a control or security center operator on an instance-by-instance basis. R3.4. Access Reviews – Attended: The Responsible Entity shall ensure a designated approver reviews access to Critical Cyber Assets, e.g., computer and/or network accounts and access R3.5. Access Reviews — Unattended: The Responsible Entity shall maintain and periodically review records of approved physical access and the cyber related work performed on Cyber Assets at unattended facilities. R3.6. Acceptable Use: The Responsible Entity shall have a policy implemented to manage the scope R3.5. Access Reviews — Unattended: The Responsible Entity shall maintain and periodically review records of approved physical access and the cyber related work performed on Cyber Assets at unattended facilities. R3.6. Acceptable Use: The Responsible Entity shall	R3.3 is covered in CIP 006 R3.4 and R3.5 is covered by CIP 003, 005 and 006.

have a policy implemented to manage the scope and acceptable use of the administrator and other generic account privileges for both attended and unattended facilities. The policy shall support a compliance 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.	
R4. Security Patch Management: The Responsible Entity shall establish a formal security patch management program for tracking, evaluating, testing, and installation of applicable security patches and upgrades to critical cyber security assets.	R 4 – "critical cyber security assets." Security should be deleted.
R4.1. The Responsible Entity shall evaluate all patches and upgrades for applicability to the individual situation, e.g. using a risk based assessment, so as to avoid un-necessary and excessive patching.	R4.1 – Should read "all relevant patches"
R4.2. The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.	R4.2 & R4.3 – this requirement is too prescriptive. A better requirement would be for the company to have a patch management policy and procedure based on its own environment.
R4.3. In the case where installation of the patch is not possible, the Responsible Entity shall use and document a compensating measure(s).	
R5. Integrity Software	
R5.1. The Responsible Entity shall use Integrity Software on all Critical Cyber Assets that are connected to a wide-area network, the Internet, or to another device that is connected to a network (e.g., printer), to prevent, limit, and/or mitigate the introduction, exposure and distribution of malicious software (malware) to other Cyber Assets within the Electronic Security Perimeter.	R5.1 – This section is unclear and would be better if written as follows: "The Responsible Entity shall use means to monitor and protect the integrity of data including software associated with critical cyber assets e.g.: technology, processes/procedures, software." to prevent, limit, and/or mitigate the introduction, exposure and distribution of malicious software (malware) to other Cyber Assets within the Electronic Security Perimeter.
R5.2. The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the Integrity Software implementation and upgrades.	R5.2 - Suggest it be deleted. Covered elsewhere.

R5.3. In the case where integrity software is not used, e.g., operational incompatibility or not available for a particular computer platform, the Responsible Entity shall use and document a compensating measure(s). R5.4. Where repetitious application of software updates are necessary, such as at unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of mal-ware. R6. Identification of Vulnerabilities and Responses R6.1. The Responsible Entity shall perform a vulnerability assessment at least annually that includes: R6.1.1. A diagnostic review of the access points to the Electronic Security Perimeter R6.1.2. Scanning for open ports/services and modems R6.1.3. Factory default accounts R6.1.4. Security patch and anti-virus version levels R6.2. The Responsible Entity shall implement a documented management action plan to remediate vulnerabilities and shortcomings, if any, identified in the assessment. R6.3. For unattended facilities that contain Critical Cyber Assets, the Responsible Entity shall perform a limited vulnerability assessment prior to each upgrade as possible given the technical capability of the Cyber Assets. R7. Retention of Systems Logs: Using monitoring systems and/or procedures either internal and/or external to Critical Cyber Assets, the Responsible Entity shall ensure it is possible to create an audit trail from logs of security-related events affecting the Critical Cyber Assets. The Responsible Entity must determine its own logging strategy to fulfill the requirement. R7.1. The Responsible Entity shall retain said log data for a period of ninety (90) calendar 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) calendar years in an exportable format, for possible use in further event analysis. R7.2. In lieu of automatically generated logs at unattended facilities, the Responsible Entity shall	R5.4 – Where remote installation of software updates is required, the responsible entity shall ensure the integrity of the software being installed prior to initiating remote installation in order to prevent annual dissemination of malware. R7 – The last sentence gives the entities the responsibility to determine their own logging strategy but R7.1 and R7.2 are contrary and prescriptive and should be deleted.

collect and retain the physical access and change records of users at each approved access session, or at a minimum annually. R8. Change Control and Configuration Management R8.1. 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 shall include change management procedures that at a minimum provide testing, modification audit trails, problem identification, a back out and recovery process shall modifications fail, and ultimately ensure the overall integrity of the Critical Cyber Assets. R8.2. The Responsible Entity shall ensure the controlled development or test environment for Cyber Assets residing in unattended facilities are not at the unattended facility. The Change Control Process for Cyber Assets at unattended facilities shall prevent the inadvertent dissemination of faulty or compromised software to multiple unattended sites.	R8 – Should be deleted as it is well covered in CIP 003.
R9. Disabling Unused Host Ports/Services: The Responsible Entity shall enable only those ports/services required for normal and emergency operations of Critical Cyber Assets. All other ports/services, including those used for testing purposes, must be disabled prior to production usage. R10. Operating Status Monitoring Tools: For maintaining situational awareness, the Responsible Entity shall ensure Critical Cyber Assets used for operating critical infrastructure are included or augmented with automated and/or process tools, where practical, to monitor operating state, utilization and performance, and cyber security events experienced by the Critical Cyber Assets themselves, and issue alarms for specified indications, as implemented. For Critical Cyber Assets in use at unattended facilities that are not capable of being electronically monitored remotely, the Responsible Entity shall review and document pertinent metrics manually during routine access/service to said equipment	R9 – Should be deleted as it is well covered in CIP 005.
R11. Back up and Recovery: The Responsible	R11 – The last sentence “For unattended

Entity shall back up on a regular basis, where technically feasible, information and data that is resident or required by Cyber Assets used to manage critical electric infrastructure. The back up must be stored in a remote or hardened site some distance away from the Critical Cyber Assets. Information stored on computer media for a prolonged period of time shall be tested at least annually to ensure that the information is recoverable. For unattended facilities, back-up and recovery materials can be effectively tested at central test facility and shall not be tested on site. C. Measures M1. Test Procedures: For all Critical Cyber Assets, the Responsible Entity shall maintain records of test procedures, results, and acceptance of successful completion.	facilities, back-up and recovery materials can be effectively tested at central test facility and shall not be tested on site." should be removed and the rest of this section moved to CIP 009.
M2. Account and Password Management: The Responsible Entity shall maintain a documented password policy and record of semi-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. Review access permissions within 24 hours for any personnel terminated for cause and seven calendar days for any personnel who have a change in status where they are not allowed access to Critical Cyber Assets (e.g., resignation, suspension, transfer, requiring escorted access, etc.).	M2. – Remove "record of semi-annual audit of this policy" as is contrary to R3.1
M3. 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, approval for installation, compensating measures, and installation date. M4. Integrity Software: The Responsible Entity's change control documentation shall include a record of all integrity software installations including: M4.1 Version level actively in use M4.2 Installation date M4.3 Or provide documentation for other compensating measures taken M5. Identification of Vulnerabilities and Responses: M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical and procedural controls, including tools	M3 - The reference to change control is dealt with in CIP 003

and procedures for monitoring the critical cyber environment for vulnerabilities. M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found. M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities. M6. Retention of Logs: M6.1 The Responsible Entity shall maintain documentation that indexes location, content, and retention schedule of all log data captured from the Critical Cyber Assets. M6.2 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. M7. Change Control and Configuration Management M7.1 The Responsible Entity shall maintain documentation identifying the controls, including tools and procedures, for managing change to and testing of Critical Cyber Assets. M7.2 The documentation shall verify that all the Responsible Entity follows a methodical approach for managing change to their Critical Cyber Assets. M8. Disabling Unused Host Ports/Services: The Responsible Entity shall disable unused ports and services, and maintain documentation of status/configuration of all ports and services available on Critical Cyber Assets. M9. Operating Status Monitoring Tools: The Responsible Entity shall maintain documentation identifying organizational, technical, and procedural controls, including tools and procedures for monitoring operating state, utilization, and performance of Critical Cyber Assets. M10. Back-up and Recovery: M10.1 The Responsible Entity shall maintain documentation that index location, content, and retention schedule of all Critical Cyber Assets' information backup data and tapes. M10.2 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.	Please align measurements and to requirements. M10.1. Replace backup data and tapes with backup media.

M10.3 The documentation shall verify that the Responsible Entity is capable of recovering from the failure or compromise of Critical Cyber Asset. D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years. 1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 Document(s) for configuration, processes, tools and procedures as described in this standard. 1.4.2 System log files as described in measure M6. 1.4.3 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.). 2. Levels of Non-Compliance 2.1. Level 1: Document(s) exist, but does not cover up to two of the specific items identified and/or the document has not been reviewed or updated in the last 12 months. 2.2. Level 2: Document(s) exist, but does not have three of the specific items identified and/or 2.2.1 A gap in the reviews for the following items exists: 2.2.1.1 Access Reviews (semi-annually for attended facilities, periodically for unattended facilities). 2.2.1.2 Security Patch Management (monthly) 2.2.1.3 Integrity Software (monthly) 2.2.2 Retention of system logs exists, but a gap of greater than three days but less than seven days exists. 2.3. Level 3: 2.3.1 Document(s) exist, but more than three of the	

items specified are not covered. 2.3.2 Test Procedures: Document(s) exist, but documentation verifying that changes to Critical Cyber Assets tested is incomplete or changes to Critical Cyber Assets were not tested. 2.3.3 Account and Password Management: Document(s) exist, but documentation verifying accounts and passwords comply with the policy does not exist. 2.3.4 Security Patch Management: Document exists, but records of security patch installations are incomplete. 2.3.5 Integrity Software: Documentation exists, but verification that all Critical Cyber Assets are being kept up to date on anti-virus software or that compensating measures are being taken does not exist. 2.3.6 Identification of Vulnerabilities and Responses: 2.3.6.1 Document exists, but annual vulnerability assessment was not completed and/or 2.3.6.2 Documentation verifying that the entity is taking appropriate actions to remediate potential vulnerabilities does not exist. 2.3.7 Retention of Logs (operator, application, intrusion detection): A gap in the logs of greater than 7 days exists. 2.3.8 Disabling Unused Host Ports/Services: Documents(s) exist, but a record of regular audits does not exist. 2.3.9 Change Control and Configuration Management: N/A 2.3.10 Operating Status Monitoring Tools: N/A 2.3.11 Backup and Recovery: Document exists, but record of annual restoration verification exercise does not exist. 2.4. Level 4: No Documentation exists E. Regional Differences 1. None Version History	

1. Title: Cyber Security — Incident Response Planning 2. Number: CIP–008–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. Security measures designed to protect Critical Cyber Assets from intrusion, disruption or other forms of compromise must be monitored on a continuous basis. This standard requires responsible entities to define the procedures that must be followed when Cyber Security Incidents are identified. This standard requires: Developing and maintaining of documented procedures, Classification of incidents, Actions to be taken, and Reporting of Incident. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard.	The references to "incidents" should say cyber security incidents.

(Proposed Effective Date: October 1, 2005 . Requirements R1. The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate and/or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items: R2. Incident Classification: The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents. R3. Cyber Security 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. R4. Cyber Security Incident Reporting: The Responsible Entity shall report all Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center ES ISAC in accordance with the Indications, Analysis & Warning Program (IAW) Standard Operating Procedure (SOP). The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. C. Measures M1. The Responsible Entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and Cyber Security Incident reporting requirements at least annually or within 90 calendar days of known changes M2. The Responsible Entity shall retain records in addition to requirements defined in Standard CIP-007-1, requirement R7 (Retention of Systems Logs) of Cyber Security Incidents for three calendar years. D. Compliance 1. Compliance Monitoring Process	

1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years. 1.4. Additional Compliance Information 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: 1.4.1 System and application log file entrie 1.4.2 Video, and/or physical access records, 1.4.3 Documented records of investigations and analysis performed, 1.4.4 Records of any action taken including any recovery actions initiated. 1.4.5 Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC. 2. Levels of Non-Compliance 2.1.Level 1 2.1.1 Documentation exists, but has not been updated with known changes within 90 calendar days. 2.2. Level 2: 2.2.1 Incident response documentation exists, but has not been updated or reviewed in the last 12 months and/or 2.2.2 Records related to Cyber Security Incidents are not maintained for three years or are incomplete. 2.3. Level 3: 2.3.1 Incident response documentation exists but is incomplete and/or 2.3.2 Cyber Security Incidents have occurred but were not reported to the ES ISAC 2.4. Level 4: No documentation exists. E. Regional Differences 1. None Version History	

1. Title:Cyber Security — Recovery Plans 2. Number: CIP–009–1 Purpose: This standard is intended to ensure that appropriate cyber 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. 3. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 3.1. Reliability Coordinator 3.2. Balancing Authority 3.3. Interchange Authority 3.4.Transmission Service Provider 3.5.Transmission Owner 3.6. Transmission Operator 3.7. Generator Owner 3.8. Generator Operator 3.9. Load Serving Entity 3.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP-002-1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. (Proposed) Effective Date: October 1, 2005 Requirements	
R1. The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan(s) at least annually. R2. The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan. R3. The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that effects the protection of Critical Cyber Assets R4. Recovery plan(s) and any updates or changes shall be communicated to personnel responsible for their operation or responsibility for such Critical Cyber Asset within seven (7) calendar	R1. Overly prescriptive. The minimum test frequency schedule should be based on a risk-based assessment and evidence kept that this testing frequency is respected.

days of development or modification. R5. The Responsible Entity shall develop training and awareness for its recovery plan(s) that follow the requirements set forth in Standard CIP–004–1 — Personnel and Training.	
C. Measures M1. The Responsible Entity shall document its Recovery Plan(s) and maintain records of all exercises or drills for at least three (3) years. M2. The Responsible Entity shall document its Recovery Plan(s) and maintain records of all exercises or drills for at least three (3) years.	M1 and M2 should be merged.
M3. The Responsible Entity shall review and update if needed, its response to events of varying duration and severity annually or as necessary.	M3 and M4 are repetitive and should be merged.
M4. The Responsible Entity shall review and update recovery plan(s) annually.	M4 contradicts R3.
M5. The Responsible Entity shall conduct drills at least every three (3) years and keep attendance records to its Recovery Plan(s) training	M5 is not consistent with R1 and needs to be clarified.
D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall make the documents described in this standard available for inspection by the compliance monitor upon request. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years. 1.4 Additional Compliance Information: Not Specified	
2. Levels of Non-Compliance 2.1 Level 1: Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year. 2.2 Level 2: Recovery plan(s) have not been reviewed, exercised, or training performed. 2.3 Level 3: Recovery plan(s) address neither the type of events that are necessary nor	2. This compliance section will not work and should be revisited. For example, a plan that has not been reviewed will contradict both level 1 and level 2. Entity which neither updates its recovery plan in the past year, nor exercised nor included in it the types of “events that are necessary” could legitimately claim any of level 1, 2 or 3

any specific roles and responsibilities. 2.4. Level 4L No recovery plan(s) exists. E. Regional Differences: None	noncompliance. Level 3 identifies a new requirement that should be identified in the requirements or measures section.

General comments

The standard still looks inconsistent in a number of areas:

a) Some of the measures and requirements language seems to be similar both in the same section of the standards and across the standards.
b) The numbering is still inconsistent.
c) 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.

The time periods prescribed throughout are still inconsistent across the CIP 002 to 009 standards.

If an entity is found not to have properly identified its critical infrastructure in 002, will this mean being scored as non-compliant in the other remaining standards?

The standard 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 exists 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.

Most references to unattended facilities do not seem to bear relevance on security measures to critical cyber assets and should be reviewed.

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 the 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**
ERCOT ECAR FRCC MAAC MAIN MAPP NPCC SERC SPP WECC NA - Not Applicable	xx	1 - Transmission Owners
		2 - RTOs, ISOs, Regional Reliability Councils
	xx	3 - Load-serving Entities
		4 - Transmission-dependent Utilities
	xx	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: **Pacific Gas and Electric Company**

Lead Contact: Lyman Shaffer

Contact Organization:

Contact Segment:

Contact Telephone: 415 973-6920

Contact Email: lhs1@pge.com

Additional Member Name	Additional Member Organization	Region*	Segment*
Bob Mathews	PG&E System Operations		
Simon Chiang	Substation Engineering		
David Hayr	Information Protection		

* 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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

1. Cyber Assets – In this definition you refer to "communication network". For the purpose of this standard, communications links connecting discrete electronic perimeters are not considered. – this should be stated clearly

2. Throughout the standard you refer to the term "authorized access", so shouldn't it be included in the definitions section? Suggested definition would be: "is Access that is granted according to an established scheme of governance."

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

Introduction/Purpose:

In the second paragraph of the introduction it reads ", where loss or compromise of these assets…" it should read ", where loss of availability or compromise of the integrity of these assets…".

Requirements:

R1.1unclear whether the intent of this is to be proscriptive or just listing examples"

R1.1.2 appears that critical cyber assets are listed as critical assets themselves – suggest striking the text 'such as …..inter-utility data exchange'

R1.1.1 – change "performing" to "with" to read: "…backup control centers with the functions of…".

R1.1.3 – This requirement should state that it excludes anything not in the direct transfer path associated with the IROL.

R1.1.7 – Shouldn't the load shedding requirements refer to the reporting requirements imposed operating standards versus the prescriptive 300 MW. Tie it to reporting criteria.

R2 – We are looking for more clarification regarding this requirement due to mixed messages from the working, the NERC 1300 Web cast, and discussions with drafting team members. If a control center and a plant have routable protocols within each of their electronic perimeters, but have no routable protocols through their electronic perimeter are both or either subject to the electronic requirements of this standard? Understanding that both are subject to the physical security requirements of this standard.

R4. – Due to the update frequency of a detailed list, this requirement should be wording in a manner that will only require senior management to sign off on functions/systems and not the detailed components of these functions/systems. The detailed list is required to be keep up to date by an operational unit.

Measures:

M5 & M6 – These measures refers to "Officers" and is not consistent with all other references to "Senior Management". These measures should also include time frames like all the other measurements (e.g. M4). Suggest a measurement of an annual review.

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.

Measures:

M5 & M10 – M5 uses the term "information security protection program" and M10 users the term "cyber security program", was this intended? If so, why? If not, this needs to be fixed.

Compliance:

2.1.1 – "for less" should be changed to "for more than"

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.

Measures:

M4.6 – Instead of reading, "The Responsible Entity shall conduct update screenings at least every five years or for cause", should read, "The Responsible Entity shall conduct personnel updates as per their documented company personnel risk assessment process at least every fives years or for cause."

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

Requirements:

R2- The requirement is very prescriptive. We're required to disable unused network ports. However, we should be allowed to use a different type of access control to ensure that unauthorized devices don't gain access to the network. We suggest the following working: Restricting access to the network: The Responsible entity shall restrict access to network ports to only those devices and individuals that are authorized to connect. This shall be accomplished through either a network authentication system such as 802.1xor by disabling unused ports on the network switches.

R3 – "Unattended" doesn't apply, you should comply with this requirement regardless if the facility is attended or unattended. (We find this control to be overly prescriptive by suggesting that the only method to secure modems is by enabling/disabling them via SCADA. There are other methods available and appears to be in conflict with R4.2 which suggests that dial-back is an acceptable method to secure modems.

R4.2 – The word "logical" is not needed.

R4, R4.2, & R5 – The reference to "organizational, technical, and procedural controls" are not consistently used in R4 and R5 sections.

R4.2 – Digital certificates is a form of Two-factor authentication. Should be removed as it's own bullet and be used as an example for Two-factor authentication.

R4.2 – In the sentence "These strong procedural or technical measures shall include at least one of the following measures", "measures" should be replaced with "methods".

R4.2.2 – we are not comfortable with the proposed use of ANI as an authentication source for modems. Dial-up accessible critical cyber assets that do not support a network connection, such as substation IED's that expose only binary or ASCII serial interfaces, shall be secured using at least one of the measures listed in R4.2, or, alternatively, using at least one of the following (or similar) measures:
- Physical activation and deactivation of the modem through SCADA, controlled by a control center or security center operator, logged, and subjected to appropriate authentication of the requesting party.
- Installation of link encryptors that, together with an IED password, provide effective two-factor authentication.
- Assignment (and periodic reassignment) of strong, unique passwords to all dial-up accessible IED's, and installation of a centralized, secure dial-out server that effectively preserves the secrecy of these passwords.

R5 – Best practices is not to necessarily perform real-time monitoring of authorized access, but rather create logs to track authorized access in a manner that creates an audit trail. We agree that you should "monitor" unauthorized access attempts. So, this requirement should be worked in a way that allows for best practices without creating unnecessary administration overhead that doesn't reduce any risk.

Measures:

M1 – Remove the reference to "all interconnected Critical Cyber Assets within the security perimeter". We agree with maintaining documents depicting the Electronic Security Perimeter(s) and all electronic access points, however, documents depicting interconnectivity within the security perimeter changes often and is captured in design and maintenance documents.

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.

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.

Introduction/Purpose:

The sentence that reads, "A System Security Management Program is necessary to minimize or prevent the risk of failure or compromise from misuse or malicious cyber activity" should read "A System Security Management Program is necessary to ensure system availability and integrity by minimizing or preventing malicious and non-malicious activity and misuse, whether authorized or unauthorized. This includes measures necessary to detect, document, and counter such threats."

Requirements:

R1 – In some cases production systems are taken off-line and removed from production mode and used for testing. We feel that this needs to be permitted and clarified within this requirement.

R2 – The second sentence in this requirement is not clear. It needs to either be clearly reworded or removed.

R3 – Instead of requiring the entity to "…establish an account password management program" it should require the entity to "perform account management".

- End the first sentence at "unauthorized system access." striking "by compromised account passwords.

- Replace "not limited to" with "must meet" or "at a minimum"

R3.1 – Replace "shall use accounts that have a strong password" with "shall use strong passwords".

R4.2 – Remove the first sentence in this requirement.

R5.1 – In this requirement it isn't clear where it must be applied. If it is intended for all CCAs, regardless if at the perimeter or internal to the perimeter, it should clearly state that.

R6.1.2 This section requires scanning for open ports/services, and modems. Vulnerability scanning on critical production process control systems is not recommended as it can crash systems We recommend that such scanning be done for off line duplicate systems.

R6.1.4 – a company may elect not to install a patch or antivirus system due to concerns about potential impact on operating systems.

R6.3 – "Unattended" doesn't apply, you should comply with this requirement regardless if the facility is attended or unattended.

R10 this is not possible on all critical cyber assets. While we can monitor performance and security events on servers and workstations, some devices may not have the ability to install software or otherwise monitor performance or security events.
R11 – The last sentence in this requirement doesn't make sense. Why can you not effectively test on-site at unattended facilities? Recommended removing this sentence.

Measures:

M2 – Fix typo. "n" should read "in". A semi annual audit of all this policy against all accounts is password is too proscriptive and onerous (especially if large # of substation devices are included). Suggest striking this measure.

M10.1 – Replace "backup data and tapes" with "backup media".

M10.3 Suggest striking or rewording this measure as it is unrealistic that there would be a verifiable plan to recover from every possible type of failure or compromise for each critical cyber or compromise. Also this seems to be an overlap with CIP 009

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

Concern is that "any suspicious event" includes most firewall

interceptions (and there may be hundreds/day) and that we have 60

minutes to report them [day or night] or be assessed a level-3

non-compliance penalty

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.

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.

All items are required to be substantially compliant by 1st quarter 2006 for TO. Given the fact that the emergency action cyber standard did not apply to a significant portion of the industry and the permanent standard will not be in effect until well into 2005, this is unreasonable particularly as it will apply to a large number of facilities, employees and procedures. The time frame for substations and other facilities other than control centers will clearly be insufficient (

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

General Comments:

1. Should clearly correlate “Requirements” to “Measures” and “Measures” to “Compliance”. This way there is a clear relationship all the way from requirements to compliance. Currently it is hard to correlate this and it appears that in several cases they don’t correspond with each other.
2. The term “shall” is used in both the “Requirements” and “Measures” sections. The term “shall” should only be used in the “Requirements” section and the “Measures” section shouldn’t use “shall” but rather performance language.
3. This standard should be broken up into two distinct standards. One with specific requirements for centralized Control Systems and one with specific requirements for plants and sub-stations. This standard seems to be more focused on Control Systems where the requirements seem to fit very well, however, due to the technology, etc. at plants and sub-stations, these requirements don’t fit as well. Also, there is a different risk model for Control Systems versus plants and sub-stations. Due to the risk difference there are should be distinct requirements for each.
4. Technical feasibility – along the lines of the comments above in 3, if this standard isn’t separated between Control Centers, plants, and sub-stations it should take into consideration the technical feasibility of the requirements and annotate it so that the “exception to standard” overhead doesn’t get out of hand. We don’t want to make this counter productive by creating a massive about of paperwork administration not allowing us to focus on the spirit of the standard.

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:	Steven L Townsend	
Organization:	Consumers Energy	
Telephone:	(517) 788-2069	
Email:	sltownsend@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.

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.

Consumers Energy has also submitted comments via the ECAR CIPP.

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.

It was mentioned in the February 2nd webcast that a guideline for Risk Based Assessment would be posted to the NERC website, when will this be available?

Are the assets listed in R1.1.1 through R1.1.8 the inclusive list that are mandatory critical assets and risk assessments will need to be done on all other assets? Or is this the mandatory list that a risk assessment must be done on to determine if this is a critical asset? If an asset is not included in this list, is it excluded from the standard?

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.

The standard needs to recognize the difference between securing a control center and securing a substation – a substation does not have the same impact that a control center will have if it is compromised.

Why is Blackstart (R1.1.6) part of the critical assets? During a Blackstart situation, cyber assets would not be used.

If multiple options exist for Blackstart, does this remove the assets from the Critical Assets list?

Does section R1.1.7 mean a substation that is capable of dropping 300 MW or a system that controls several substations that the total of the load dropped is greater than 300 MW?

If you only have dial-up access (R2.3), do the remaining standards apply?

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 clarify sections R2.2 and R2.3, they are somewhat confusing.

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.

Consumers Energy has also submitted comments via the ECAR CIPP.

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.

There is still redundancy in the standards, i.e. – unused ports/services appears in CIP-005-1 and CIP-007-1 standards. While it is understood that each of the standards needs to stand alone on its own merits, what assurances are there that a future revision to one standard will not cause a conflict with the same item in another standard.

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.

Consumers Energy has also submitted comments via the ECAR CIPP.

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.

In the February 2nd webcast, it was stated for section R6.1 to Confirm patches are correctly installed using commercially available software. It was also stated that this is to be accomplished by testing for the vulnerability by using hacking tools. Is that what is truly meant? Or should we just be using commercial software to check for the proper patches installed?

Please clarify the 1st sentence in section R8.2, it is very confusing and unable to determine what is meant by this statement.

Need a Where Applicable statement for section R10.

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.

Consumers Energy has also submitted comments via the ECAR CIPP.

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.

Consumers Energy has also submitted comments via the ECAR CIPP.

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.

The need to secure Control Centers has been recognized for some time and implementation has also been underway while the need for securing substations and plants is new. It will be extremely difficult and expensive to meet the 1st quarter 2007 due date for these standards for substations and plants. We would recommend that the "Auditably Compliment" target for substations and plants be set to a later time period (i.e. – 1st quarter 2008).

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:	Earl Cahoe	
Organization:	Portland General Electric	
Telephone:	503-464-8892	
Email:	earl.cahoe@pgn.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.

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.

Definition of Critical Asset
Recommendation: Put boundaries around the scope. Terminate the definition after the term "… period of time." The last two phrases "… detrimental impact on the reliability or operability of the electric grid…" and "…significant risk to public health and safety…" can be interpreted to broadly.

Definition of Cyber Security Incident
Recommendation: At the beginning of the first bullet rephrase the sentence to read "Compromises or was a serious attempt to compromise…".

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.

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.

Requirements, R1.1.5
Recommendation: Need a definitive list of Regional Reliability Organizations. Define "largest single contingency" or give an example.

Measures, M2
Recommendation: Please provide an example. Would a statement like "ABC Company used a qualitative risk assessment with xxx as the criteria" be sufficient?

Measures, M6
Recommendation: Add the words "or designee's" after "… senior management officer's …". Adding a network device shouldn't require a senior VP's approval.

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.

Requirements, R4
Comment: This will be extremely expensive to implement, especially if the support for the critical cyber asset is outsourced.
Recommendation: in R4.2, remove the word "all" before the word "hardware" in the first sentence. This can be extremely expensive to implement for some devices.

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.

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.

Requirements, R3
Recommended wording: The Responsible Entity shall secure dial-up modem connections. Protection of the connection may be either remote activation/de-activation of dial-up connectivity via SCADA commands from the security or control center, or by using encryption devices meeting security level 2, or bettter, of Federal Information Processing Standards Publication (FIPS PUB) 140-1, Security Requirements for Cryptographic Modules, to ensure authenticity of the accessing device and/or application.The use of encryption modems pairs that require a secure handshake negates the need for "physically deactivating" them.

Requirements, R5
Question: is this really necessary if encryption modems pairs utilizing a secure handshake are used? See R3 above.

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.

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.

Recommendation: Creating a duplicate test environment can be very expensive. Suggest adding language that allows the vendor's testing results to be used especially if the support is outsourced to the vendor.

Requirements, R2
Comment: The wording is confusing. We're not sure what is intended.

Requirements, R4.3
Recommendation: We suggest similar language be added to each of the requirements ie, if the requirement can't be followed, allow the use of compensating measures.

Requirements, R8.2
Recommendation: Toward the end of the first sentence, add the words "permanently stored" after the words "… facilities are not…".

Requirements, R11
Question: Does this include "protective relay settings" on some critical cyber assets?

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.

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.

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.

Question: When something is to be Auditablilty Compliant in 1st quarter of 2006, does that mean, for the prior year the measures should have been in-place or does it mean starting in the 1st quarter of 2006, the measures should be in-place? In other words in the 1st quarter of 2006, would the auditors be auditing 2005's stated level of compliance or 2006's current level of compliance?

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:	Robert Strauss	
Organization:	New York State Electric & Gas Corporation	
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.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NYSEG along with NPCC feels that there are many incidents have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>.

We are concerned that "suspicious event" is too broad. We recommend changing the Cyber Security Incident definition to <<Any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.>>

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NYSEG concurs with NPCC that the answer to question 2 is "yes."

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NYSEG concurs with NPCC, that we strongly believe that CIP-002 is not ready for ballot. We believe it is important that this Standard specify that the Critical Assets to be considered are a subset of the Critical Assets as defined in the Definitions section.

Requirements R1.1.1 to R1.1.9, inclusive, are too prescriptive. This list belongs in a FAQ. We feel that cyber security personnel should not maintain a list of non-cyber equipment. Perhaps the FAQ should include a statement that <<the Responsible Entity should use a cross-functional team or other methods that are appropriate for that organization>>.

We suggest the Purpose be altered to

<<
This standard is intended to ensure that appropriate cyber 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.

With the increased use of standard technologies to connect Control Center computer systems to the bulk electrical systems, corporate business systems, and the internet, separation between the critical assets of the bulk electrical system and untrusted infrastructure has been dramatically reduced. This connectivity requires that the Control Center systems put in place a high level of Cyber Security measures to protect the Control Center and bulk electrical system assets.

Business and operational demands for managing and maintaining 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 Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system.

The Critical Cyber Assets are identified by the application of a risk-based assessment procedure on the operation of cyber assets supporting the monitoring and control of the interconnected bulk electric system.
>>

We recommend changing Requirement R4 to <<Member(s) of senior management or designee must approve the list of Critical Assets and the list of Critical Cyber Assets.>>

We recommend changing Measure M5 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Cyber Assets must be maintained.>>

We recommend changing Measure M6 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Cyber Assets must be maintained.>>

Please clarify the performance reset period in Compliance 1.2. What is being reset? Why is it being reset?

Recommend that Compliance 1.2 change from 30 days back to the 90 days specified in 1200.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NYSEG concurs with NPCC that CIP-003 needs a little more work before it is ready for ballot. This answer assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot, for more information see the response to the previous question.

We do not agree with C.M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets. We recommend that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>

Please explain what <<information security protection programs>> C.M5 refers to.

We feels that C.M10 is too prescriptive. The Compliance Submittal is signed by an authorized representative of the Responsible Entity. That commits the Entity to that information. If it is later discovered that person did not have authorization, then the Entity did not submit compliance on time, which makes the Responsible Entity non-compliant. This incents Entities to insure the appropriately documented information is submitted on-time.

We are concerned that C.M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the structure of internal corporate relationships>> too frequently.

We feel that C.M13.1 and C.M.13.2 are overly prescriptive and should be removed.

We question how to document continual engagement by executives. If it cannot be document, then it cannot be measured. We recommend removing <<and that executive level management is continually engaged in the process>> from C.M13.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4.

The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NSYEG concurs with NPCC that CIP-004 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

We believe this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.

Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.

Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003.

Measure 4.6 should be modified. The requirement for a regular 5 year update to the security screening is not consistent with Requirement R4, which states that a risk based approach be used. The need for rescreening should be cause only.

Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NYSEG concurs with NPCC that CIP-005 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

We requests clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.

Requirement R4.2's third bullet is not clear. We recommend changing from

<<

Out of band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication.

>>

to

<<

Out of band authentication procedures to augment static user id and password access. (e.g. Access will not be enabled via static user id and password authentication unless a telephone call is received from the entity requesting access. On receipt of the telephone call and after successful procedural authentication of the calling party, an administrator will enable access allowing the entitiy to utilize their static user id and password.)

>>

We believe that Requirement R3 is one of many solution to securing dial-in access. Other solutions are bullet items under Requirement R4.2. We recommend that Requirement R3 become another bullet item under Requirement R4.2.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NYSEG concurs with NPCC that CIP-006 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

The term "nearest six-wall boundary" is used in the Purpose. This term confuses some people. We recommend using <<bounded by the nearest walls, floor and ceiling>> instead.

Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2.

Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.

Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement.

Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.

Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Measure M4 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NYSEG concurs with NPCC that CIP-007 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Requirement R1 assumes that every Responsible Entity has a test system and test unit for every device. We do not agree that assumption. We do not agree that every patch on every device needs to be tested. If the same patch is applied to the same device, then it needs to be tested once. If the vendor approves the patch and the Responsible Entity applies that patch to all those devices, then the Responsible Entity has secured those devices for this standard. The main source of these objections is the last paragraph in this requirement. We recommend deleting that paragraph. We recommend changing the second sentence in the previous paragraph from
<<
Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment.>>
to
<<
Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment, where available.>>
We like the phrase <<as possible given the technical capability of the Critical Cyber Asset>> in Requirement R6.3. Perhaps this phrase should be used in a revised Requirement R1.

Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006.

Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.

Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.

Requirement R3.6 should be modified. The second sentence repeats the first, as such it is necessary and may confuse some.

Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>.

Requirement R4.1 is too prescriptive and should be deleted.

The <<monthly review>> in Requirement R4.2 is too presciptive. We recommend changing R4.2 from
<<
The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.
>>
to

<<
The Responsible Entity shall perform a routine review of the security patches available for each Critical Cyber Asset. Formal processes shall be used to document their implementation or the reason for not installing the patch.
>>

Add <<where technically feasible>> to the end of Requirement R4.3.

Requirement R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means.

Requirement R5.3 allows exception to R5.1. As such, these Requirements should be combined, otherwise one could be non-compliant with R5.1 and fully compliant with R5.3 while the intent appears to be full compliance with R5.1 and R5.3.

The combined requirement should allow technically feasible alternative solutions.

Change Requirement R5.2 from
<<
The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.
>>
to
<<
Where integrity software is deemed to be technically implementable and has been implemented, the Responsible Entity shall perform a monthly review of the integrity software to ensure that the release level of the integrity software is functionally effective and maintainable for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.
>>

We do not agree with <<site-specific installation>> in Requirement 5.4. We recommend changing from
<<
Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of malware.
>>
to
<<
Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each software deployment in order to prevent manual dissemination of malware.
>>

Change Requirement R6.1 from
<<
The Responsible Entity shall perform a vulnerability assessment at least annually that includes:

>>
to
<<
The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes:
>>

Change Requirement 6.1.3 from
<<
Factory default accounts
>>
to
<<
Scanning for factory default accounts
>>

Change Requirement 6.1.4 from
<<
Security patches and anti-virus version levels
>>
to
<<
Assessing security patches and/or anti-virus version levels, as appropriate
>>

The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assesssment schedule than an attended facility?

The title of Requirement R7 is too broad. We recommend changing this title from
<<Retention of System Logs>>
to
<<Retention of Appropriate System Logs>>
The last sentence of this requirement says the Responsible Entity determines its logging strategy. We believe this means the Responsible Entity decides which are the appropriate system logs to retain.

Requirement R9 should clarify that it pertains to ports inside the perimeter. Requirement R2 of CIP-005 covers ports at the perimeter.

The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.

Requirement R11 belongs in CIP-009. This requirement should be moved to that standard. This requirement references Critical Assets. That is not correct. It should a requirement for the backup and recovery of Critical Cyber Assets. The requirement starts with <<on a regular basis>>, and the third sentence says <<at least annually>>. The requirement should stipulate one or the other. We recommend removing <<annually>>. The last sentence is unclear and should be deleted.

Change Measure M2. The semi-annual audit is too prescriptive. This requirements recognizes that the frequency of password changes should be determined by risk assessment.

<<where applicable>> should added to the end of Measure 4.3.

Change the Measures M5.1 - M5.3 from
<<
M5.1 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.
M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found.
M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities.
>>
to
<<
M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments.
M5.2 The documentation shall include a record of the results of the annual vulnerability assessment.
M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions.
>>

Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the perimeter.

Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.

Which Requirement and Measurement is Compliance 2.1 associated with?

Compliance 2.2.1.1 needs to be changed so that it is consistent with changes to the corresponding Requirement(s) and Measure(s). This compliance is restricted to <<inside the perimeter>>. There should be no stated difference in the time frames for attended and unattended facilities.

Clarify if Compliance 2.3 should be read as [2.3.1 or 2.3.2 or 2.3.3 (etc)] OR [2.3.1 and 2.3.2 and 2.3.3 (etc)]. We suggest that all of these standards include a statement regarding compliance levels with multiple items.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NYSEG concurs with NPCC that CIP-008 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from
<<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>>
to
<<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>>

Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3.

The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows
<<
The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.
>>

Compliance 1.4 stipulates a requirement that is not in the second posting. We recommend creating a Requirement R2 as follows
<<
R2. The Responsible Entity shall keep all records related to each Cyber Security Incident for three calendar years. This includes, where appropriate, but is not limited to the following:
R2.1 System and application log file entries,
R2.2 Appropriate physical access records,
R2.3 Documented records of investigations and analysis performed, as available,
R2.4 Records of any action taken including any recovery actions initiated.
R2.5 Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.
>>

These changes call for a different Measure M2. <<The Responsible Entity shall retain records for each Cyber Security Incident for three calendar years.>>

We recommend changing Compliance 1.2 from
<<
The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance reset period shall be one (1) calendar year.
>>
to
<<
The compliance monitoring period shall keep be three (3) calendar years. The performance reset period shall be one (1) calendar year.
>>

We recommend changing Compliance 1.3 from
<<
The Responsible Entity shall keep documents specified in this standard for three calendar years.
>>
to
<<
The Responsible Entity shall keep all data specified in this standard for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.
>>

We recommend changing Compliance 2.1.1 from
<<
Documentation exists, but has not been updated with known changes with 90 calendar days.
>>
to
<<
Documentation necessary to demonstrate compliance with Measure M1 exists, but has not been updated within 90 calendar days of known changes.
>>

We recommend changing Compliance 2.2.1 from
<<
Incident response documentation exists, but has not been updated or reviewed within the last 12 months
>>
to
<<
Cyber Security Incident Response Plan documentation exists, but has not been updated or reviewed within the last 12 months
>>

We recommend changing Compliance 2.2.2 from
<<
Incident response documentation exists but is incomplete
>>
to
<<
Cyber Security Incident Response Plan documentation exists but is incomplete
>>

We request clarification on the threshold for Compliance 2.3.2.

Change Compliance 2.4 from
<<
No documentation exists
>>
to
<<
2.4.1 Cyber Security Incident Response Plan documentation does not exist
2.4.2 Cyber Security Incidents have occurred and none were reported to the ES-ISAC

>>

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NYSEG concurs with NPCC that CIP-009 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

We are not sure how broad this standard is. If this is the Recovery Plans of Critical Cyber Assets from Cyber Security Incidents, then the following comments apply.

Requirements R1 and R2 should be swapped. We recommend changing the first requirement from
<<
The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan.
>>
to
<<
The Responsible Entity shall specify the appropriate response to Cyber Security Incidents of varying duration and severity that would require the activation of a Critical Cyber Asset Recovery Plan.
>>
Furthermore, we recommend changing the second requirement from
<<
The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan at least annually.
>>
to
<<
The Responsible Entity shall create recovery plan(s) for those events and assets indentified in R1 and exercise its recovery plan(s) as defined by its risk based assessment.
>>

We believe that Requirement R3 has the right intention, but its wording is too broad. We recommend changing from
<<
The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.
>>
to
<<
The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan(s).
>>

Requirement R5 is covered in CIP-004. R5 should be deleted.

We believe that Measures M2 and M3 are duplicates. We recommend deleting Measure M2.

Measure M3 corresponds to Requirement R3. We changed Requirement R3. Measure M3 needs a similar modification from
<<
The Responsible Entity shall review and update recovery plan(s) annually.
>>
to
<<
The Responsible Entity shall review and update recovery plan(s) as prescribed by its risk based assessment.
>>

Since Requirement R5 is deleted, the corresponding Measure M4 should be deleted. This is covered in CIP-004.

Compliance 1.3 restates Measure M1. Compliance 1.3 needs different words or should be deleted.

Compliance 2.1 should be changed from
<<
Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year
>>
to
<<
Recovery plan(s) exist, but have not been reviewed or updated, if necessary, in the last calendar year
>>

As posted, if a Responsible Entity has not reviewed their recovery paln(s) in the last calendar year, they are Level 1 and Level 2 non-compliant. This is confusing. Also, training is covered in CIP-004. Compliance 2.2 should be changed from
<<
Recovery plan(s) have not been reviewed, exercised or training performed.
>>
to
<<
Recovery plan(s) have not been exercised according to the Responsible Entity's risk based assessment.
>>

Compliance 2.3 includes specific roles and responsibilities that are not in the Requirements or the Measures. It is confusing and inappropriate to introduce new requirements in Compliance. The reference to <<types of events that are necessary>> is confusing. This standard specifies no types of events as <<necessary>>.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NYSEG concurs with NPCC that the Implementation Plan does not allow enough time for compliance. First, these standards have substantial changes from 1200. A Responsible Entity could be compliant with 1200 and require much work before they are compliant with these standards. Secondly, budgets are established months ahead of time. Some Responsible Entities have frozen their 2005 budgets. For either reason. there are enough Entities that will not meet the initial dates for auditable compliance or substantial compliance (first quarter of 2006) .

In fact most entities 2006 budgets will be submitted and approved prior to the final approval and implementation of these standards . At a minimum we recommend that the 2006 dates change to 2007 dates, the 2007 dates change to 2008 dates, etc. A more practical and efficient approach would be for RC and BA to follow the 1200 requirements for 2006, then the BA and RC would be required to be substantially compliant in 2007 and auditably compliant in 2008. All other Responisible Entities would be required to meet the 1200 standards in 2007, substantially compliant in 2008 and auditably compliant in 2009.

We are concerned with compliance for substations. Substations are part of the <<Other Facilities>>. We recommend the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.

Clarify what dates the compliance submittal is for. Is the first quarter submittal of 2007 for January 1, 2006 to December 31, 2006? Or is the 2007 submittal as of a year ending on the submittal date? Or is the 2007 submittal what the Entity has as of that submittal date?

If the Functional Model is not implemented according to the Functional Model schedule, what is the impact on the Cyber Security Implementation Plan?

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:	Francis J. Flynn, Jr., PE	
Organization:	National Grid USA	
Telephone:	1-508-389-2578	
Email:	francis.flynn@us.ngrid.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.

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.

National Grid has some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

National Grid feels that there are many incidents that may have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>.

We are concerned that "suspicious event" is too broad. We recommend changing the Cyber Security Incident definition to <<Any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.>>

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.

Yes to Question regarding assessment methodology.

National Grid has some other General Comments regarding this standard as defined below.

This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

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.

NO

National Grid has some General Comments.

This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NPCC strongly believes that CIP-002 is not ready for ballot. We believe it is important that this Standard specify that the Critical Assets to be considered are a subset of the Critical Assets as defined in the Definitions section.

Requirements R1.1.1 to R1.1.9, inclusive, are too prescriptive. This list belongs in a FAQ. We feel that cyber security personnel should not maintain a list of non-cyber equipment. Perhaps the FAQ should include a statement that <<the Responsible Entity should use a cross-functional team or other methods that are appropriate for that organization>>.

We suggest the Purpose be altered to

<<
This standard is intended to ensure that appropriate cyber 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.

With the increased use of standard technologies to connect Control Center computer systems to the bulk electrical systems, corporate business systems, and the internet, separation between the critical assets of the bulk electrical system and untrusted infrastructure has been dramatically reduced. This connectivity requires that the Control Center systems put in place a high level of Cyber Security measures to protect the Control Center and bulk electrical system assets.

Business and operational demands for managing and maintaining 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 Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system.

The Critical Cyber Assets are identified by the application of a risk-based assessment procedure on the operation of cyber assets supporting the monitoring and control of the interconnected bulk electric system.
>>

National Grid recommends that Requirement R2.1 The Cyber Asset uses a routable protocol or

Be change to: R2.1 The Cyber Asset uses a routable protocol that is in fact routed over a Wide Area Network (WAN) or;

National Grid recommends changing Requirement R4 to <<Member(s) of senior management or designee must approve the list of Critical Assets and the list of Critical Cyber Assets.>>

We recommend changing Measure M5 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Cyber Assets must be maintained.>>

We recommend changing Measure M6 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Cyber Assets must be maintained.>>

Please clarify the performance reset period in Compliance 1.2. What is being reset? Why is it being reset?

Recommend that Compliance 1.2 change from 30 days back to the 90 days specified in 1200.

Review of all Requirements and Measures must be performed by the drafting team. Throughout the document there are inconsistancies between requirements and measures. The drafting team must resolve all these inconsistancies. They are to numerous to mention. The drafting team must look at them all. We find that the defined measures are requirements and should be detailed as requirements.

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.

National Grid has some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

National Grid feels CIP-003 needs a little more work before it is ready for ballot. This answer assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot, for more information see the response to the previous question.

We do not agree with C.M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets. We recommend that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>

Please explain what <<information security protection programs>> C.M5 refers to.

We feels that C.M10 is too prescriptive. The Compliance Submittal is signed by an authorized representative of the Responsible Entity. That commits the Entity to that information. If it is later discovered that person did not have authorization, then the Entity did not submit compliance on time, which makes the Responsible Entity non-compliant. This incents Entities to insure the appropriately documented information is submitted on-time.

We are concerned that C.M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the structure of internal corporate relationships>> too frequently.

We feel that C.M13.1 and C.M.13.2 are overly prescriptive and should be removed.

We question how to document continual engagement by executives. If it cannot be document, then it cannot be measured. We recommend removing <<and that executive level management is continually engaged in the process>> from C.M13.

In section D of compliance 2.1.4 references 'an information security protection prgram exists but has not been reviewed in the last calendear year'. National Grid cannot find a Requirement within the standard that this is required. The Drafting Team must clarify and clearly explain and document what the requirement is.

Review of all Requirements and Measures must be performed by the drafting team. Throughout the document there are inconsistancies between requirements and measures. The drafting team must resolve all these inconsistancies. They are to numerous to mention. The drafting team must look at them all. We find that the defined measures are requirements and should be detailed as requirements.

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.

National Grid has some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

National Grid feels CIP-004 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

National Grid feels this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.

Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.

Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003.

Measure 4.6 should be modified. The requirement for a regular 5 year update to the security screening is not consistent with Requirement R4, which states that a risk based approach be used. The need for rescreening should be cause only.

Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures.

Review of all Requirements and Measures must be performed by the drafting team. Throughout the document there are inconsistancies between requirements and measures. The drafting team must resolve all these inconsistancies. They are to numerous to mention. The drafting team must look at them all. We find that the defined measures are requirements and should be detailed as requirements.

National Grid believes that the Levels of Non-Compliance within this standard appars to penalize very large corporations more, where the possibility of the number of instances that personnel might be terminated where they do not meet the turnaround time on control list updates , etc. would not be met. An example of this is if you have 5 errors in an organization that has a list of 10,000 people vs 5 errors where there is a list of 50 people, are these instances both treated equally? Please clarify this point.

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.

National Grid has some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

National Grid beleives CIP-005 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

National Grid requests clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.

Requirement R4.2's third bullet is not clear. We recommend changing from
<<
Out of band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication.
>>
to
<<
Out of band authentication procedures to augment static user id and password access. (e.g. Access will not be enabled via static user id and password authentication unless a telephone call is received from the entity requesting access. On receipt of the telephone call and after successful procedural authentication of the calling party, an administrator will enable access allowing the entitiy to utilize their static user id and password.)
>>

National Grid believes that Requirement R3 - "Where remote activation of dial-up connectivity via SCADA-activated relays from the security or control center is technically feasible,….." is one of many solutions to securing dial-in access. Other solutions are bullet items under Requirement R4.2. National Grid highly recommends that Requirement R3 become another bullet item under Requirement R4.2. Otherwise the System Operator whose main task is to Monitor, Control and Operate the Bulk Power System becomes a clerk and begions performing tasks that are not part of their respective job functions.

Review of all Requirements and Measures must be performed by the drafting team. Throughout the document there are inconsistancies between requirements and measures. The drafting team must resolve all these inconsistancies. They are to numerous to mention. The drafting team must look at them all. We find that the defined measures are requirements and should be detailed as requirements.

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.

National Grid has some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

National Grid believes CIP-006 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

The term "nearest six-wall boundary" is used in the Purpose. This term confuses some people. We recommend using <<bounded by the nearest walls, floor and ceiling>> instead.

Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2.

Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.

Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement.

Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.

Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Measure M4 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.

Review of all Requirements and Measures must be performed by the drafting team. Throughout the document there are inconsistancies between requirements and measures. The drafting team must resolve all these inconsistancies. They are to numerous to mention. The drafting team must look at them all. We find that the defined measures are requirements and should be detailed as requirements.

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.

National Grid has some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

National Grid believes CIP-007 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Requirement R1 assumes that every Responsible Entity has a test system and test unit for every device. We do not agree that assumption. We do not agree that every patch on every device needs to be tested. If the same patch is applied to the same device, then it needs to be tested once. If the vendor approves the patch and the Responsible Entity applies that patch to all those devices, then the Responsible Entity has secured those devices for this standard. The main source of these objections is the last paragraph in this requirement. We recommend deleting that paragraph. We recommend changing the second sentence in the previous paragraph from
<<
Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment.>>
to
<<
Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment, where available.>>
We like the phrase <<as possible given the technical capability of the Critical Cyber Asset>> in Requirement R6.3. Perhaps this phrase should be used in a revised Requirement R1.

Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006.

Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.

Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.

Requirement R3.6 should be modified. The second sentence repeats the first, as such it is necessary and may confuse some.

Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>.

Requirement R4.1 is too prescriptive and should be deleted.

The <<monthly review>> in Requirement R4.2 is too presciptive. We recommend changing R4.2 from
<<
The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.
>>
to
<<
The Responsible Entity shall perform a routine review of the security patches available for each Critical Cyber Asset. Formal processes shall be used to document their implementation or the reason for not installing the patch.
>>

Add <<where technically feasible>> to the end of Requirement R4.3.

Requirement R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means.

Requirement R5.3 allows exception to R5.1. As such, these Requirements should be combined, otherwise one could be non-compliant with R5.1 and fully compliant with R5.3 while the intent appears to be full compliance with R5.1 and R5.3.

The combined requirement should allow technically feasible alternative solutions.

Change Requirement R5.2 from
<<
The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.
>>
to
<<
Where integrity software is deemed to be technically implementable and has been implemented, the Responsible Entity shall perform a monthly review of the integrity software to ensure that the release level of the integrity software is functionally effective and maintainable for each Critical

Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.
>>

We do not agree with <<site-specific installation>> in Requirement 5.4. We recommend changing from
<<
Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of malware.
>>
to
<<
Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each software deployment in order to prevent manual dissemination of malware.
>>

Change Requirement R6.1 from
<<
The Responsible Entity shall perform a vulnerability assessment at least annually that includes:
>>
to
<<
The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes:
>>

Change Requirement 6.1.3 from
<<
Factory default accounts
>>
to
<<
Scanning for factory default accounts
>>

Change Requirement 6.1.4 from
<<
Security patches and anti-virus version levels
>>
to
<<
Assessing security patches and/or anti-virus version levels, as appropriate
>>

The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assesssment schedule than an attended facility?

The title of Requirement R7 is too broad. We recommend changing this title from

<<Retention of System Logs>>
to
<<Retention of Appropriate System Logs>>
The last sentence of this requirement says the Responsible Entity determines its logging strategy. We believe this means the Responsible Entity decides which are the appropriate system logs to retain.

Requirement R9 should clarify that it pertains to ports inside the perimeter. Requirement R2 of CIP-005 covers ports at the perimeter.

The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.

Requirement R11 belongs in CIP-009. This requirement should be moved to that standard. This requirement references Critical Assets. That is not correct. It should a requirement for the backup and recovery of Critical Cyber Assets. The requirement starts with <<on a regular basis>>, and the third sentence says <<at least annually>>. The requirement should stipulate one or the other. We recommend removing <<annually>>. The last sentence is unclear and should be deleted.

Change Measure M2. The semi-annual audit is too prescriptive. This requirements recognizes that the frequency of password changes should be determined by risk assessment.

<<where applicable>> should added to the end of Measure 4.3.

Change the Measures M5.1 - M5.3 from
<<
M5.1 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.
M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found.
M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities.
>>
to
<<
M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments.
M5.2 The documentation shall include a record of the results of the annual vulnerability assessment.
M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions.
>>

Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the perimeter.

Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.

Which Requirement and Measurement is Compliance 2.1 associated with?

Compliance 2.2.1.1 needs to be changed so that it is consistent with changes to the corresponding Requirement(s) and Measure(s). This compliance is restricted to <<inside the perimeter>>. There should be no stated difference in the time frames for attended and unattended facilities.

Clarify if Compliance 2.3 should be read as [2.3.1 or 2.3.2 or 2.3.3 (etc)] OR [2.3.1 and 2.3.2 and 2.3.3 (etc)]. We suggest that all of these standards include a statement regarding compliance levels with multiple items.

Review of all Requirements and Measures must be performed by the drafting team. Throughout the document there are inconsistancies between requirements and measures. The drafting team must resolve all these inconsistancies. They are to numerous to mention. The drafting team must look at them all. We find that the defined measures are requirements and should be detailed as requirements.

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.

National Grid has some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

National Grid believes CIP-008 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from
<<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>>
to
<<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>>

Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3.

The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows
<<
The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.

>>

Compliance 1.4 stipulates a requirement that is not in the second posting. We recommend creating a Requirement R2 as follows
<<
R2. The Responsible Entity shall keep all records related to each Cyber Security Incident for three calendar years. This includes, where appropriate, but is not limited to the following:
R2.1 System and application log file entries,
R2.2 Appropriate physical access records,
R2.3 Documented records of investigations and analysis performed, as available,
R2.4 Records of any action taken including any recovery actions initiated.
R2.5Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.
>>

These changes call for a different Measure M2. <<The Responsible Entity shall retain records for each Cyber Security Incident for three calendar years.>>

We recommend changing Compliance 1.2 from
<<
The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance reset period shall be one (1) calendar year.
>>
to
<<
The compliance monitoring period shall keep be three (3) calendar years. The performance reset period shall be one (1) calendar year.
>>

We recommend changing Compliance 1.3 from
<<
The Responsible Entity shall keep documents specified in this standard for three calendar years.
>>
to
<<
The Responsible Entity shall keep all data specified in this standard for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.
>>

We recommend changing Compliance 2.1.1 from
<<
Documentation exists, but has not been updated with known changes with 90 calendar days.
>>
to
<<
Documentation necessary to demonstrate compliance with Measure M1 exists, but has not been updated within 90 calendar days of known changes.
>>

We recommend changing Compliance 2.2.1 from
<<

Incident response documentation exists, but has not been updated or reviewed within the last 12 months
>>
to
<<
Cyber Security Incident Response Plan documentation exists, but has not been updated or reviewed within the last 12 months
>>

We recommend changing Compliance 2.2.2 from
<<
Incident response documentation exists but is incomplete
>>
to
<<
Cyber Security Incident Response Plan documentation exists but is incomplete
>>

We request clarification on the threshold for Compliance 2.3.2.

Change Compliance 2.4 from
<<
No documentation exists
>>
to
<<
2.4.1 Cyber Security Incident Response Plan documentation does not exist
2.4.2 Cyber Security Incidents have occurred and none were reported to the ES-ISAC
>>

Review of all Requirements and Measures must be performed by the drafting team. Throughout the document there are inconsistancies between requirements and measures. The drafting team must resolve all these inconsistancies. They are to numerous to mention. The drafting team must look at them all. We find that the defined measures are requirements and should be detailed as requirements.

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.

National Grid has some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

National Grid believes CIP-009 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

We are not sure how broad this standard is. If this is the Recovery Plans of Critical Cyber Assets from Cyber Security Incidents, then the following comments apply.

Requirements R1 and R2 should be swapped. We recommend changing the first requirement from
<<
The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan.
>>
to
<<
The Responsibel Entity shall specify the appropriate response to Cyber Security Incidents of varying duration and severity that would require the activation of a Critical Cyber Asset Recovery Plan.
>>
Furthermore, we recommend changing the second requirement from
<<
The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan at least annually.
>>
to
<<
The Responsible Entity shall create recovery plan(s) for those events and assets indentified in R1 and exercise its recovery plan(s) as defined by its risk based assessment.
>>

We believe that Requirement R3 has the right intention, but its wording is too broad. We recommend changing from
<<
The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.
>>
to
<<
The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan(s).
>>

Requirement R5 is covered in CIP-004. R5 should be deleted.

We believe that Measures M2 and M3 are duplicates. We recommend deleting Measure M2.

Measure M3 corresponds to Requirement R3. We changed Requirement R3. Measure M3 needs a similar modification from
<<
The Responsible Entity shall review and update recovery plan(s) annually.
>>
to
<<
The Responsible Entity shall review and update recovery plan(s) as prescribed by its risk based assessment.
>>

Since Requirement R5 is deleted, the corresponding Measure M4 should be deleted. This is covered in CIP-004.

Compliance 1.3 restates Measure M1. Compliance 1.3 needs different words or should be deleted.

Compliance 2.1 should be changed from
<<
Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year
>>
to
<<
Recovery plan(s) exist, but have not been reviewed or updated, if necessary, in the last calendar year
>>

As posted, if a Responsible Entity has not reviewed their recovery paln(s) in the last calendar year, they are Level 1 and Level 2 non-compliant. This is confusing. Also, training is covered in CIP-004. Compliance 2.2 should be changed from
<<
Recovery plan(s) have not been reviewed, exercised or training performed.
>>
to
<<
Recovery plan(s) have not been exercised according to the Responsible Entity's risk based assessment.
>>

Compliance 2.3 includes specific roles and responsibilities that are not in the Requirements or the Measures. It is confusing and inappropriate to introduce new requirements in Compliance. The reference to <<types of events that are necessary>> is confusing. This standard specifies no types of events as <<necessary>>.

Review of all Requirements and Measures must be performed by the drafting team. Throughout the document there are inconsistancies between requirements and measures. The drafting team must resolve all these inconsistancies. They are to numerous to mention. The drafting team must look at them all. We find that the defined measures are requirements and should be detailed as requirements.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NPCC feels the Implementation Plan does not allow enough time for compliance. First, these standards have substantial changes from 1200. A Responsible Entity could be compliant with 1200 and require much work before they are compliant with these standards. Secondly, budgets are established months ahead of time. Some Responsible Entities have frozen their 2005 budgets. For either reason. there are enough Entities that will not meet the initial dates for auditable compliance or substantial compliance (first quarter of 2006) . We recommend that the 2006 dates change to 2007 dates, the 2007 dates change to 2008 dates, etc.

We are concerned with compliance for substations. Substations are part of the <<Other Facilities>>. We recommend the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.

Clarify what dates the compliance submittal is for. Is the first quarter submittal of 2007 for January 1, 2006 to December 31, 2006? Or is the 2007 submittal as of a year ending on the submittal date? Or is the 2007 submittal what the Entity has as of that submittal date?

If the Functional Model is not implemented according to the Functional Model schedule, what is the impact on the Cyber Security Implementation Plan?

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:	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.

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.

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.

Critical Asset

We recommend clarification through a FAQ on what is considered a large quantity of customers and what constitutes an extended period of time. Alternatively, the definition could be modified to reflect that the responsible entity is responsible for defining what it considers to be a significant or detrimental impact.

Cyber Assets

The association of Cyber Assets to the bulk electric system occurs through the definition of Critical Cyber Assets. Also, the standard now includes other Cyber Assets connected within the Electronic Security Perimeter. The definition of Cyber Assets should not include the association to the bulk electric system assets. We recommend that this definition be changed to:

Programmable electronic devices and communication networks including hardware, software, and data.

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.

1)

R1.1 combines both tangible and intangible assets in a single, long sentence. For clarity, we recommend that section R1.1 read:

Critical Assets: The Responsible Entity shall identify its Critical Assets. For the purpose of this standard the list of Critical Assets consists of those facilities, systems, and equipment, which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a detrimental impact on the reliability or operability of the electric grid. Also to be included are critical operating functions and tasks that affect the interconnected bulk electric system such as, but not limited to: monitoring and control, load and frequency control, emergency actions, contingency analysis, special protection systems, power plant control, substation control, and real-time information exchange.

2)

R1.1 could be interpreted that all assets that meet requirements R1.1.1 through R1.1.8 are automatically added to the list of critical assets, regardless of the outcome of the risk-based assessment.

We recommend that the last sentence in R1.1 be changed from:

Those Critical Assets including the following:

to:

The following assets must be considered in the risk-based assessment:

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.

1)
We believe that the risk-based assessment and applying greater protections to Critical Cyber Assets is a sound security practice introduced in this standard. However, R3 and M3 could be interpreted that all assets within the perimeter are subject to the CIP-002 through CIP-009 standards. If this interpretation is correct, it could result in non-critical assets being added to the scope of these standards and negate the benefits of the risk-based assessment.

The purpose of R3 should be to identify other assets that are within the same Electronic Security Perimeter as identified Critical Cyber Assets. R3 should not define protection mechanisms. We recommend that R3 be changed to:

The responsible entity shall identify other Cyber Assets within the same Electronic Security Perimeter as the identified Critical Cyber Assets.

2)
In M3 the sentence reads: …Critical Cyber Assets as identified under Requirement R3…

Critical Cyber assets are identified in R2, so the sentence should be changed to:
…Critical Cyber Assets asssts identified under Requirement R2…

3)
Please provide more direction, perhaps in a FAQ, on whether voice and PBX telecommunications equipment should be considered in the risk-based assessment. Or should they be considered support systems as described in FAQ 13?

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.

1)
The requirement for change management in R4.2 is nearly identical to CIP-007-1 R8.1. We recommend that change management only be defined as a requirement in one standard.

2)
R5 does not accurately describe the scope of R5.1 through R5.3. R5 describes management of access to information associated with Critical Cyber Assets. R5.1 through R5.3 describes management of physical and electronic access to Critical Cyber Assets.

We recommend that the following be deleted from R5: …information associated with…

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.

1)
M4.6 requires update to the personnel risk assessment 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 require reassessments for employees of the responsible entity.

2)
Is the intent of M2 to require that all personnel with access to Critical Cyber Assets be retrained annually on cyber security, or just that the training program needs to be reviewed and updated annually?
We recommend that the training program be reviewed and updated annually. We also recommend that since M1 requires quarterly reinforcement of sound security practices, that the responsible entity will be responsible for determining if any retraining is necessary.

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.

1)

We believe that the risk-based assessment and applying greater protections to Critical Cyber Assets is a sound security practice introduced in this standard. However, applying all requirements of CIP-005 to non-Critical Cyber Assets within the defined Electronic Security Perimeter (referred to as other Cyber Assets in R3 of CIP-002) negates the benefits of the risk-based assessment. For other Cyber Assets, only R3 and R4 should be required.

We recommend that the last sentence in R1 be changed to:

Other Cyber Assets as identified in R3 of CIP-002 must comply with R3 and R4 of this standard.

2)

Levels of non-compliance under D2 do not allow for any gaps in monitoring. One minute of lost logging is a Level 1 violation. Since 100% uptime is almost impossible, no one could be compliant.

The physical monitoring in CIP-006 has a better approach - it looks at aggregate gaps within a time period when measuring levels of non-compliance. We recommend replacing D2.1.2, 2.2.2, and 2.3.4 of this standard with the D2.1.2, 2.2.2, 2.3.2 from CIP-006.

If the CIP-006 approach is not used, we recommend changing 2.1.2 to:

Access to any Critical Cyber Asset was unmonitored for 24 hours or more.

3)

M2 requires responsible entities to maintain documentation of all ports and services available on Critical Cyber Assets. This requirement will be very difficult to implement and of little value. We recommend removing this requirement.

4)

R6 calls for quarterly reviews of documentation and processes. M6 calls for annual reviews of documents. Process documentation is not likely to change very often, so quarterly reviews are of low value. We recommend that the review period be yearly and only be specified in the measures section.

5)

The organizational and procedure references of R4 and M4 are redundant with R5 of CIP003. We recommend that R4 only address technical controls.

6)

R2 is almost identical to R9 of CIP-007. We recommend that this requirement only be specified in one standard.

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.

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.

1)
Several requirements in this standard reference unattended facilities. These requirements specify special provisions that need to be taken at unattended facilities (e.g. change management and virus checking). Cyber Assets in unattended facilities that are connected to a WAN do not require special provisions. We recommend clarifying through a FAQ the definition of an unattended facility.

2)
In R1 the scope of any security testing should be for compliance to company cyber security standards, such as password standards. Requiring responsible entities to perform specialized testing of all vendor software used in an organization as implied during the Webcast is not feasible. Responsible entities cannot be specialists in vendor software testing since the details of most vulnerabilities are not released to the public. Responsible entities must be able to accept the security certifications provided by the vendor.

3)
R3.3 describes physical access to unattended facilities. Physical access controls are defined in CIP-006. We recommend that R3.3 be deleted.

4)
R3.4 requires semi-annual reviews of access rights. M18 of CIP-003 requires annual reviews of access rights. We recommend that R3.4 from this standard be consolidated with R5.2 of CIP-003.

5)
R6 requires annual vulnerability assessments. Vulnerability scanning is a mitigating control to ensure that other controls such as change management, security testing, and patch management are effective. We recommend that vulnerability scans be performed once every three years.

6)
M2 requires auditing of passwords against the responsible entities policy. It is not clear if the intent is to ensure that the system is configured to enforce password standards such as length and complexity or if the intent is to check for weak passwords using password-cracking tools. We recommend that this measurement be clarified.

7)
We recommend that the last sentence in M2 be changed from:
… have a change n status …
to:
…have a change in status …

8)
M2 requires review of access permissions within 24 hours for any personnel terminated for cause. This is redundant with M4.3 of CIP-004. We recommend that this measurement only be specified in one standard.

9)
R9 is almost identical to R2 of CIP-005. We recommend that this requirement only be specified in one standard.

10)
M8 requires responsible entities to maintain documentation of all ports and services available on Critical Cyber Assets. This requirement will be very difficult to implement and of little value. We recommend removing this requirement.

11)
We recommend that an FAQ be created to define integrity software.

12)
D1.2 requires that data shall be kept for three years. R7.1 requires that logs should be kept for 90 days. We request that these data retention periods be clarified.

13)
FAQ #13 references question one above. Should the reference really be to FAQ #12?

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.

1)
We recommend removing the word ALL from R4. The IAW SOP has detailed criteria for what sort of incidents should be reported.

2)
The measures do not cover all aspects of R1 such as assessing, mitigating and containing. We recommend that the measures include all aspects of the requirements.

3)
If multiple responsible entities are affected by the same incident, do they all report it to the ES ISAC? We recommend that this scenario be clarified in a FAQ.

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.

1)
R1 requires that recovery plans be exercised at least annually. M4 requires that the responsible entity conduct drills at least every three years. If a drill is different than an exercise, we recommend that the terms be defined. If a drill is not different than an exercise, we recommend that the testing periods for R1 and M4 be the same.

2)
Is the training in R5 meant to be additional, focused training on recovery processes, or is it the general training referred to in CIP-004?

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.

Until the requirements and measurements of these standards are more clearly defined, we cannot make a determination if there is enough time for compliance.

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:	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.

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.

Since there is no place for overall/general comments, the following applies to all standards:

The high level numbering of requirements and measures must match. This is true in some standards, but in others, the numbering in the measures do not match requirements.

While the changes in the standards are highlighted in a separate document, they will be easier to follow in a change section at the beginning of each standard as a preamble to the standard itself.

The standards expressly exclude nuclear facilities. In the absence of cyber security standards for nuclear facilities, does this exclusion not introduce a considerable vulnerability in the overall reliable operation of the bulk electric system? It is generally understood that any Federal requirement which are more stringent overrides these standards.

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.

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.

R1: the word "preferred" in "Responsible Entities shall identify their critical Assets using their preferred risk-based assessment." might leave things too open for different interpretations. Either replace with another word (determined??) and/or give more guidance.

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.

The Measures are not properly aligned with the requirements. This makes the document hard to follow.

M-2 States a “no longer than 3-year period” for reviewing the cyber security policy. Non-Compliance Level 1 2.1.2 makes this an annual requirement. D 2.1.2 should be revised to reflect the 3 year review requirement.

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.

Measure M4.4 currently states:

"The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel prior to being granted authorized 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 identity verification (e.g., Social Security Number verification in the U.S.) 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."

The operating requirements and environments of Responsible Entities vary widely. Prescribed requirements may not be appropriate depending on these requirements and environments. In addition, the background check requirement should not be contingent on any “bargaining agreement” . It is our opinion that this type of requirement is similar to a local law and the law overrides.

Proposed M4.4:

"The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel prior to being granted authorized access to Critical Cyber Assets in accordance with federal, state, provincial, and local laws. Based on this risk assessment, the Responsible Entity will identify personnel which warrant further assessment, which must include a minimum of identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check. Entities may conduct more detailed reviews, as permitted by law, depending upon thecriticality of the position."

Measure M4.6 currently states:

"The Responsible Entity shall conduct update screenings at least every five years or for cause."

Con Edison feels that the Responsible Entity's risk assessment process should determine update screenings.

Proposed M4.6:

"The Responsible Entity shall conduct update screenings as determined by its documented personnel risk assessment process or for cause."

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.

R6/M6: R6 states 90 days while M6 states "annually". R6 should define an annual review, consistent with other cyber security 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.

R2/M2 not clear; give examples of "industry or government, generally accepted, risk assessment procedure."

The content of Requirements does not necessarily match the content of the Measurements; for example R2 talks about Physical Access Control while M3 and not M2 talks about that.

D.1.3: it is not clear what documents are referred to in 1.3 (Compliance section) to be kept for three calendar years.

D.2.1.1: neglects to mention (as in M1) that the 90 day review applies in the case of modification to the perimeter or physical security methods.
Change to:
2.1.1 Document(s) exist, but have not been reviewed for more than 1 year or have not been updated within 90 days of modifications.

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.

R1/M1: tests performed by vendors to verify the effectiveness of the patch should be deemed acceptable; for example, a patch tested and released by an EMS vendor would not have to be tested again; a security patch tested and released by Microsoft would not have to be tested again for its effectiveness at remediating the vulnerability. It is unreasonable to expect the Responsible Entity to verify that a vendor supplied patch to fix a specific vulnerability is indeed effective by developing, in cases where exploit code is not available, and running exploit code to verify the effectiveness of the patch. The Responsible Entity should only be required to perform functional quality assuarnce prior to applying the patch in production. The Responsible Entity should only be expected to verify that the patch has been correctly installed. The requirement for vulnerability assessment addresses the testing of vulnerabilities on a regular basis.

R.6.3: doesn't the "limited vulnerability assessment" here imply that the unattended Critical Cyber Assets are less critical than the attended one?

R5.1 This could be made clearer. Why state Wide area network and then include any networked device it may connect to. A statement like “Any Critical Cyber Asset connected to a network or device connected to a network” would mean the same and has less ambiguity.

R8 and R9 are covered in CIP-003.

M10 Back-up and Recovery - The Requirement, Measure and Compliance sections do not match. The Requirement states “information stored on computer media for a prolonged period of time must be tested annually.” The Measure and Compliance sections state that you must do an annual restoration exercise. We have several instances in our backup procedures were nothing is stored on computer media longer than 30 days. I do not interpret this as a prolonged period of time. The

Measure and Compliance sections mention documentation not mentioned in the requirement section.

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.

The requirements and measures section is not consistent in qualifying incidents as cyber incidents. This standard only applies to cyber incidents.

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.

Change R3 to:

R3. The Responsible Entity shall review recovery plan(s) at least annually and update these recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.

M5 requires drills at least every 3 years. R1 requires this at least annually.

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.

The scope and requirements of the standards have been substantially expanded from Urgent Action Standard 1200 and will not be finalized until September 2005. Because of budget planning cycles and in consideration of the substantial financial commitment required to meet these expanded requirements, full Auditable Compliance should be deferred to 2008 for entities owning a large number of field facilities (i.e. other than BA and RC).

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 the 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**
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: **NPCC CP9**

Lead Contact: Guy Zito

Contact Organization: NPCC

Contact Segment: 2

Contact Telephone: 212-840-1070

Contact Email: gzito@npcc.org

Additional Member Name	Additional Member Organization	Region*	Segment*
Ralph Rufrano	New York Power Authority	NPCC	1
Kathleen Goodman	ISO-New England	NPCC	2
Roger Champagne	TransEnergie, Quebec	NPCC	1
Peter Lebro	US National Grid	NPCC	1
David Kiguel	Hydro One Networks, Ontario	NPCC	1
Khaqan Khan	The IESO, Ontario	NPCC	2
Alan Adamson	New York State Reliability Counc	NPCC	2
Brian Hogue	NPCC	NPCC	2
Guy Zito	NPCC	NPCC	2
Bob Pelligrini	United Illuminating	NPCC	1
Greg Campoli	New York ISO	NPCC	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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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 devided 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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

~~——~~NPCC Participating Members~~We~~ have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NPCC Participating Members feel~~s~~ that there are many incidents have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>.

~~We~~NPCC Participating Members are concerned that "suspicious event" is too broad,~~. We~~and recommends changing the Cyber Security Incident definition to <<Any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.>>

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

———YES

~~We~~NPCC Participating Members have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

The NPCC Participating Member's response to answer ~~to~~ question 2 is "yes."-

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO

~~We~~NPCC Participating Members have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

~~NPCC strongly believes that~~ CIP-002 is not ready for ballot. ~~We believe i~~It is important that this Standard specify that the Critical Assets to be considered are a subset of the Critical Assets as defined in the Definitions section.

Requirements R1.1.1 to R1.1.9, inclusive, are too prescriptive. This list belongs in a FAQ. ~~We feel that c~~Cyber security personnel should not maintain a list of non-cyber equipment. Perhaps the FAQ should include a statement that <<the Responsible Entity should use a cross-functional team or other methods that are appropriate for that organization>>.

~~We~~NPCC Participating Members suggest the Purpose be altered to

<<
This standard is intended to ensure that appropriate cyber 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.

With the increased use of standard technologies to connect Control Center computer systems to the bulk electrical systems, corporate business systems, and the internet, separation between the critical assets of the bulk electrical system and untrusted infrastructure has been dramatically reduced. This connectivity requires that the Control Center systems put in place a high level of Cyber Security measures to protect the Control Center and bulk electrical system assets.

Business and operational demands for managing and maintaining 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 Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system.

The Critical Cyber Assets are identified by the application of a risk-based assessment procedure on the operation of cyber assets supporting the monitoring and control of the interconnected bulk electric system.
>>

~~We recommend c~~Change~~ing~~ Requirement R4 to <<Member(s) of senior management or designee must approve the list of Critical Assets and the list of Critical Cyber Assets.>>

~~We recommend c~~Change~~ing~~ Measure M5 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Cyber Assets must be maintained.>>

~~We recommend c~~Change~~ing~~ Measure M6 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Cyber Assets must be maintained.>>

Please clarify the performance reset period in Compliance 1.2. What is being reset? Why is it being reset?

Recommend that Compliance 1.2 change from 30 days back to the 90 days specified in 1200.

A general statement that applies to all the Cyber Security Standards is that the Measures, Requirements and Levels of non-Compliance need to be reviewed/revisited to ensure there is consistency. The drafting tem should ensure that with ALL these standards, additional requirements aren't being introduced in the compliance section. A requirement should have a measure and associated levels of non-compliance associated with not meeting it. These levels must be carefully reviewed to identify and prioritize which are really critical to Cyber Security, i.e. documention in some instances is not as critical to the reliability of the Bulk Power System as evaluating incidents. The corresponding levels of non-compliance should individually be reviewed and reflect this.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

~~—~~NO

~~We~~NPCC Participating Members have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

~~NPCC feels~~ CIP-003 needs a little more work before it is ready for ballot. This answer assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot, for more information see the response to the previous question.

NPCC Participating Members~~We~~ do not agree with C.M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets,~~. We~~and it is recommended that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>

Please explain what <<information security protection programs>> C.M5 refers to.

~~We~~ NPCC Participating Members feel~~s~~ that C.M10 is too prescriptive. The Compliance Submittal is signed by an authorized representative of the Responsible Entity. That commits the Entity to that information. If it is later discovered that person did not have authorization, then the Entity did not submit compliance on time, which makes the Responsible Entity non-compliant. This incents Entities to insure the appropriately documented information is submitted on-time.

~~We~~NPCC Participating Members are concerned that C.M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the structure of internal corporate relationships>> too frequently.

~~We~~NPCC Participating Members feel that C.M13.1 and C.M.13.2 are overly prescriptive and should be removed.

Also~~We question~~ how does an organization~~to~~ document continual engagement by executives. If it cannot be document, then it cannot be measured. We recommend removing <<and that executive level management is continually engaged in the process>> from C.M13.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

A general statement that applies to all the Cyber Security Standards is that the Measures, Requirements and Levels of non-Compliance need to be reviewed/revisited to ensure there is consistency. The drafting tem should ensure that with ALL these standards, additional requirements aren't being introduced in the compliance section. A requirement should have a measure and associated levels of non-compliance associated with not meeting it. These levels must be carefully reviewed to identify and prioritize which are really critical to Cyber Security, i.e. documention in some instances is not as critical to the reliability of the Bulk Power System as evaluating incidents. The corresponding levels of non-compliance should individually be reviewed and reflect this.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

~~—~~NO

~~We~~NPCC Participating Members have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

~~NPCC feels~~ CIP-004 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

NPCC Participating Members feel~~s~~ this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.

Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.

Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003.

Measure 4.6 should be modified. The requirement for a regular 5 year update to the security screening is not consistent with Requirement R4, which states that a risk based approach be used. The need for rescreening should be cause only.

Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures.

A general statement that applies to all the Cyber Security Standards is that the Measures, Requirements and Levels of non-Compliance need to be reviewed/revisited to ensure there is consistency. The drafting tem should ensure that with ALL these standards, additional requirements aren't being introduced in the

compliance section. A requirement should have a measure and associated levels of non-compliance associated with not meeting it. These levels must be carefully reviewed to identify and prioritize which are really critical to Cyber Security, i.e. documention in some instances is not as critical to the reliability of the Bulk Power System as evaluating incidents. The corresponding levels of non-compliance should individually be reviewed and reflect this. .

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

~~———~~NO

NPCC Participating Members~~We~~ have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

~~NPCC feels~~ CIP-005 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

NPCC Participating Members request~~s~~ clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.

Requirement R4.2's third bullet is not clear. We recommend changing from
<<
Out of band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication.
>>
to
<<
Out of band authentication procedures to augment static user id and password access. (e.g. Access will not be enabled via static user id and password authentication unless a telephone call is received from the entity requesting access. On receipt of the telephone call and after successful procedural authentication of the calling party, an administrator will enable access allowing the entitiy to utilize their static user id and password.)
>>

~~We believe that~~ Requirement R3 is one of many solution to securing dial-in access. Other solutions are bullet items under Requirement R4.2. We recommend that Requirement R3 become another bullet item under Requirement R4.2.

A general statement that applies to all the Cyber Security Standards is that the Measures, Requirements and Levels of non-Compliance need to be reviewed/revisited to ensure there is consistency. The drafting tem should ensure that with ALL these standards, additional requirements aren't being introduced in the compliance section. A requirement should have a measure and associated levels of non-compliance associated with not meeting it. These levels must be carefully reviewed to identify and prioritize which

are really critical to Cyber Security, i.e. documention in some instances is not as critical to the reliability of the Bulk Power System as evaluating incidents. The corresponding levels of non-compliance should individually be reviewed and reflect this.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO

NPCC Participating Members~~We~~ have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

~~NPCC feels~~ CIP-006 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

The term "nearest six-wall boundary" is used in the Purpose. This term confuses some people. We recommend using <<bounded by the nearest walls, floor and ceiling>> instead.

Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2.

Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.

Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement.

Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.

Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Measure M4 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.

A general statement that applies to all the Cyber Security Standards is that the Measures, Requirements and Levels of non-Compliance need to be reviewed/revisited to ensure there is consistency. The drafting tem should ensure that with ALL these standards, additional requirements aren't being introduced in the compliance section. A requirement should have a measure and associated levels of non-compliance associated with not meeting it. These levels must be carefully reviewed to identify and prioritize which are really critical to Cyber Security, i.e. documention in some instances is not as critical to the reliability of the Bulk Power System as evaluating incidents. The corresponding levels of non-compliance should individually be reviewed and reflect this.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO

NPCC Participating Members~~We~~ have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

~~NPCC feels~~ CIP-007 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Requirement R1 assumes that every Responsible Entity has a test system and test unit for every device. We do not agree that assumption. We do not agree that every patch on every device needs to be tested. If the same patch is applied to the same device, then it needs to be tested once. If the vendor approves the patch and the Responsible Entity applies that patch to all those devices, then the Responsible Entity has secured those devices for this standard. The main source of these objections is the last paragraph in this requirement. We recommend deleting that paragraph. We recommend changing the second sentence in the previous paragraph from
<<
Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment.>>
to
<<
Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment, where available.>>
We like the phrase <<as possible given the technical capability of the Critical Cyber Asset>> in Requirement R6.3. Perhaps this phrase should be used in a revised Requirement R1.

Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006.

Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.

Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.

Requirement R3.6 should be modified. The second sentence repeats the first, as such it is necessary and may confuse some.

Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>.

Requirement R4.1 is too prescriptive and should be deleted.

The <<monthly review>> in Requirement R4.2 is too presciptive. We recommend changing R4.2 from
<<
The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.
>>
to
<<
The Responsible Entity shall perform a routine review of the security patches available for each Critical Cyber Asset. Formal processes shall be used to document their implementation or the reason for not installing the patch.
>>

Add <<where technically feasible>> to the end of Requirement R4.3.

Requirement R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means.

Requirement R5.3 allows exception to R5.1. As such, these Requirements should be combined, otherwise one could be non-compliant with R5.1 and fully compliant with R5.3 while the intent appears to be full compliance with R5.1 and R5.3.

The combined requirement should allow technically feasible alternative solutions.

Change Requirement R5.2 from
<<
The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.
>>
to
<<
Where integrity software is deemed to be technically implementable and has been implemented, the Responsible Entity shall perform a monthly review of the integrity software to ensure that the release level of the integrity software is functionally effective and maintainable for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.

>>

~~We~~NPCC Participating Members do not agree with <<site-specific installation>> in Requirement 5.4. and~~We~~ recommend changing from
<<
Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of malware.
>>
to
<<
Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each software deployment in order to prevent manual dissemination of malware.
>>

Change Requirement R6.1 from
<<
The Responsible Entity shall perform a vulnerability assessment at least annually that includes:
>>
to
<<
The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes:
>>

Change Requirement 6.1.3 from
<<
Factory default accounts
>>
to
<<
Scanning for factory default accounts
>>

Change Requirement 6.1.4 from
<<
Security patches and anti-virus version levels
>>
to
<<
Assessing security patches and/or anti-virus version levels, as appropriate
>>

The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assesssment schedule than an attended facility?

The title of Requirement R7 is too broad. We recommend changing this title from
<<Retention of System Logs>>
to

<<Retention of Appropriate System Logs>>
The last sentence of this requirement says the Responsible Entity determines its logging strategy. We believe this means the Responsible Entity decides which are the appropriate system logs to retain.

Requirement R9 should clarify that it pertains to ports inside the perimeter. Requirement R2 of CIP-005 covers ports at the perimeter.

The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.

Requirement R11 belongs in CIP-009. This requirement should be moved to that standard. This requirement references Critical Assets. That is not correct. It should a requirement for the backup and recovery of Critical Cyber Assets. The requirement starts with <<on a regular basis>>, and the third sentence says <<at least annually>>. The requirement should stipulate one or the other. We recommend removing <<annually>>. The last sentence is unclear and should be deleted.

Change Measure M2. The semi-annual audit is too prescriptive. This requirements recognizes that the frequency of password changes should be determined by risk assessment.

<<where applicable>> should added to the end of Measure 4.3.

Change the Measures M5.1 - M5.3 from
<<
M5.1 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.
M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found.
M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities.
>>
to
<<
M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments.
M5.2 The documentation shall include a record of the results of the annual vulnerability assessment.
M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions.
>>

Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the perimeter.

Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.

Which Requirement and Measurement is Compliance 2.1 associated with?

Compliance 2.2.1.1 needs to be changed so that it is consistent with changes to the corresponding Requirement(s) and Measure(s). This compliance is restricted to <<inside the perimeter>>. There should be no stated difference in the time frames for attended and unattended facilities.

Clarify if Compliance 2.3 should be read as [2.3.1 or 2.3.2 or 2.3.3 (etc)] OR [2.3.1 and 2.3.2 and 2.3.3 (etc)]. We suggest that all of these standards include a statement regarding compliance levels with multiple items.

A general statement that applies to all the Cyber Security Standards is that the Measures, Requirements and Levels of non-Compliance need to be reviewed/revisited to ensure there is consistency. The drafting tem should ensure that with ALL these standards, additional requirements aren't being introduced in the compliance section. A requirement should have a measure and associated levels of non-compliance associated with not meeting it. These levels must be carefully reviewed to identify and prioritize which are really critical to Cyber Security, i.e. documention in some instances is not as critical to the reliability of the Bulk Power System as evaluating incidents. The corresponding levels of non-compliance should individually be reviewed and reflect this.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO

~~We~~NPCC Participating Members have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

~~NPCC feels~~ CIP-008 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from
<<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>>
to
<<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>>

Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3.

The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows
<<
The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.
>>

Compliance 1.4 stipulates a requirement that is not in the second posting. We recommend creating a Requirement R2 as follows

<<
R2. The Responsible Entity shall keep all records related to each Cyber Security Incident for three calendar years. This includes, where appropriate, but is not limited to the following:
R2.1 System and application log file entries,
R2.2 Appropriate physical access records,
R2.3 Documented records of investigations and analysis performed, as available,
R2.4 Records of any action taken including any recovery actions initiated.
R2.5 Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.
>>

These changes call for a different Measure M2. <<The Responsible Entity shall retain records for each Cyber Security Incident for three calendar years.>>

~~We~~NPCC Participating Members recommend changing Compliance 1.2 from
<<
The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance reset period shall be one (1) calendar year.
>>
to
<<
The compliance monitoring period shall keep be three (3) calendar years. The performance reset period shall be one (1) calendar year.
>>

~~We recommend c~~Change~~ing~~ Compliance 1.3 from
<<
The Responsible Entity shall keep documents specified in this standard for three calendar years.
>>
to
<<
The Responsible Entity shall keep all data specified in this standard for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.
>>

~~We recommend c~~Change~~ing~~ Compliance 2.1.1 from
<<
Documentation exists, but has not been updated with known changes with 90 calendar days.
>>
to
<<
Documentation necessary to demonstrate compliance with Measure M1 exists, but has not been updated within 90 calendar days of known changes.
>>

~~We recommend c~~Change~~ing~~ Compliance 2.2.1 from
<<
Incident response documentation exists, but has not been updated or reviewed within the last 12 months
>>
to
<<

Cyber Security Incident Response Plan documentation exists, but has not been updated or reviewed within the last 12 months
>>

~~We recommend c~~Change~~ing~~ Compliance 2.2.2 from
<<
Incident response documentation exists but is incomplete
>>
to
<<
Cyber Security Incident Response Plan documentation exists but is incomplete
>>

~~We request c~~Clarification is requested on the threshold for Compliance 2.3.2.

Change Compliance 2.4 from
<<
No documentation exists
>>
to
<<
2.4.1 Cyber Security Incident Response Plan documentation does not exist
2.4.2 Cyber Security Incidents have occurred and none were reported to the ES-ISAC
>>

A general statement that applies to all the Cyber Security Standards is that the Measures, Requirements and Levels of non-Compliance need to be reviewed/revisited to ensure there is consistency. The drafting tem should ensure that with ALL these standards, additional requirements aren't being introduced in the compliance section. A requirement should have a measure and associated levels of non-compliance associated with not meeting it. These levels must be carefully reviewed to identify and prioritize which are really critical to Cyber Security, i.e. documention in some instances is not as critical to the reliability of the Bulk Power System as evaluating incidents. The corresponding levels of non-compliance should individually be reviewed and reflect this.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO

NPCC Participating Members~~We~~ have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

~~NPCC feels~~ CIP-009 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

~~We are not sure~~It is unclear how broad this standard is. If this is the Recovery Plans of Critical Cyber Assets from Cyber Security Incidents, then the following comments apply.

Requirements R1 and R2 should be swapped. We recommend changing the first requirement from
<<
The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan.
>>
to
<<
The Responsibel Entity shall specify the appropriate response to Cyber Security Incidents of varying duration and severity that would require the activation of a Critical Cyber Asset Recovery Plan.
>>
Furthermore, we recommend changing the second requirement from
<<
The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan at least annually.
>>
to
<<
The Responsible Entity shall create recovery plan(s) for those events and assets indentified in R1 and exercise its recovery plan(s) as defined by its risk based assessment.
>>

~~We believe that~~ Requirement R3 appears to have~~has~~ the right intention, but its wording is too broad. ~~We recommend c~~Change~~ing~~ from

<<
The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.
>>
to
<<
The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan(s).
>>

Requirement R5 is covered in CIP-004. R5 should be deleted.

~~We believe that~~ Measures M2 and M3 are duplicates. ~~We recommend d~~Delete~~ing~~ Measure M2.

Measure M3 corresponds to Requirement R3. ~~We~~ change~~d~~is required for Requirement R3. Measure M3 needs a similar modification from
<<
The Responsible Entity shall review and update recovery plan(s) annually.
>>
to
<<
The Responsible Entity shall review and update recovery plan(s) as prescribed by its risk based assessment.
>>

Since Requirement R5 is deleted, the corresponding Measure M4 should be deleted. This is covered in CIP-004.

Compliance 1.3 restates Measure M1. Compliance 1.3 needs different words or should be deleted.

Compliance 2.1 should be changed from
<<
Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year
>>
to
<<
Recovery plan(s) exist, but have not been reviewed or updated, if necessary, in the last calendar year
>>

As posted, if a Responsible Entity has not reviewed their recovery paln(s) in the last calendar year, they are Level 1 and Level 2 non-compliant. This is confusing. Also, training is covered in CIP-004.
Compliance 2.2 should be changed from
<<
Recovery plan(s) have not been reviewed, exercised or training performed.
>>
to
<<
Recovery plan(s) have not been exercised according to the Responsible Entity's risk based assessment.
>>

Compliance 2.3 includes specific roles and responsibilities that are not in the Requirements or the Measures. It is confusing and inappropriate to introduce new requirements in Compliance. The reference to <<types of events that are necessary>> is confusing. This standard specifies no types of events as <<necessary>>.

A general statement that applies to all the Cyber Security Standards is that the Measures, Requirements and Levels of non-Compliance need to be reviewed/revisited to ensure there is consistency. The drafting tem should ensure that with ALL these standards, additional requirements aren't being introduced in the compliance section. A requirement should have a measure and associated levels of non-compliance associated with not meeting it. These levels must be carefully reviewed to identify and prioritize which are really critical to Cyber Security, i.e. documention in some instances is not as critical to the reliability of the Bulk Power System as evaluating incidents. The corresponding levels of non-compliance should individually be reviewed and reflect this.

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.

~~———~~**NO**

~~We~~**NPCC Participating Members have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.**

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

~~NPCC feels t~~**The Implementation Plan does not allow enough time for compliance. First, these standards have substantial changes from 1200. A Responsible Entity could be compliant with 1200 and require much work before they are compliant with these standards. Secondly, budgets are established months ahead of time. Some Responsible Entities have frozen their 2005 budgets. For either reason. there are enough Entities that will not meet the initial dates for auditable compliance or substantial compliance (first quarter of 2006) . We recommend that the 2006 dates change to 2007 dates, the 2007 dates change to 2008 dates, etc.**

There is~~We are~~ concern~~ed~~ with compliance for substations. Substations are part of the <<Other Facilities>>. Therefore it is~~We~~ recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.

Clarify what dates the compliance submittal is for. Is the first quarter submittal of 2007 for January 1, 2006 to December 31, 2006? Or is the 2007 submittal as of a year ending on the submittal date? Or is the 2007 submittal what the Entity has as of that submittal date?

If the Functional Model is not implemented according to the Functional Model schedule, what is the impact on the Cyber Security Implementation Plan?

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**
☐ **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

Lead Contact: **Karl Tammar**

Contact Organization: **NYISO**

Contact Segment: **2**

Contact Telephone: **518-356-6205**

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**
Peter Henderson	**IESO**		**2**
Peter Brandien	**ISO-NE**		**2**
Bill Phillips	**MISO**		**2**
Karl Tammar	**NYISO**		**2**
Bruce Balmat	**PJM**		**2**
Charles Yeung	**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.

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.

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.

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.

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.

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.

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.

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAC approves Standard 1300 SAR, draft 1 posting (July 1, 2003)

2. SAC approves Standard 1300 SAR, draft 2 posting (December 1, 2003) 3.

SAC appoints Standard 1300 Drafting Team (June 23, 2004) 4. Drafting Team

posts draft 1 for comment (September 15, 2004)

5. Drafting Team posts draft 2 of Standard CIP–002–1 (Draft 1, Std 1300, section 1302) (January 17, 2005)

Description of Current Draft:

The current draft reformats Standard 1300, section 1302 into the new NERC Standards format and is to be posted for a 30-day posting period for public review and comment. This draft includes revisions based on public comments received during the posting of Draft 1.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Review comments to draft 2 and revise as needed	February 17, 2005 –March 15, 2005
2. Post Draft 3 for 45-day public comment period	March 15, 2005– April 30, 2005
3. Post Final Draft for 30-day public review, solicit Ballot Body	June 1–30, 2005
4. First ballot of Standard CIP–002–1	July 1–10, 2005
5. Respond to comments, post for recirculation ballot	July 21–31, 2005
6. 30-day posting before board adoption	August 1–31, 2005
7. Board adopts Standard CIP–002–1	September 1, 2005
8. Effective date	October 1, 2005

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data associated with bulk electric system assets.

Critical Asset: 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.

Cyber 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.

Electronic Security Perimeter: 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.

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.

Critical Cyber Assets: Those Cyber Assets essential to the reliable operation of Critical Assets.

Introduction 1. Title: Cyber Security — Critical Cyber Assets 2. Number: CIP–002–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. Business and operational demands for managing and maintaining 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 Responsible Entities identify and protect critical Cyber Assets that support the reliable operation of the bulk electric system. The Critical Assets are identified by the application of a risk-based assessment procedure on the operation of the interconnected bulk electric system. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service provider 4.5.Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. 5. (Proposed) Effective Date: October 1, 2005 Requirements R1.1. Responsible Entities shall identify their Critical Assets using their preferred risk-based assessment. A list	

of Critical Assets is then the basis to identify a list of associated critical Cyber Assets that must be protected by this standard. R1.2. Critical Assets: The Responsible Entity shall identify its Critical Assets. For the purpose of this standard the list of Critical Assets consists of those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a detrimental impact on the reliability or operability of the electric grid and critical operating functions and tasks affecting the interconnected bulk electric system such as, but not limited to: monitoring and control, load and frequency control, emergency actions, contingency analysis, special protection systems, power plant control, substation control and real-time information exchange. Those Critical Assets include the following: R1.3. Control centers and backup control centers performing the functions of a Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generation Owner, Generation Operator and Load Serving Entities. R1.4. Systems, equipment and facilities critical to operating functions and tasks supporting control centers and backup control centers such as telemetering, monitoring and control, automatic generation control, real-time power system modeling and real-time inter-utility data exchange. R1.5. Transmission substations associated with elements monitored as Interconnection Reliability Operating Limits (IROL) R1.6. Generating resources under control of a common system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. R1.7. Generation control centers having control of generating resources that when summed meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. R1.8. Systems, equipment and facilities critical to System Restoration, including Blackstart generators and substations associated with transmission lines used for initial system restoration. R1.9. Systems, equipment and facilities critical to automatic load shedding under control of a common system capable of load shedding 300 MW or greater. R1.10. Special Protection Systems whose misoperation can negatively affect elements associated with an IROL.	

R1.11. Additional Critical Assets: The Responsible Entity shall utilize a risk-based assessment to identify any additional Critical Assets. The risk-based assessment documentation must include a description of the assessment including the determining criteria and evaluation procedure. R1.12. The Responsible Entity shall identify the critical Cyber Assets associated with each Critical Asset listed in section R1. For the purpose of this standard, Critical Cyber Assets will be limited to those Cyber Assets having the following characteristics: R1.13. The Cyber Asset uses a routable protocol, or R1.14. The Cyber Asset is dial-up accessible. R1.15. Dial-up accessible Critical Cyber Assets which do not use a routable protocol require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter R1.16. Any other Cyber Asset within the same Electronic Security Perimeter as identified Critical Cyber Assets must be protected to ensure the security of the Critical Cyber Assets. R1.17. A member of senior management must approve the list of Critical Assets and the list of Critical Cyber Assets. C. Measures M1. The Responsible Entity shall maintain its approved list of Critical Assets as identified in R1. M2. The Responsible Entity shall maintain documentation depicting the risk-based assessment used to identify its Critical Assets in R1. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure. M3. The Responsible Entity shall maintain its approved list of Critical Cyber Assets as identified under Requirement R2 and all other Cyber Assets as identified under Requirement R3. M4. The Responsible Entity shall review, and as necessary, update the documentation referenced in M1, M2, and M3 at least annually, or within 30 calendar days of the addition of, removal of, or modification to any Critical Asset or critical Cyber Asset. M5. A signed and dated record of the senior management officer's approval of the list of Critical Assets must be maintained. M6. A signed and dated record of the senior management officer's approval of the list of Critical Cyber Assets must be maintained.	

D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe Verify annually that necessary updates were made within 30 calendar days of asset additions, deletions or modifications. The performance-reset period shall be one (1) calendar year. The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. 1.3. Data Retention The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.3.1 Documentation of the approved list of Critical Assets, 1.3.2. Documentation depicting the risk-based methodology used to identify its Critical Assets. The document or set of documents shall include a description of the methodology including the determining criteria and evaluation procedure. 1.3.3. Documentation of approved list of Critical Cyber Assets, and 1.3.4 Documentation of the senior management official's approval of both the Critical Asset list and the critical Cyber Asset list. 1.4 Additional Compliance Information: Not Specified Levels of Non-Compliance Level 1: The required documents exist, but have been updated with known changes within thirty (30) calendar days. Level 2: The required documents exist, but have not been approved, updated or reviewed in the last calendar year. Level 3: One or more document(s) missing. Level 4: No Documents exist. E. Regional Differences 1. None Version History	

Introduction 1. Title: Cyber Security Management controls 2. Number: CIP–003–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. 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. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2.balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. 5. (Proposed) Effective Date: October 1, 2005 B. Requirements R1. 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 controls. R2. The Responsible Entity shall document and implement a program for the protection of critical information associated with Critical Cyber Assets R1. The Responsible Entity shall identify all information, regardless of media type, related to the entities Critical Cyber Assets whose compromise could	

impact the reliability and/or availability of the bulk electric system for which the entity is responsible. This includes 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.	The last sentence in "this" R1 should be deleted as it is redundant.
R2. The Responsible Entity shall categorize information related to Critical Cyber Assets to aid personnel with access to this information in determining what information can be disclosed to unauthorized personnel; as well as the relative sensitivity of information that should not be disclosed outside of the entity without proper authorization. R3. Responsible Entities must identify the information access controls related to Critical Cyber Assets based on classification level as defined by the individual entity. R3. The Responsible Entity shall assign a member of senior management with responsibility for leading and managing the entity's implementation and adherence of the cyber security standard. This person, or their designated delegate, must authorize any deviation or exception from the requirements of this standard. Any such deviation or exception and its authorization must be documented.	The words "from the requirements of this standard" should be replaced by "from the requirements of the NERC CIP series of standards".
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 categorized in Requirement R2 of this standard. R4. 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. This governance process must include: R4. 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 prior to the system being promoted to operate in a production environment.	This sentence is redundant and should be deleted: Roles and responsibilities shall also be defined for the access, use, and handling of critical information as identified and categorized in Requirement R2 of this standard.

R5. 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.	"and ultimately ensure the overall integrity of the Critical Cyber Assets." is superfluous.
R5. The Responsible Entity shall institute and document a process for management of access to information associated with Critical Cyber Assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible.	This instance of R5 is redundant and should be deleted as it is stated in R2.
R6. 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.	
R7. 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.	
R8. Responsible Entities shall define and document procedures to ensure that modification, suspension, or termination of user access to Critical Cyber Assets is accomplished in a time frame that ensures Critical Cyber Assets are not put at significant risk. All access revocations/changes must be authorized and documented.	
C. Measures	
M1. The Responsible Entity shall maintain its written cyber security policy stating the entity's commitment to protect Critical Cyber Assets.	
M2. The Responsible Entity shall review the cyber security policy as often as determined by the entity with a minimum review period not to exceed three years.	
M3. The Responsible Entity shall maintain documentation of any deviations or exemptions authorized by the current senior management official responsible for the cyber security program.	
M4. 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.	
M5. The Responsible Entity shall review the information security protection program at least	Remove sections M5 & M6 because they are scope creep and are covered in M7

annually. M6. The Responsible Entity shall perform an assessment of the information security protection program to ensure compliance with the documented processes at least annually. M7. The Responsible Entity shall document the procedures used to secure the information that has been identified as critical cyber information according to the categorization level assigned to that information. M8. The Responsible Entity shall assess the critical cyber information identification and categorization procedures to ensure compliance with the documented processes at least annually. M9. The Responsible Entity shall maintain in its policy the defined roles and responsibilities for the handling of critical cyber information. M10. The current senior management official responsible for the cyber security program shall be identified by name, title, business phone, business address, and date of designation. M11. Changes to the current senior management official must be documented within 30 calendar days of the effective date. M12. The Responsible Entity shall review the roles and responsibilities of Critical Cyber Asset owners, custodians, and users at least annually. M13. 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. M13.1. The Responsible Entity shall have a defined process that maintains a current list of designated personnel responsible for authorizing systems suitable for the production environment. M13.2. 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. M14. The Responsible Entity shall have a defined process that maintains a current list of designated personnel responsible to authorize access to Critical Cyber Assets to reflect any change in status that affects the designated personnel's ability to authorize access to those Critical Cyber Assets.	Suggest "procedures" in M7 and M8 be changed to "controls". M 10 is too prescriptive. Name, Title and Date of Designation are adequate here. Maintaining the other information is too onerous and does not provide any value. M13.1 is a duplicate of M 12 M13.2 – There is not a requirement for Change Management in this standard. This text should be moved to the requirements section. M14 – This statement is redundant - to reflect any change in status that affects the designated personnel's ability to authorize access to those

M15. The list of designated personnel responsible to authorize access to Critical Cyber Assets shall identify each designated person by name, title, business phone, business address, date of designation, and list of systems/applications they are responsible to authorize access for. The list of authorizers shall be reviewed for accuracy at least annually. M16. 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. M17. The Responsible Entity shall ensure that any authorized change in user access to Critical Cyber Assets is documented. Documentation shall be reviewed at least annually to ensure compliance with entities' documented access control processes. M18. The Responsible Entity shall review user access rights to confirm access is still required at least annually. D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.3.1 Written cyber security policy; 1.3.2 The name, title, business address, and business phone number of the current designated senior management official and the date of his or her designation. 1.3.3 Documentation of justification for any deviations or exemptions. 1.3.4 Documented review results of this standard and mitigation strategies for the information security protection program. Review results will be kept for a minimum of 3 years. 1.3.5 The list of approving authorities for access to critical cyber information assets. 1.3.6 The name(s) of the designated approving authority(s) responsible for authorizing systems suitable	Critical Cyber Assets. M15 – same comment as M10 M17 and M18 should be deleted. This measure duplicates measures 4.1 and 4.2 of CIP 004. 1.3.4 – if this is required, it should be moved to a requirements section.

for production. 1.4. Additional Compliance Information: Not specified 2. Levels of Non Compliance 2.1 Level 1: 2.1.1 A current senior management official was not designated for less than 30 calendar days during a calendar year; or 2.1.2 A written cyber security policy exists but has not been reviewed in the last calendar year, or 2.1.3 Deviations from requirements or written cyber security policy are not documented within 30 calendar days of the deviation, or exception, or 2.1.4 An information security protection program exists but has not been reviewed in the last calendar year, or 2.1.5 Processes to protect information associated with Critical Cyber Assets have not been reviewed in the last calendar year. 2.2. Level 2: 2.2.1 A current senior management official was not designated for 30 or more calendar days, but less than 60 calendar days during a calendar year, or 2.2.2 Access to critical cyber information has not been assessed within the last calendar year, or 2.2.3 An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or 2.2.4 The list of designated personnel responsible to authorize access to critical cyber information has not been kept current and has not been reviewed within the last calendar year. 2.3. Level 3: 2.3.1 A current senior management official was not designated for 60 or more calendar days, but less than 90 calendar days during a calendar year, or 2.3.2 Deviations to policy are not documented or authorized by the current senior management official or delegate responsible for the cyber security program, or 2.3.3 Roles and/or responsibilities are not clearly and distinctly defined, or 2.3.4 Controls for the testing and assessment of new or replacement systems and software patches/changes have not been identified or the list of designated approving authorities is not maintained and up to date. .4. Level 4: 2.4.1 A current senior management official was not designated for more than 90 calendar days during a calendar year; or 2.4.2 No cyber security policy exists, or	

2.4.3 No information security program exists, or 2.4.4 Roles and responsibilities have not been defined, or 2.4.5 Executive management has not been engaged in the cyber security program, or 2.4.6 No corporate governance program exists, or 2.4.7 Access authorizations have not been reviewed within the last calendar year, or 2.4.8 There is no authorizing authority to validate systems that are to be promoted to production, or 2.4.9 The list of designated personnel responsible to authorize access to logical or physical Critical Cyber Assets does not exist or, 2.4.10 Access revocations/changes are not authorized and/or documented. E. Regional Differences 1. None Version History	

Personnel & Training

Introduction 1. Title: Cyber Security — Personnel & Training 2. Number: CIP–004–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. Personnel having authorized 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. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 5.(Proposed) Effective Date: October 1, 2005 B. Requirements Responsible Entity shall comply with the following requirements of this standard R1. Awareness — The Responsible Entity shall	

develop, maintain and document its security awareness program to ensure personnel subject to the standard receive on-going reinforcement in sound security practices. R2. Training — The Responsible Entity shall develop and maintain a company specific cyber security-training program that will be reviewed annually. This program will ensure that all personnel having authorized 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. R3. Records — The Responsible Entity shall prepare and maintain records to document training, awareness reinforcement, and background screening of all personnel having authorized access to Critical Cyber Assets and shall be provided for authorized inspection upon request. R4. Personnel Risk Assessment — The Responsible Entity shall subject all personnel having access to Critical Cyber Assets, including contractors and service vendors, to a documented company personnel risk assessment process prior to being granted authorized access to Critical Assets. C. Measures M1. 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: M1.1 Direct communications (e.g., emails, memos, computer based training, etc.); M1.2 Security reminders (e.g., posters, intranet, brochures, etc.); M1.3 Management support (e.g., presentations, all-hands meetings, etc.). M2. Training — The Responsible Entity shall develop and maintain a company-specific cyber security annual training program that includes, at a minimum, the following required items: M2.1 The cyber security policy; M2.2 Physical and elctronic access controls to Critical Cyber Assets; M2.3 The proper release of Critical Cyber Assetn	

formation; M2.4 Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident. M3. Records — The Responsible Entity shall develop and maintain records to adequately document compliance with this standard. M3.1 The Responsible Entity shall maintain documentation of all personnel who have access to Critical Cyber Assets and the date of completion of their training. M3.2 The Responsible Entity shall maintain documentation that it has reviewed and updated its training program annually. M4. Personnel Risk Assessment — The Responsible Entity shall: M4.1 Maintain a list of all authorized personnel with access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets within the security perimeter(s). M4.2 Review the document referred to in measure M4.1 of this standard quarterly, and update the listing within seven calendar days of any substantive change of personnel. M4.3 Physical and electronic access revocation must be completed within 24 hours for any personnel terminated for cause and seven calendar days for any personnel who have a change in status where they are not allowed access to Critical Cyber Assets (e.g., resignation, suspension, transfer, requiring escorted access, etc.). M4.4 The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel prior to being granted authorized 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 identity verification (e.g., Social Security Number verification in the U.S.) 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. M4.5 The Responsible Entity shall ensure that adverse employment actions are consistent with the Responsible Entity's legal and human resources practices for hiring and retention of employees or	M2.4 – this is a new requirement and there is no matching requirement in this standard. M4.1, 4.2, 4.3 are redundant as they are covered in CIP 003.

contractors. M4.6 The Responsible Entity shall conduct update screenings at least every five years or for cause. D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years, and personnel risk assessment documents for the duration of employee employment. Contractor and service vendor records will be maintained for the duration of their engagement. 1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 Document(s) for compliance, training, awareness and screening; 1.4.2 Records of changes to access authorization lists verifying that changes were made within prescribed time frames; 1.4.3 Supporting documentation (e.g., checklists, access request/authorization documents); 1.4.4 Verification that quarterly and annual security awareness have been conducted; 1.4.5 Verification that personnel risk assessments are being conducted 2. Levels on Non-Compliance 2.1.1 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 2.1.2 One instance of personnel termination (employee, contractor or service provider) in which the access control list was not updated within 24 hours for cause or seven calendar days for other personnel changes; or 2.1.3 Personnel risk assessment program exists, but	M4.6 – this should refer to risk assessment as in R4 rather than screenings.

not properly documented, or 2.1.4 Training program exists, but records of training either do not exist or reveal some key personnel were not trained as required; or 2.1.5 Awareness program exists, but not applied consistently or with the minimum of quarterly reinforcement. 2.2. Level 2: 2.2.1 Access control document(s) exist, but have not been updated or reviewed for more than six months but less than 12 months; or 2.2.2 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 seven calendar days or 24 hours if termination for cause; or 2.2.3 Training program exists, but doesn't not cover one of the specific items identified, or 2.2.4 Awareness program does not exist or is not implemented, or 2.2.5 Personnel risk assessment program exists, but is not consistently applied. 2.3. Level 3: 2.3.1 Access control list exists, but does not include service vendors; and contractors or 2.3.2 More than five instances of personnel termination (employee, contractor or service vendor) in which the access control list was not updated within seven business days or 24 hours if termination for cause; or 2.3.3 A personnel risk assessment program does not exist; or 2.3.4 Training documents exist, but do not cover two or more of the specified items. .4. Level 4: 2.4.1 Access control rights list does not exist; or 2.4.2 No training program exists addressing Critical Cyber Assets E. Regional Defences: None Version History:	2.3.1 – Please include a matching requirement or delete this paragraph.

Introduction 1. Title: Cyber Security — Electronic Security 2. Number: CIP–005–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. 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. Applicability When used in within the text of this standard, “Responsible Entity” shall mean 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities.	

Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1 5. (Proposed) Effective Date: October 1, 2005 B. Requirements	
R1. 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 nonCritical Cyber Assets within the defined Electronic Security Perimeter, these non-Critical Cyber Assets must comply with the requirements of this standard.	R1 – delete the first sentence. Repeating the term Electronic Security Perimeters is redundant. The rest of the paragraph is helpful but should not be contained in a requirements statement. Could be moved to the Electronic Security Perimeter definition or to an FAQ.
R2. Disabling unused Network Ports/Services: The Responsible Entity shall enable only those ports/services required for normal and emergency operations of Critical Cyber Assets. All other ports/services, including those used for testing purposes, must be disabled prior to production usage.	
R3. The Responsible Entity shall secure dial-up modem connections. Where remote activation of dial-up connectivity via SCADA activated relays from the security or control center is technically feasible, dial-up equipment at unattended facilities shall be physically deactivated when not in approved use and remotely activated upon approval of activation. In all other cases, the Responsible Entity shall implement procedural or technical measures to ensure authenticity of the accessing device and/or application.	R3 – attended or unattended is irrelevant to security in this paragraph.
R4. Electronic Access Controls — The Responsible Entity shall implement the organizational, technical and procedural controls to permit or deny logical access at all	

electronic access points to the Electronic Security Perimeter(s) and the Critical Cyber Assets within the Electronic Security Perimeter(s). R4.1. These Electronic Security Perimeter access controls shall implement an access control model, which denies access by default unless explicit access permissions are specified. R4.2. 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. These strong procedural or technical measures shall include at least one of the following measures: Two-factor authentication Digital certificates Out-of-band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication One time use passwords In dial-up access, automatic number identification (ANI) to augment static user id and password authentication In dial-up access, call back to augment static user id and password authentication R4.3. Where technically feasible, electronic access control devices shall display an appropriate use banner upon interactive access attempts. R5. 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. R6. Documentation Review and Maintenance - The Responsible Entity shall ensure that all documentation by this standard reflect current configurations and processes. The entity shall conduct a review of these documents at least every 90 calendar days to ensure accuracy and shall update all documents within 30 calendar days following the implementation of changes. C. Measures M1. Electronic Security Perimeter — The Responsible	R4 – The phrase “and the Critical Cyber Assets within the Electronic Security Perimeter(s).” is confusing given that this standard refers to Electronic Security Perimeter. R4.2 – Did y’all mean “remote access” or really “external interactive logical access”? Please clarify. R4.2 – Suggest that indicating “Strong procedural or technical controls” is all that is required. R4.2 – this is too prescriptive for a standard. Would be better as a guideline because technology changes so rapidly. R4.3 – should be removed. This is not a security measure but a legal support measure. R5 – Monitoring authorized access should be replaced with logging authorized access. R6. We could find no requirements for the creation of any documents in the requirements section of this standard.

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 entity shall ensure that all systems hosting Critical Cyber Assets have been identified and are within the Electronic Security Perimeter(s) documented.	M1 establishes a new requirement to document interconnected critical cyber assets within the security perimeter which is not reflected in the requirements.
M2. Disabling unused Network Ports/Services: The Responsible Entity shall disable unused ports and services, and maintain documentation of status/configuration of all ports and services available on Critical Cyber Assets. M3. Dial-up Modems: M3.1 The Responsible Entity shall maintain a documented policy for securing dial-up modem connections to Critical Cyber Assets, and a record of an annual audit of all dial-up modem connections and ports against the policy and documented configuration. M3.2 The documentation shall verify that the Responsible Entity has taken the appropriate actions to secure dial-up access to all Critical Cyber Assets. M4. Electronic Access Controls M4.1 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). M4.2 For each control, the document or set of documents shall identify and describe, at a minimum, M1.4.2 The access request and authorization process implemented for that control, M2.4.2 The authentication methods used, and M3.4.2 A periodic review process for authorization rights, in accordance with management policies and controls defined in Standard CIP–003–1, and ongoing supporting documentation (e.g. access request and authorization documents, review checklists) verifying that these have been implemented. M5. Monitoring Electronic Access Control — The Responsible Entity shall maintain a document or set of documents to identify and describe: M5.1 Organizational, technical and procedural controls, including tools and procedures, for monitoring electronic (logical) access.	M2, M3.1 and M3.2 establish new requirements which are not covered in the requirements section.
M5.2 Supporting documents, including access records and logs, to verify that the tools and procedures are	M5.2 – this appears to be the same as CIP 007, R 7/M6.

functioning and being used as designed. M5.3 Processes, procedures and technical controls implemented to review 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. Documents that record these reviews shall be identified. M6. Documentation Review and Maintenance: — The Responsible Entity shall review the documents referenced in this standard at least annually and shall update these documents within 30 calendar days of the modification of the network or controls. D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep document revisions and security incident related data (such as unauthorized access reports) for three (3) 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 calendar days. The compliance monitor shall keep audit records for three years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years, and personnel risk assessment documents for the duration of employee employment. Contractor and service vendor records will be maintained for the duration of their engagement. 1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 Document(s) for configuration, processes, tools and procedures as described in this standard; 1.4.2 Records of electronic access to Critical Cyber Assets (e.g. access logs, intrusion detection logs) 1.4.3 Supporting documentation (e.g. checklists, access request/authorization documents) 1.4.4 Verification that necessary updates were made at least annually or within 90 calendar days of a modification 2. Levels of Non-Compliance 2.1 Level 1:	M6 contradicts R6 of this standard. 1.2 there is an inconsistency with CIP 007 R 7.1. 1.4.4 – Not consistent with requirements or measures.

2.1.1 Document(s) exist, but have not been updated with known changes within the 90calendar day period and/or, 2.1.2 Access to any Critical Cyber Asset was unmonitored for a period that does not exceed 24 hours. 2.2. Level 2: 2.2.1 Document(s) exist, but have not been updated or reviewed in the last 12 months and/or, 2.2.2 Monitoring is in place, but a gap in the access records exists for one calendar day or more but for less than seven calendar days. 2.3. Level 3: 2.3.1 Electronic Security Perimeter: Document exists, but no verification that all critical assets are within the perimeter(s) described or, 2.3.2 Disabling Unused Network Ports/Services: Documents(s) exist, but a record of regular audits does not exist. 2.3.3 Electronic Access Controls: 2.3.3.1 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 2.3.3.2 Required documents exist, but records for some transactions are missing. 2.3.4 Electronic Access Monitoring: 2.3.4.1 Access not monitored to any Critical Cyber Asset for one week or more; or 2.3.4.2 Access records reveal access by personnel not approved on the access control list. 2.4. Level 4: 2.4.1 No document or no monitoring of access exists E. Regional Differences 1: None Version History	2.1.2 – This is not a realistic requirement as it deals mainly with the reliability/availability of systems. A better measure would be to verify that the monitoring processes are in place or the failure of a monitoring process was corrected within 24 hours. 2.3.2 – The word audit is a new requirement and has specific connotations. The word regular is un-measurable. A better expression would “record of [time period] validations or assessments”. 2.3.3 – Delete this section because it is not measurable.

A. Introduction

1. Title: Cyber Security — Physical Security 2. Number: CIP–006–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. 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) (nearest six-wall boundary) within which these Cyber Assets reside.	Delete (nearest six-wall boundary) as this is already covered in the definition above or move it to the definition.
4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 5. (Proposed) Effective Date: October 1, 2005 Requirements R1. Security Plan: The Responsible Entity shall document its implementation of the following requirements in its physical security plan. R1.1. The identification of the Physical Security Perimeters(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). R1.2. The implementation of the necessary measures to control access at all access points of these perimeter(s) and the Critical Assets within them. R1.3. Implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the Critical Cyber Assets. R2. 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) following an industry or government, generally accepted, risk assessment procedure. R3. 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. R4. Logging physical access: The Responsible Entity shall implement the technical and procedural mechanisms for logging physical access. R5. Maintenance and testing: The Responsible Entity shall implement a 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.	
R6. Documents for configuration, processes, tools, and procedures: The Responsible Entity shall maintain the specified documentation concerning its implementation of its Physical Security Plan. C. Measures	R6 – Duplicates R1.
M1. Documentation Review and Maintenance: The Responsible Entity shall review and update its physical security plan at least annually or within 90 days of modification to the perimeter or physical security methods.	M1 – 90 days is not found in the requirements section.
M2. 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).	
M3. Physical Access Controls: The Responsible Entity shall implement one or more of the following	M3 – this is too prescriptive and does not respect changing technologies. The words “or

physical access methods: Card Key: A means of electronic access where the access rights of the cardholder 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 Enclosure: A cage/safe/cabinet system that controls physical access to the Critical Cyber Asset (for environments where the nearest six-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 all physical access point through the Physical Security Perimeter. The documentation shall identify and describe, at a minimum, the access request, authorization, and revocation process implemented for that control, and a periodic review process for verifying authorization rights, in accordance with management policies and controls defined in Standard CIP–003–1, and on-going supporting documentation. M4. 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 or point of facility access.	equivalent" would make this section better. The term "Security Officers" is confusing and should be changed to "Security Personnel". M4. This is redundant. These requirements are referred to in R1 and M1.

Alarm Systems	A system that indicates a door or gate has been opened without authorization. These alarms must report back to a central monitoring station. Examples include card key alarm systems, 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 describe processes to review records for unauthorized access. The Responsible Entity shall have a process for creating unauthorized access reports.

M5. 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 or remote verification
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.

M6. Maintenance and testing of physical security systems: 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.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep document revisions and other security event-related data including unauthorized access reports for three calendar years. The Responsible Entity shall keep audit records for 90 days. The compliance monitor shall keep audit records for three years. The performance-reset period shall be one (1) calendar year.	
1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years.	1.3 If the documents referred to are video records, then this is excessive, unless the documents relate to a significant security incident.
1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 The Physical Security Plan 1.4.2 Document(s) for configuration, processes, tools, and procedures as described in this standard. 1.4.3 Records of physical access to Critical Cyber Assets (e.g., manual access logs, automated access logs). 1.4.4 Supporting documentation (e.g., checklists, access request/authorization documents) 1.4.5 Verification that necessary updates were made at least annually or within 90 days of a modification.	
2. Levels of Non-Compliance 2.1. Level 1: 2.1.1 Document(s) exist, but have not been updated or reviewed within the last 90 days and/or 2.1.2 Access control, monitoring and logging exists, but aggregate interruptions in system availability over a calendar year exist for more than seven days, but less than 1 month.	2.1.1 Not consistent with M1.
2.2. Level 2: 2.2.1 Document(s) exist, but have not been updated or reviewed in the last 6 months and/or 2.2.2 Access control, monitoring and logging exists, but aggregate interruptions in system availability over a calendar year exist for more than one month, but less than three months.	2.2.1 Requires more stringent compliance than level 1 compliance.
2.3. Level 3: 2.3.1 Document(s) exist, but have not been updated or reviewed in the last 12 months and/or 2.3.2 Access control, monitoring and logging exists, but aggregate interruptions in system availability	

over a calendar year exist for more than three months. 2.4. Level 4: 2.4.1 No access control, or no monitoring, or no logging of access exists. E. Regional Differences 1. None Version History	

1. Title: Cyber Security — Systems Security Management 2. Number: CIP–007–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. A System Security Management Program is necessary to minimize or prevent the risk of failure or compromise from misuse or malicious cyber activity. 4. Applicability When used within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. While there are significant differences between attended and unattended facilities that contain Critical Cyber Assets, the requirements below will apply to both unless specifically differentiated. R1. Test Procedures — Attended Facilities: The Responsible Entity shall use documented information security test procedures to augment functional test and acceptance procedures for all new systems and significant changes to existing	This standard is a prime example of the need for a technical writer's review of the standards. It is much more prescriptive than the rest and demonstrates the lack of homogeneity across the standards. R1 – Delete. This requirement is well covered in CIP 003, R4 and R5

critical cyber security assets. The Responsible Entity shall ensure that significant changes include but are not limited to security patches, cumulative service packs, new releases, 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 non-production environment. All testing shall be performed in a manner that precludes adversely affecting the production system and operation. The Responsible Entity shall document full detail of the test environment. The Responsible Entity shall verify that all changes to Critical Cyber Assets were successfully tested for known security vulnerabilities prior to being rolled into production, on a controlled non-production system.	
R2. Test Procedures – Unattended Facilities: The Responsible Entity shall not store test documentation, security procedures, and acceptance procedures at an unattended facility but at another secured attended facility. The Responsible Entity shall conduct security test procedures for Critical Cyber Assets at the unattended facility on a controlled non-production environment located at another secure attended facility.	R2 – Delete. This requirement is well covered in CIP 003, R4 and R5
R3. Account and Password Management: The Responsible Entity shall 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 shall establish, implement, and document end user account (administrator, system, and individual) management that include but are not limited to: R3.1. Strong Passwords: In the absence of more sophisticated authentication methods that are stronger than passwords and don't require a password, (e.g., multi-factor access controls, certificates, or bio-metric), the Responsible Entity shall use accounts that have a strong password. For example, a password consisting of a combination of	R3 – use "account management" instead of "establish an account password management program" R3 – "by compromised account passwords" should be struck as unnecessary. R3 – "that include but are not limited to:" should say "that must meet at a minimum:

alpha, numeric, and special characters with a minimum of six characters to the extent allowed by the existing technology. Passwords shall be changed periodically per a risk-based frequency to reduce the risk of password cracking. R3.2. Generic Account Management – Attended: The Responsible Entity shall have a process for managing factory default accounts, e.g., administrator or guest. The process shall include the removal, disabling, or renaming of these accounts where possible. For those accounts that must remain, passwords shall be changed prior to putting any system into service. Where technically supported, individual accounts shall be used (in contrast to a group account). Where individual accounts are not supported, the Responsible Entity shall 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 (automated or manual), and steps for securing the account in the event of staff changes, e.g., change in assignment or exit. R3.3. Generic Account Management – Unattended: For unattended facilities, the Responsible Entity shall ensure the physical access to Cyber Assets by approved users is authorized by a control or security center operator on an instance-by-instance basis. R3.4. Access Reviews – Attended: The Responsible Entity shall ensure a designated approver reviews access to Critical Cyber Assets, e.g., computer and/or network accounts and access R3.5. Access Reviews — Unattended: The Responsible Entity shall maintain and periodically review records of approved physical access and the cyber related work performed on Cyber Assets at unattended facilities. R3.6. Acceptable Use: The Responsible Entity shall have a policy implemented to manage the scope R3.5. Access Reviews — Unattended: The Responsible Entity shall maintain and periodically review records of approved physical access and the cyber related work performed on Cyber Assets at unattended facilities. R3.6. Acceptable Use: The Responsible Entity shall	R3.3 is covered in CIP 006 R3.4 and R3.5 is covered by CIP 003, 005 and 006.

have a policy implemented to manage the scope and acceptable use of the administrator and other generic account privileges for both attended and unattended facilities. The policy shall support a compliance 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.	
R4. Security Patch Management: The Responsible Entity shall establish a formal security patch management program for tracking, evaluating, testing, and installation of applicable security patches and upgrades to critical cyber security assets.	R 4 – "critical cyber security assets." Security should be deleted.
R4.1. The Responsible Entity shall evaluate all patches and upgrades for applicability to the individual situation, e.g. using a risk based assessment, so as to avoid un-necessary and excessive patching.	R4.1 – Should read "all relevant patches"
R4.2. The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.	R4.2 & R4.3 – this requirement is too prescriptive. A better requirement would be for the company to have a patch management policy and procedure based on its own environment.
R4.3. In the case where installation of the patch is not possible, the Responsible Entity shall use and document a compensating measure(s).	
R5. Integrity Software	
R5.1. The Responsible Entity shall use Integrity Software on all Critical Cyber Assets that are connected to a wide-area network, the Internet, or to another device that is connected to a network (e.g., printer), to prevent, limit, and/or mitigate the introduction, exposure and distribution of malicious software (malware) to other Cyber Assets within the Electronic Security Perimeter.	R5.1 – This section is unclear and would be better if written as follows: "The Responsible Entity shall use means to monitor and protect the integrity of data including software associated with critical cyber assets e.g.: technology, processes/procedures, software." to prevent, limit, and/or mitigate the introduction, exposure and distribution of malicious software (malware) to other Cyber Assets within the Electronic Security Perimeter.
R5.2. The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the Integrity Software implementation and upgrades.	R5.2 - Suggest it be deleted. Covered elsewhere.

R5.3. In the case where integrity software is not used, e.g., operational incompatibility or not available for a particular computer platform, the Responsible Entity shall use and document a compensating measure(s). R5.4. Where repetitious application of software updates are necessary, such as at unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of mal-ware. R6. Identification of Vulnerabilities and Responses R6.1. The Responsible Entity shall perform a vulnerability assessment at least annually that includes: R6.1.1. A diagnostic review of the access points to the Electronic Security Perimeter R6.1.2. Scanning for open ports/services and modems R6.1.3. Factory default accounts R6.1.4. Security patch and anti-virus version levels R6.2. The Responsible Entity shall implement a documented management action plan to remediate vulnerabilities and shortcomings, if any, identified in the assessment. R6.3. For unattended facilities that contain Critical Cyber Assets, the Responsible Entity shall perform a limited vulnerability assessment prior to each upgrade as possible given the technical capability of the Cyber Assets. R7. Retention of Systems Logs: Using monitoring systems and/or procedures either internal and/or external to Critical Cyber Assets, the Responsible Entity shall ensure it is possible to create an audit trail from logs of security-related events affecting the Critical Cyber Assets. The Responsible Entity must determine its own logging strategy to fulfill the requirement. R7.1. The Responsible Entity shall retain said log data for a period of ninety (90) calendar 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) calendar years in an exportable format, for possible use in further event analysis. R7.2. In lieu of automatically generated logs at unattended facilities, the Responsible Entity shall	R5.4 – Where remote installation of software updates is required, the responsible entity shall ensure the integrity of the software being installed prior to initiating remote installation in order to prevent annual dissemination of malware. R7 – The last sentence gives the entities the responsibility to determine their own logging strategy but R7.1 and R7.2 are contrary and prescriptive and should be deleted.

collect and retain the physical access and change records of users at each approved access session, or at a minimum annually. R8. Change Control and Configuration Management R8.1. 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 shall include change management procedures that at a minimum provide testing, modification audit trails, problem identification, a back out and recovery process shall modifications fail, and ultimately ensure the overall integrity of the Critical Cyber Assets. R8.2. The Responsible Entity shall ensure the controlled development or test environment for Cyber Assets residing in unattended facilities are not at the unattended facility. The Change Control Process for Cyber Assets at unattended facilities shall prevent the inadvertent dissemination of faulty or compromised software to multiple unattended sites.	R8 – Should be deleted as it is well covered in CIP 003.
R9. Disabling Unused Host Ports/Services: The Responsible Entity shall enable only those ports/services required for normal and emergency operations of Critical Cyber Assets. All other ports/services, including those used for testing purposes, must be disabled prior to production usage. R10. Operating Status Monitoring Tools: For maintaining situational awareness, the Responsible Entity shall ensure Critical Cyber Assets used for operating critical infrastructure are included or augmented with automated and/or process tools, where practical, to monitor operating state, utilization and performance, and cyber security events experienced by the Critical Cyber Assets themselves, and issue alarms for specified indications, as implemented. For Critical Cyber Assets in use at unattended facilities that are not capable of being electronically monitored remotely, the Responsible Entity shall review and document pertinent metrics manually during routine access/service to said equipment	R9 – Should be deleted as it is well covered in CIP 005.
R11. Back up and Recovery: The Responsible	R11 – The last sentence “For unattended

Entity shall back up on a regular basis, where technically feasible, information and data that is resident or required by Cyber Assets used to manage critical electric infrastructure. The back up must be stored in a remote or hardened site some distance away from the Critical Cyber Assets. Information stored on computer media for a prolonged period of time shall be tested at least annually to ensure that the information is recoverable. For unattended facilities, back-up and recovery materials can be effectively tested at central test facility and shall not be tested on site. C. Measures M1. Test Procedures: For all Critical Cyber Assets, the Responsible Entity shall maintain records of test procedures, results, and acceptance of successful completion.	facilities, back-up and recovery materials can be effectively tested at central test facility and shall not be tested on site." should be removed and the rest of this section moved to CIP 009.
M2. Account and Password Management: The Responsible Entity shall maintain a documented password policy and record of semi-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. Review access permissions within 24 hours for any personnel terminated for cause and seven calendar days for any personnel who have a change in status where they are not allowed access to Critical Cyber Assets (e.g., resignation, suspension, transfer, requiring escorted access, etc.).	M2. – Remove "record of semi-annual audit of this policy" as is contrary to R3.1
M3. 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, approval for installation, compensating measures, and installation date. M4. Integrity Software: The Responsible Entity's change control documentation shall include a record of all integrity software installations including: M4.1 Version level actively in use M4.2 Installation date M4.3 Or provide documentation for other compensating measures taken M5. Identification of Vulnerabilities and Responses: M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical and procedural controls, including tools	M3 - The reference to change control is dealt with in CIP 003

and procedures for monitoring the critical cyber environment for vulnerabilities. M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found. M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities. M6. Retention of Logs: M6.1 The Responsible Entity shall maintain documentation that indexes location, content, and retention schedule of all log data captured from the Critical Cyber Assets. M6.2 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. M7. Change Control and Configuration Management M7.1 The Responsible Entity shall maintain documentation identifying the controls, including tools and procedures, for managing change to and testing of Critical Cyber Assets. M7.2 The documentation shall verify that all the Responsible Entity follows a methodical approach for managing change to their Critical Cyber Assets. M8. Disabling Unused Host Ports/Services: The Responsible Entity shall disable unused ports and services, and maintain documentation of status/configuration of all ports and services available on Critical Cyber Assets. M9. Operating Status Monitoring Tools: The Responsible Entity shall maintain documentation identifying organizational, technical, and procedural controls, including tools and procedures for monitoring operating state, utilization, and performance of Critical Cyber Assets. M10. Back-up and Recovery: M10.1 The Responsible Entity shall maintain documentation that index location, content, and retention schedule of all Critical Cyber Assets' information backup data and tapes. M10.2 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.	Please align measurements and to requirements. M10.1. Replace backup data and tapes with backup media.

M10.3 The documentation shall verify that the Responsible Entity is capable of recovering from the failure or compromise of Critical Cyber Asset. D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years. 1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 Document(s) for configuration, processes, tools and procedures as described in this standard. 1.4.2 System log files as described in measure M6. 1.4.3 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.). 2. Levels of Non-Compliance 2.1. Level 1: Document(s) exist, but does not cover up to two of the specific items identified and/or the document has not been reviewed or updated in the last 12 months. 2.2. Level 2: Document(s) exist, but does not have three of the specific items identified and/or 2.2.1 A gap in the reviews for the following items exists: 2.2.1.1 Access Reviews (semi-annually for attended facilities, periodically for unattended facilities). 2.2.1.2 Security Patch Management (monthly) 2.2.1.3 Integrity Software (monthly) 2.2.2 Retention of system logs exists, but a gap of greater than three days but less than seven days exists. 2.3. Level 3: 2.3.1 Document(s) exist, but more than three of the	

items specified are not covered. 2.3.2 Test Procedures: Document(s) exist, but documentation verifying that changes to Critical Cyber Assets tested is incomplete or changes to Critical Cyber Assets were not tested. 2.3.3 Account and Password Management: Document(s) exist, but documentation verifying accounts and passwords comply with the policy does not exist. 2.3.4 Security Patch Management: Document exists, but records of security patch installations are incomplete. 2.3.5 Integrity Software: Documentation exists, but verification that all Critical Cyber Assets are being kept up to date on anti-virus software or that compensating measures are being taken does not exist. 2.3.6 Identification of Vulnerabilities and Responses: 2.3.6.1 Document exists, but annual vulnerability assessment was not completed and/or 2.3.6.2 Documentation verifying that the entity is taking appropriate actions to remediate potential vulnerabilities does not exist. 2.3.7 Retention of Logs (operator, application, intrusion detection): A gap in the logs of greater than 7 days exists. 2.3.8 Disabling Unused Host Ports/Services: Documents(s) exist, but a record of regular audits does not exist. 2.3.9 Change Control and Configuration Management: N/A 2.3.10 Operating Status Monitoring Tools: N/A 2.3.11 Backup and Recovery: Document exists, but record of annual restoration verification exercise does not exist. 2.4. Level 4: No Documentation exists E. Regional Differences 1. None Version History	

1. Title: Cyber Security — Incident Response Planning 2. Number: CIP–008–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. Security measures designed to protect Critical Cyber Assets from intrusion, disruption or other forms of compromise must be monitored on a continuous basis. This standard requires responsible entities to define the procedures that must be followed when Cyber Security Incidents are identified. This standard requires: Developing and maintaining of documented procedures, Classification of incidents, Actions to be taken, and Reporting of Incident. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard.	The references to "incidents" should say cyber security incidents.

(Proposed Effective Date: October 1, 2005 . Requirements R1. The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate and/or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items: R2. Incident Classification: The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents. R3. Cyber Security 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. R4. Cyber Security Incident Reporting: The Responsible Entity shall report all Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center ES ISAC in accordance with the Indications, Analysis & Warning Program (IAW) Standard Operating Procedure (SOP). The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. C. Measures M1. The Responsible Entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and Cyber Security Incident reporting requirements at least annually or within 90 calendar days of known changes M2. The Responsible Entity shall retain records in addition to requirements defined in Standard CIP-007-1, requirement R7 (Retention of Systems Logs) of Cyber Security Incidents for three calendar years. D. Compliance 1. Compliance Monitoring Process	

1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years. 1.4. Additional Compliance Information 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: 1.4.1 System and application log file entrie 1.4.2 Video, and/or physical access records, 1.4.3 Documented records of investigations and analysis performed, 1.4.4 Records of any action taken including any recovery actions initiated. 1.4.5 Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC. 2. Levels of Non-Compliance 2.1.Level 1 2.1.1 Documentation exists, but has not been updated with known changes within 90 calendar days. 2.2. Level 2: 2.2.1 Incident response documentation exists, but has not been updated or reviewed in the last 12 months and/or 2.2.2 Records related to Cyber Security Incidents are not maintained for three years or are incomplete. 2.3. Level 3: 2.3.1 Incident response documentation exists but is incomplete and/or 2.3.2 Cyber Security Incidents have occurred but were not reported to the ES ISAC 2.4. Level 4: No documentation exists. E. Regional Differences 1. None Version History	

1. Title:Cyber Security — Recovery Plans 2. Number: CIP–009–1 Purpose: This standard is intended to ensure that appropriate cyber 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. 3. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 3.1. Reliability Coordinator 3.2. Balancing Authority 3.3. Interchange Authority 3.4.Transmission Service Provider 3.5.Transmission Owner 3.6. Transmission Operator 3.7. Generator Owner 3.8. Generator Operator 3.9. Load Serving Entity 3.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP-002-1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. (Proposed) Effective Date: October 1, 2005 Requirements	
R1. The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan(s) at least annually. R2. The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan. R3. The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that effects the protection of Critical Cyber Assets R4. Recovery plan(s) and any updates or changes shall be communicated to personnel responsible for their operation or responsibility for such Critical Cyber Asset within seven (7) calendar	R1. Overly prescriptive. The minimum test frequency schedule should be based on a risk-based assessment and evidence kept that this testing frequency is respected.

days of development or modification. R5. The Responsible Entity shall develop training and awareness for its recovery plan(s) that follow the requirements set forth in Standard CIP–004–1 — Personnel and Training.	
C. Measures M1. The Responsible Entity shall document its Recovery Plan(s) and maintain records of all exercises or drills for at least three (3) years. M2. The Responsible Entity shall document its Recovery Plan(s) and maintain records of all exercises or drills for at least three (3) years.	M1 and M2 should be merged.
M3. The Responsible Entity shall review and update if needed, its response to events of varying duration and severity annually or as necessary.	M3 and M4 are repetitive and should be merged.
M4. The Responsible Entity shall review and update recovery plan(s) annually.	M4 contradicts R3.
M5. The Responsible Entity shall conduct drills at least every three (3) years and keep attendance records to its Recovery Plan(s) training	M5 is not consistent with R1 and needs to be clarified.
D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall make the documents described in this standard available for inspection by the compliance monitor upon request. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years. 1.4 Additional Compliance Information: Not Specified	
2. Levels of Non-Compliance 2.1 Level 1: Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year. 2.2 Level 2: Recovery plan(s) have not been reviewed, exercised, or training performed. 2.3 Level 3: Recovery plan(s) address neither the type of events that are necessary nor	2. This compliance section will not work and should be revisited. For example, a plan that has not been reviewed will contradict both level 1 and level 2. Entity which neither updates its recovery plan in the past year, nor exercised nor included in it the types of “events that are necessary” could legitimately claim any of level 1, 2 or 3

any specific roles and responsibilities. 2.4. Level 4L No recovery plan(s) exists. E. Regional Differences: None	noncompliance. Level 3 identifies a new requirement that should be identified in the requirements or measures section.

February 16th 2005

ISO/RTO Council General comments to NERC CIP Draft Standards 002-009

The standard still looks inconsistent in a number of areas:

a) Some of the measures and requirements language seems to be similar both in the same section of the standards and across the standards.
b) The numbering is still inconsistent.
c) 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.

The time periods prescribed throughout are still inconsistent across the CIP 002 to 009 standards.

If an entity is found not to have properly identified its critical infrastructure in 002, will this mean being scored as non-compliant in the other remaining standards?

The standard 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 exists 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.

Most references to unattended facilities do not seem to bear relevance on security measures to critical cyber assets and should be reviewed.

NERC needs to ensure that the level of non-compliance is commensurate to the violation's impact to reliability rather than merely being an administrative violation.

ISO/RTO Council Comments on the

Implementation Plan
for Cyber Security Standards
CIP-002-1 through CIP-009-1

2/16/05

The intent of the proposed NERC cyber security standard is to ensure that all entities responsible for the reliability of the bulk electric systems of North America identify and protect critical cyber assets that control or could impact the reliability of the bulk electric systems. This implementation plan is based on the following assumptions; Cyber Security Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP006-1, CIP-007-1, CIP-008-1, and CIP-009-1 are approved by the ballot body and the NERC Board of Trustees no later than September 1, 2005. The NERC Functional Model is implemented in concert with the passage of the Version 0 standards. Entities have registered to the NERC Functional Model. Cyber Security Standards CIP-002-1 through CIP-009-1 become effective October 1, 2005. To provide time for responsible entities to examine their policies and procedures, to assemble the necessary documentation, and to meet the requirements of these standards, compliance assessment will begin starting in 2006. Implementation Schedule Beginning with the first quarter of 2006, NERC and its Regions will develop self-certification forms as part of their compliance and enforcement programs. The Regions will distribute these forms to the	The following is the position of the ISO/RTO Council Members: Since the standard will not become official before October 1, 2005, it is not realistic to expect an acceptable level of auditable compliance in Q1 2006. • NERC CIP 002-009 is much deeper and wider than NERC 1200 and will require a significant compliance effort. • 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 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. Change 2006 to 2007 (and successive columns) and change from auditably to substantially compliant. A good requirement would be to require a corporate implementation plan for compliance 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.

applicable functional entities within their respective Regions. Regions may ask other entities to provide self-certification forms if they believe they are performing one of the functions identified in the standard. In such cases, the completion of a self-certification form by those other entities will be voluntary. All applicable entities will complete and submit the appropriate Regional self-certification forms, indicating their compliance, or degree of non-compliance, to the requirements of these standards. These self-certification forms will be submitted to the appropriate NERC Regional Reliability Council, which will hold the individual responses as confidential. It will be the responsibility of the Regional Compliance Manager to summarize the results of the self-certification and provide that summary to the NERC Compliance Program. Responsibility for compliance with these standards remains with the "Responsible Entity". The following table identifies when entities must be Auditably Compliant (AC) or Substantially Compliant (SC) with a requirement. Auditably Compliant means the entity meets the full intent of the requirement and can prove compliance to an auditor. The intent of the proposed NERC cyber security standard is to ensure that all entities responsible for the reliability of the bulk electric systems of North America identify and protect critical cyber assets that control or could impact the reliability of the bulk electric systems. This implementation plan is based on the following assumptions; Cyber Security Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP006-1, CIP-007-1, CIP-008-1, and CIP-009-1 are approved by the ballot body and the NERC	Recommendation: The entity must identify the dates when the document retention processes must begin to be compliant with the standard.

Board of Trustees no later than September 1, 2005. The NERC Functional Model is implemented in concert with the passage of the Version 0 standards. Entities have registered to the NERC Functional Model. Cyber Security Standards CIP-002-1 through CIP-009-1 become effective October 1, 2005. To provide time for responsible entities to examine their policies and procedures, to assemble the necessary documentation, and to meet the requirements of these standards, compliance assessment will begin starting in 2006. Implementation Schedule Beginning with the first quarter of 2006, NERC and its Regions will develop self-certification forms as part of their compliance and enforcement programs. The Regions will distribute these forms to the applicable functional entities within their respective Regions. Regions may ask` other entities to provide self-certification forms if they believe they are performing one of the functions identified in the standard. In such cases, the completion of a self-certification form by those other entities will be voluntary. All applicable entities will complete and submit the appropriate Regional self-certification forms, indicating their compliance, or degree of non-compliance, to the requirements of these standards. These self-certification forms will be submitted to the appropriate NERC Regional Reliability Council, which will hold the individual responses as confidential. It will be the responsibility of the Regional Compliance Manager to summarize the results of the self-certification and provide that summary to the NERC Compliance Program. Responsibility for compliance with these	

standards remains with the “Responsible Entity”. The following table identifies when entities must be Auditably Compliant (AC) or Substantially Compliant (SC) with a requirement. Auditably Compliant means the entity meets the full intent of the requirement and can prove compliance to an auditor. Substantially Compliant means an entity has begun the process to become compliant with a requirement, but is not yet Auditably Compliant. The table has two sections for each standard. The first section defines the implementation schedule for Balancing Authorities (BA) and Reliability Coordinators (RC). The second section defines the implementation schedule for Interchange Authorities (IA), Transmission Providers (TP), Transmission Owners (TO), Transmission Operators (TOP), Generation Owners (GO), Generation Operators (GOP) and Load Serving Entities (LSE).	

Compliance Schedule for Standards CIP-002-1 through CIP-009-1

	1st Qtr		1st Qtr 2007		2008 & Beyond	
Requi	Contr	Other Facilit	Control	Other Facilit	Control	Other Facilities
Standard CIP-002-1 – Critical Cyber Assets BA & RC						
FAC		SC	AC	AC	AC	AC
FAC		SC	AC	AC	AC	AC
FAC		SC	AC	AC	AC	AC
FAC		SC	AC	AC	AC	AC
Standard CIP-002-1 – Critical Cyber Assets IA, TP, TO, TOP, GO, GOP, LSE						
FSC		SC	AC	AC	AC	AC
FSC		SC	AC	AC	AC	AC
FSC		SC	AC	AC	AC	AC
FSC		SC	AC	AC	AC	AC
Standard CIP-003-1 – Security Management Controls						
FAC		SC	AC	AC	AC	AC

FAC	SC	AC	AC	AC	AC
FAC	SC	AC	AC	AC	AC
FAC	SC	AC	AC	AC	AC
FAC	SC	AC	AC	AC	AC
Standard CIP-003-1 – Security Management Controls					
FSC	SC	AC	AC	AC	AC
FSC	SC	AC	AC	AC	AC
FSC	SC	AC	AC	AC	AC
FSC	SC	AC	AC	AC	AC
FSC	SC	AC	AC	AC	AC
Standard CIP-004-1 – Personnel & Training BA & RC					
FAC	SC	AC	AC	AC	AC
FAC	SC	AC	AC	AC	AC
FAC	SC	AC	AC	AC	AC

	1st Qtr 2006		1st Qtr 2007		2008 & Beyond	
Requirement	Control	Other Facilities	Control	Other Facilities	Control	Other Facilities
R4	SC	SC	SC	SC	AC	AC
Standard CIP-004-1 – Personnel & Training IA, TP, TO, TOP, GO, GOP, LSE						
R1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	SC	SC	AC	AC
Standard CIP-005-1 – Electronic Security BA & RC						
R1	AC	SC	AC	AC	AC	AC
R2	AC	SC	AC	AC	AC	AC
R3	AC	SC	AC	AC	AC	AC
R4	AC	SC	AC	AC	AC	AC
R5	AC	SC	AC	AC	AC	AC
R6	AC	SC	AC	AC	AC	AC
Standard CIP-005-1 – Electronic Security IA, TP, TO, TOP, GO, GOP, LSE						
R1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	AC	AC	AC	AC
R5	SC	SC	AC	AC	AC	AC
R6	SC	SC	AC	AC	AC	AC
Standard CIP-006-1 – Physical Security BA & RC						
R1	AC	SC	AC	AC	AC	AC
R2	AC	SC	AC	AC	AC	AC
R3	AC	SC	AC	AC	AC	AC
R4	AC	SC	AC	AC	AC	AC
R5	AC	SC	AC	AC	AC	AC
R6	AC	SC	AC	AC	AC	AC
Standard CIP-006-1 – Physical Security IA, TP, TO, TOP, GO, GOP, LSE						
R1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	AC	AC	AC	AC
R5	SC	SC	AC	AC	AC	AC
R6	SC	SC	AC	AC	AC	AC
Standard CIP-007-1 – Systems Security Management						

	1st Qtr 2006		1st Qtr 2007		2008 & Beyond	
COMM	Control	Other Facilit	Control	Other Facilit	Control	Other Facilit
R4	AC	SC	AC	AC	AC	AC
R5	AC	SC	AC	AC	AC	AC
Standard CIP-009-1 – Recovery Plans IA, TP, TO, TOP, GO, GOP, LSE						
1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	AC	AC	AC	AC
R5	SC	SC	AC	AC	AC	AC

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:	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.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NPCC feels that there are many incidents have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>.

We are concerned that "suspicious event" is too broad. We recommend changing the Cyber Security Incident definition to <<Any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.>>

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NPCC strongly believes that CIP-002 is not ready for ballot. We believe it is important that this Standard specify that the Critical Assets to be considered are a subset of the Critical Assets as defined in the Definitions section.

Requirements R1.1.1 to R1.1.9, inclusive, are too prescriptive. This list belongs in a FAQ. We feel that cyber security personnel should not maintain a list of non-cyber equipment. Perhaps the FAQ should include a statement that <<the Responsible Entity should use a cross-functional team or other methods that are appropriate for that organization>>.

We suggest the Purpose be altered to

<<
This standard is intended to ensure that appropriate cyber 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.

With the increased use of standard technologies to connect Control Center computer systems to the bulk electrical systems, corporate business systems, and the internet, separation between the critical assets of the bulk electrical system and untrusted infrastructure has been dramatically reduced. This connectivity requires that the Control Center systems put in place a high level of Cyber Security measures to protect the Control Center and bulk electrical system assets.

Business and operational demands for managing and maintaining 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 Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system.

The Critical Cyber Assets are identified by the application of a risk-based assessment procedure on the operation of cyber assets supporting the monitoring and control of the interconnected bulk electric system.
>>

We recommend changing Requirement R4 to <<Member(s) of senior management or designee must approve the list of Critical Assets and the list of Critical Cyber Assets.>>

We recommend changing Measure M5 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Cyber Assets must be maintained.>>

We recommend changing Measure M6 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Cyber Assets must be maintained.>>

Please clarify the performance reset period in Compliance 1.2. What is being reset? Why is it being reset?

Recommend that Compliance 1.2 change from 30 days back to the 90 days specified in 1200.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NPCC feels CIP-003 needs a little more work before it is ready for ballot. This answer assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot, for more information see the response to the previous question.

We do not agree with C.M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets. We recommend that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>

Please explain what <<information security protection programs>> C.M5 refers to.

We feels that C.M10 is too prescriptive. The Compliance Submittal is signed by an authorized representative of the Responsible Entity. That commits the Entity to that information. If it is later discovered that person did not have authorization, then the Entity did not submit compliance on time, which makes the Responsible Entity non-compliant. This incents Entities to insure the appropriately documented information is submitted on-time.

We are concerned that C.M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the structure of internal corporate relationships>> too frequently.

We feel that C.M13.1 and C.M.13.2 are overly prescriptive and should be removed.

We question how to document continual engagement by executives. If it cannot be document, then it cannot be measured. We recommend removing <<and that executive level management is continually engaged in the process>> from C.M13.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NPCC feels CIP-004 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

NPCC feels this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.

Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.

Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003.

Measure 4.6 should be modified. The requirement for a regular 5 year update to the security screening is not consistent with Requirement R4, which states that a risk based approach be used. The need for rescreening should be cause only.

Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NPCC feels CIP-005 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

NPCC requests clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.

Requirement R4.2's third bullet is not clear. We recommend changing from

<<

Out of band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication.

>>

to

<<

Out of band authentication procedures to augment static user id and password access. (e.g. Access will not be enabled via static user id and password authentication unless a telephone call is received from the entity requesting access. On receipt of the telephone call and after successful procedural authentication of the calling party, an administrator will enable access allowing the entitiy to utilize their static user id and password.)

>>

We believe that Requirement R3 is one of many solution to securing dial-in access. Other solutions are bullet items under Requirement R4.2. We recommend that Requirement R3 become another bullet item under Requirement R4.2.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NPCC feels CIP-006 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

The term "nearest six-wall boundary" is used in the Purpose. This term confuses some people. We recommend using <<bounded by the nearest walls, floor and ceiling>> instead.

Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2.

Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.

Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement.

Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.

Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Measure M4 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should

be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NPCC feels CIP-007 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Requirement R1 assumes that every Responsible Entity has a test system and test unit for every device. We do not agree that assumption. We do not agree that every patch on every device needs to be tested. If the same patch is applied to the same device, then it needs to be tested once. If the vendor approves the patch and the Responsible Entity applies that patch to all those devices, then the Responsible Entity has secured those devices for this standard. The main source of these objections is the last paragraph in this requirement. We recommend deleting that paragraph. We recommend changing the second sentence in the previous paragraph from
<<
Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment.>>
to
<<
Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment, where available.>>
We like the phrase <<as possible given the technical capability of the Critical Cyber Asset>> in Requirement R6.3. Perhaps this phrase should be used in a revised Requirement R1.

Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006.

Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.

Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.

Requirement R3.6 should be modified. The second sentence repeats the first, as such it is necessary and may confuse some.

Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>.

Requirement R4.1 is too prescriptive and should be deleted.

The <<monthly review>> in Requirement R4.2 is too presciptive. We recommend changing R4.2 from
<<

The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.
>>
to
<<
The Responsible Entity shall perform a routine review of the security patches available for each Critical Cyber Asset. Formal processes shall be used to document their implementation or the reason for not installing the patch.
>>

Add <<where technically feasible>> to the end of Requirement R4.3.

Requirement R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means.

Requirement R5.3 allows exception to R5.1. As such, these Requirements should be combined, otherwise one could be non-compliant with R5.1 and fully compliant with R5.3 while the intent appears to be full compliance with R5.1 and R5.3.

The combined requirement should allow technically feasible alternative solutions.

Change Requirement R5.2 from
<<
The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.
>>
to
<<
Where integrity software is deemed to be technically implementable and has been implemented, the Responsible Entity shall perform a monthly review of the integrity software to ensure that the release level of the integrity software is functionally effective and maintainable for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.
>>

We do not agree with <<site-specific installation>> in Requirement 5.4. We recommend changing from
<<
Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of malware.
>>
to
<<
Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each software deployment in order to prevent manual dissemination of malware.

>>

Change Requirement R6.1 from
<<
The Responsible Entity shall perform a vulnerability assessment at least annually that includes:
>>
to
<<
The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes:
>>

Change Requirement 6.1.3 from
<<
Factory default accounts
>>
to
<<
Scanning for factory default accounts
>>

Change Requirement 6.1.4 from
<<
Security patches and anti-virus version levels
>>
to
<<
Assessing security patches and/or anti-virus version levels, as appropriate
>>

The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assesssment schedule than an attended facility?

The title of Requirement R7 is too broad. We recommend changing this title from
<<Retention of System Logs>>
to
<<Retention of Appropriate System Logs>>
The last sentence of this requirement says the Responsible Entity determines its logging strategy. We believe this means the Responsible Entity decides which are the appropriate system logs to retain.

Requirement R9 should clarify that it pertains to ports inside the perimeter. Requirement R2 of CIP-005 covers ports at the perimeter.

The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.

Requirement R11 belongs in CIP-009. This requirement should be moved to that standard. This requirement references Critical Assets. That is not correct. It should a requirement for the backup and recovery of Critical Cyber Assets. The requirement starts with <<on a regular basis>>, and the

third sentence says <<at least annually>>. The requirement should stipulate one or the other. We recommend removing <<annually>>. The last sentence is unclear and should be deleted.

Change Measure M2. The semi-annual audit is too prescriptive. This requirements recognizes that the frequency of password changes should be determined by risk assessment.

<<where applicable>> should added to the end of Measure 4.3.

Change the Measures M5.1 - M5.3 from
<<
M5.1 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.
M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found.
M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities.
>>
to
<<
M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments.
M5.2 The documentation shall include a record of the results of the annual vulnerability assessment.
M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions.
>>

Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the perimeter.

Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.

Which Requirement and Measurement is Compliance 2.1 associated with?

Compliance 2.2.1.1 needs to be changed so that it is consistent with changes to the corresponding Requirement(s) and Measure(s). This compliance is restricted to <<inside the perimeter>>. There should be no stated difference in the time frames for attended and unattended facilities.

Clarify if Compliance 2.3 should be read as [2.3.1 or 2.3.2 or 2.3.3 (etc)] OR [2.3.1 and 2.3.2 and 2.3.3 (etc)]. We suggest that all of these standards include a statement regarding compliance levels with multiple items.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NPCC feels CIP-008 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from
<<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>>
to
<<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>>

Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3.

The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows
<<
The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.
>>

Compliance 1.4 stipulates a requirement that is not in the second posting. We recommend creating a Requirement R2 as follows
<<
R2. The Responsible Entity shall keep all records related to each Cyber Security Incident for three calendar years. This includes, where appropriate, but is not limited to the following:
R2.1 System and application log file entries,
R2.2 Appropriate physical access records,
R2.3 Documented records of investigations and analysis performed, as available,
R2.4 Records of any action taken including any recovery actions initiated.
R2.5 Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.
>>

These changes call for a different Measure M2. <<The Responsible Entity shall retain records for each Cyber Security Incident for three calendar years.>>

We recommend changing Compliance 1.2 from
<<

The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance reset period shall be one (1) calendar year.
>>
to
<<
The compliance monitoring period shall keep be three (3) calendar years. The performance reset period shall be one (1) calendar year.
>>

We recommend changing Compliance 1.3 from
<<
The Responsible Entity shall keep documents specified in this standard for three calendar years.
>>
to
<<
The Responsible Entity shall keep all data specified in this standard for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.
>>

We recommend changing Compliance 2.1.1 from
<<
Documentation exists, but has not been updated with known changes with 90 calendar days.
>>
to
<<
Documentation necessary to demonstrate compliance with Measure M1 exists, but has not been updated within 90 calendar days of known changes.
>>

We recommend changing Compliance 2.2.1 from
<<
Incident response documentation exists, but has not been updated or reviewed within the last 12 months
>>
to
<<
Cyber Security Incident Response Plan documentation exists, but has not been updated or reviewed within the last 12 months
>>

We recommend changing Compliance 2.2.2 from
<<
Incident response documentation exists but is incomplete
>>
to
<<
Cyber Security Incident Response Plan documentation exists but is incomplete
>>

We request clarification on the threshold for Compliance 2.3.2.

Change Compliance 2.4 from
<<
No documentation exists
>>
to
<<
2.4.1 Cyber Security Incident Response Plan documentation does not exist
2.4.2 Cyber Security Incidents have occurred and none were reported to the ES-ISAC
>>

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

NPCC feels CIP-009 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

We are not sure how broad this standard is. If this is the Recovery Plans of Critical Cyber Assets from Cyber Security Incidents, then the following comments apply.

Requirements R1 and R2 should be swapped. We recommend changing the first requirement from
<<
The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan.
>>
to
<<
The Responsibel Entity shall specify the appropriate response to Cyber Security Incidents of varying duration and severity that would require the activation of a Critical Cyber Asset Recovery Plan.
>>
Furthermore, we recommend changing the second requirement from
<<
The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan at least annually.
>>
to
<<
The Responsible Entity shall create recovery plan(s) for those events and assets indentified in R1 and exercise its recovery plan(s) as defined by its risk based assessment.
>>

We believe that Requirement R3 has the right intention, but its wording is too broad. We recommend changing from

<<
The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.
>>
to
<<
The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan(s).
>>

Requirement R5 is covered in CIP-004. R5 should be deleted.

We believe that Measures M2 and M3 are duplicates. We recommend deleting Measure M2.

Measure M3 corresponds to Requirement R3. We changed Requirement R3. Measure M3 needs a similar modification from
<<
The Responsible Entity shall review and update recovery plan(s) annually.
>>
to
<<
The Responsible Entity shall review and update recovery plan(s) as prescribed by its risk based assessment.
>>

Since Requirement R5 is deleted, the corresponding Measure M4 should be deleted. This is covered in CIP-004.

Compliance 1.3 restates Measure M1. Compliance 1.3 needs different words or should be deleted.

Compliance 2.1 should be changed from
<<
Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year
>>
to
<<
Recovery plan(s) exist, but have not been reviewed or updated, if necessary, in the last calendar year
>>

As posted, if a Responsible Entity has not reviewed their recovery paln(s) in the last calendar year, they are Level 1 and Level 2 non-compliant. This is confusing. Also, training is covered in CIP-004. Compliance 2.2 should be changed from
<<
Recovery plan(s) have not been reviewed, exercised or training performed.
>>
to
<<
Recovery plan(s) have not been exercised according to the Responsible Entity's risk based assessment.
>>

Compliance 2.3 includes specific roles and responsibilities that are not in the Requirements or the Measures. It is confusing and inappropriate to introduce new requirements in Compliance. The reference to <<types of events that are necessary>> is confusing. This standard specifies no types of events as <<necessary>>.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

RGE concurs with NPCC that the Implementation Plan does not allow enough time for compliance. First, these standards have substantial changes from 1200. A Responsible Entity could be compliant with 1200 and require much work before they are compliant with these standards. Secondly, budgets are established months ahead of time. Some Responsible Entities have frozen their 2005 budgets. For either reason. there are enough Entities that will not meet the initial dates for auditable compliance or substantial compliance (first quarter of 2006) .

In fact most entities 2006 budgets will be submitted and approved prior to the final approval and implementation of these standards . At a minimum we recommend that the 2006 dates change to 2007 dates, the 2007 dates change to 2008 dates, etc. A more practical and efficient approach would be for RC and BA to follow the 1200 requirements for 2006, then the BA and RC would be required to be substantially compliant in 2007 and auditably compliant in 2008. All other Responsible Entities would be required to meet the 1200 standards in 2007, substantially compliant in 2008 and auditably compliant in 2009.

We are concerned with compliance for substations. Substations are part of the <<Other Facilities>>. We recommend the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.

Clarify what dates the compliance submittal is for. Is the first quarter submittal of 2007 for January 1, 2006 to December 31, 2006? Or is the 2007 submittal as of a year ending on the submittal date? Or is the 2007 submittal what the Entity has as of that submittal date?

If the Functional Model is not implemented according to the Functional Model schedule, what is the impact on the Cyber Security Implementation Plan?

In the definitions: the terms such as: significant impact, large quantities of customers and extended periods time should be better defined.

Comments on Critical Standard CIP–002

Standard CIP–002–1 — Cyber Security — Critical Cyber Assets

R1.1. Responsible Entities shall identify their Critical Assets using their preferred risk-based assessment. A list of Critical Assets is then the basis to identify a list of associated critical Cyber Assets that must be protected by this standard.

M2. The Responsible Entity shall maintain documentation depicting the risk-based to identify its Critical Assets in R1. The documentation shall include a description methodology including the determining criteria and evaluation procedure.

Need more definition on risk based assessment. What are the minimum elements this should include. I appreciate the flexibility of giving the responsible entity some flexibility here, but I'm also struggling with what this needs to be included in a risk assessment.

R1.6. Generating resources under control of a common system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization.

R1.7. Generation control centers having control of generating resources that when summed meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization.

Better define Regional Reliability Organization

Does the 80% criteria mean the single largest generating unit within SERC? Those entities without large generators would not be affected by this requirement?

R1.13. The Cyber Asset uses a routable protocol, or

Further define routable protocol (i.e. IP address?)

Standard CIP–003–1 — Cyber Security — Security Management Controls

R4. 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. This governance process must include:

In many cases, these systems will be purchased/installed from vendors. This requirement needs to make provisions for those systems. Responsible Entities should ensure all purchased software systems are adequately tested to secure its Critical Cyber Assets.

Standard CIP–004–1 — Cyber Security — Personnel & Training

No comment

Standard CIP–005–1 — Cyber Security — Electronic Security

No comment

Standard CIP–006–1 — Cyber Security — Physical Security

No comments, an overall note. This standard addresses physical security as it applies to cyber assets. For generation facilities, this is a small piece of the puzzle. Our security plans address physical security as it applies to all critical assets. We would apply the same philosophy for physical security to a DCS room as a water intake structure. Unless I'm misinterpreting this section of the regulations, it does not preclude this approach.

Standard CIP–007–1 — Cyber Security —Systems Security Management

R4.1. The Responsible Entity shall evaluate all patches and upgrades for applicability to the individual situation, e.g. using a risk based assessment, so as to avoid un-necessary and excessive patching.

Need to allow for validation by the software developer. In most cases, this software on many of these systems are proprietary and the impact of a patch is unknown to the purchaser. Need to make provisions for verification from the vendor.

R11. Back up and Recovery: The Responsible Entity shall back up on a regular basis, where technically feasible, information and data that is resident or required by Cyber Assets used to manage critical electric infrastructure. The back up must be stored in a remote or hardened site some distance away from the Critical Cyber Assets. Information stored on computer media for a prolonged period of time **shall be tested at least annually to ensure that the information is recoverable**. For unattended facilities, back-up and recovery materials can be effectively tested at central test facility and shall not be tested on site.

Could you change the requirement from "annually" to "periodically". I can see where this may create more problems than it solves. Let the Responsible Entity document and justify his reasoning for choosing the period based on support for the system and criticality. The method of verification should also be documented. For example in an operational environment, there may be not system available to do a system restore without putting a critical system at risk. It may be that the media is shipped to the vendor's site for restoration on a test environment. Results could be documented and filed.

Standard CIP–008–1 — Cyber Security — Incident Reporting and Response Planning

No comments

Standard CIP–009–1 — Cyber Security — Recovery Plans

No comments

Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1

Putting these requirements in place will pose a significant challenge at plants given the number of critical systems. Recommend the following changes:

Standard CIP–005–1 — Cyber Security — Electronic Security
Standard CIP–006–1 — Cyber Security — Physical Security
Standard CIP–007–1 — Cyber Security —Systems Security Management

Substantially Compliant 1st Quarter 07, Auditably Compliant 1st Quarter 08

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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:	**Mr. Dennis Kalma**		
Organization:	**Alberta Electric System Operator (AESO)**		
Telephone:	**403-539-2584**		
Email:	**dennis.kalma@aeso.ca**		
	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		

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Please see attached comment form.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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 comment form.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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 comment form.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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 comment form.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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 comment form.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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 comment form.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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 comment form.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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 comment form.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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 comment form.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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 comment form.

Standard Development Roadmap

Yhis section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1 . SAC approves Standard 1300 SAR, draft 1 posting (July 1, 2003)
2. SAC approves Standard 1300 SAR, draft 2 posting (December 1, 2003)
3. SAC appoints Standard 1300 Drafting Team (June 23, 2004)
4. Drafting Team posts draft 1 for comment (September 15, 2004)
S. Drafting Team posts draft 2 of Standard CIP-002-1 (Draft 1, Std 1300, section 1302) (January 17, 2005)

Description of Current Draft:

The current draft reformats Standard 1300, section 1302 into the new NERC Standards format and is to be posted for a 30-day posting period for public review and comment. This draft includes revisions based on public comments received during the posting of Draft 1.

Future Development Plan:

	Anticipated Actions	**Anticipated Date**
1.	Review comments to draft 2 and revise as needed	February 17, 2005 -March 15, 2005
2.	Post Draft 3 for 45-day public comment period	March 15, 2005- April 30,2005
3.	Post Final Draft for 30-day public review, solicit Ballot Body	June 1-30,2005
4.	First ballot of Standard CIP--002-1	July 1-10, 2005
5.	Respond to comments, post for recirculation ballot	July 21-31, 2005
6.	30-day posting before board adoption	August 1-31, 2005
7.	Board adopts Standard CIP-002-1	September 1, 2005
8.	Effective date	October 1, 2005

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Termsalready defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removedfrom the individual standard and added to the Glossary.

Cyber Assets: Thos ' e programmable electronic devices and communication networks including hardware, software, and data associated with bulk electric system assets.

Critical Asset: 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.

Cyber 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.

Electronic Security Perimeter: 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.

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.

Critical Cyber Assets: Those Cyber Assets essential to the reliable operation of Critical Assets.

Critical Cyber Assets

1. Title: Cyber Security - Critical Cyber Assets 2. Number: CIP-002-1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. Business and operational demands for managing and maintaining 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 Responsible Entities identify and protect critical Cyber Assets that support the reliable operation of the bulk electric system. The Critical Assets are identified by the application of a risk-based assessment procedure on the operation of the interconnected bulk electric system. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities.	Should be a reference that these standards should be read as a group – e.g.: See also CIP002-009

5. (Proposed) Effective Date: October 1, 2005 B. Requirements R1.1. Responsible Entities shall identify their Critical Assets using their preferred risk-based assessment. A list of Critical Assets is then the basis to identify a list of associated critical Cyber Assets that must be protected by this standard. R1.2. Critical Assets: The Responsible Entity shall identify its Critical Assets. For the purpose of this standard the list of Critical Assets consists of those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a detrimental impact on the reliability or operability of the electric grid and critical operating functions and tasks affecting the interconnected bulk electric system such as, but not limited to: monitoring and control, load and frequency control, emergency actions, contingency analysis, special protection systems, power plant control, substation control and real-time information exchange. Those Critical Assets include the following: R1.3. Control centers and backup control centers performing the functions of a Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generation Owner, Generation Operator and Load Serving Entities. R1.4. Systems, equipment and facilities critical to operating functions and tasks supporting control centers and backup control centers such as telemetering, monitoring and control, automatic generation control, real-time power system modeling and real-time inter-utility data exchange. R1.5. Transmission substations associated with elements monitored as Interconnection Reliability Operating Limits (IROL) R1.6. Generating resources under control of a common system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. R1.7. Generation control centers having control of generating resources that when summed meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. R1.8. Systems, equipment and facilities critical to System Restoration, including Blackstart generators and substations associated with transmission lines used for initial system restoration. R1.9. Systems, equipment and facilities critical to automatic load shedding under control of a common	

system capable of load shedding 300 MW or greater. R1.10. Special Protection Systems whose misoperation can negatively affect elements associated with an IROL. R1.11. Additional Critical Assets: The Responsible Entity shall utilize a risk-based assessment to identify any additional Critical Assets. The risk-based assessment documentation must include a description of the assessment including the determining criteria and evaluation procedure. R1.12. The Responsible Entity shall identify the critical Cyber Assets associated with each Critical Asset listed in section Rl. For the purpose of this standard, Critical Cyber Assets will be limited to those Cyber Assets having the following characteristics: R1.13. The Cyber Asset uses a routable protocol, or R1.14. The Cyber Asset is dial-up accessible. R1.15. Dial-up accessible Critical Cyber Assets which do not use a routable protocol require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter R1.16. Any other Cyber Asset within the same Electronic Security Perimeter as identified Critical Cyber Assets must be protected to ensure the security of the Critical Cyber Assets. R1.17. A member of senior management must approve the list of Critical Assets and the list of Critical Cyber Assets. C. Measures M1. The Responsible Entity shall maintain its approved list of Critical Assets as identified in RI. - M2. The Responsible Entity shall maintain documentation depicting the risk-based assessment used to identify its Critical Assets in Rl. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure. M3. The Responsible Entity shall maintain its approved list of Critical Cyber Assets as identified under Requirement R2 and all other Cyber Assets as identified under Requirement R3. M4. The Responsible Entity shall review, and as necessary, update the documentation referenced in MI, M2, and M3 at least annually, or within 30 calendar days of the addition of, removal of, or modification to any Critical Asset or critical Cyber Asset. M5. A signed and dated record of the senior	If there are no assets, the entity must maintain a document outlining the process which must be reviewed annually.

management officer's approval of the list of Critical Assets must be maintained. M6. A signed and dated record of the senior management officer's approval of the list of Critical Cyber Assets must be maintained D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe Verify annually that necessary updates were made within 30 calendar days of asset additions, deletions or modifications. The performance-reset period shall be one (1) calendar year. The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. 1.3. Data Retention The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.3.1 Documentation of the approved list of Critical Assets, 1.3.2 Documentation depicting the risk-based assessment methodology used to identify its Critical Assets. The document or set of documents shall include a description of the methodology including the determining criteria and evaluation procedure, 1.3.3 Documentation of the approved list of Critical Cyber Assets, and 1.3.4 Documentation of the senior management official's approval of both the Critical Asset list and the critical Cyber Asset list. 1.4. Additional Compliance Information Not specified 2. Levels of Non-Compliance 2.1. Level 1: The required documents exist, but have not been updated with known changes within thirty (30) calendar days 2.2. Level 2: The required documents exist, but have not been approved, updated or reviewed in the last calendar year. 2.3. Level 3: One or more document(s) missing.	If there are no critical cyber assets, the entity must still name a senior officer and do an annual review. i.e.: must have a program in place regardless of owning critical cyber assets.

2.4. Level 4: No document(s) exist. E. Regional Differences 1. None Version History	

Security Management Controls

1. Title: Cyber Security - Security Management Controls 2. Number: CIP-003-1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. 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. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP-002-1. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP-002-1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. 5. (Proposed) Effective Date: October 1, 2005 B. Requirements R1. 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 controls. R2. The Responsible Entity shall document and implement a program for the protection of critical information associated with Critical Cyber Assets RI. The Responsible Entity shall identify all information, regardless of media type, related to the entities Critical Cyber Assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible. This includes 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. R2. The Responsible Entity shall categorize information related to Critical Cyber Assets to aid personnel with access to this information in determining what information can be disclosed to unauthorized personnel; as well as the relative sensitivity of information that should not be disclosed outside of the entity without proper authorization. R3. Responsible Entities must identify the information access controls related to Critical Cyber Assets based on classification level as defined by the individual entity. R3. The Responsible Entity shall assign a member of senior management with responsibility for leading and managing the entity's implementation and adherence of the cyber security standard. This person, or their designated delegate, 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 categorized in Requirement R2 of this standard. R4. Responsible Entities shall define and document a structure of relationships and decisionmaking processes that identify and represent executive level management's ability to direct and control the entity in order to secure its Critical Cyber Assets. This governance process must include: R4. 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 prior to the system being promoted to operate in a production environment. R5. 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. R5. The Responsible Entity shall institute and document a process for management of access to information associated with Critical Cyber Assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible. R6. 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. R7. 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. R8. Responsible Entities shall define and document procedures to ensure that modification, suspension, or termination of user access to Critical Cyber Assets is accomplished in a time frame that ensures Critical Cyber Assets are not put at significant risk. All access revocations/changes must be authorized and documented. 1.	It is not clear how compliance would be measured for this requirement – what is significant risk? 2. Does it matter who in the company authorizes revocations and changes? 3. Is this authority "delegatable" during absences of the authorized person? Is it local company policy that applies?
C. Measures M1. The Responsible Entity shall maintain its written cyber security policy stating the entity's commitment to protect Critical Cyber Assets. M2. The Responsible Entity shall review the cyber security policy as often as determined by the entity with a minimum review period not to exceed three years. M3. The Responsible Entity shall maintain documentation of any deviations or exemptions authorized by the current senior management official responsible for the cyber security program. M4. 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. M5. The Responsible Entity shall review the information security protection program at least annually. M6. The Responsible Entity shall perform an assessment of the information security protection program to ensure compliance with the documented processes at least annually. M7. The Responsible Entity shall document the procedures used to secure the information that has been identified as critical cyber information according to the categorization level assigned to that information. M8. The Responsible Entity shall assess the critical cyber	

information identification and categorization procedures to ensure compliance with the documented processes at least annually. M9. The Responsible Entity shall maintain in its policy the defined roles and responsibilities for the handling of critical cyber information. M10. The current senior management official responsible for the cyber security program shall be identified by name, title, business phone, business address, and date of designation. M11. Changes to the current senior management official must be documented within 30 calendar days of the effective date. M12. The Responsible Entity shall review the roles and responsibilities of Critical Cyber Asset owners, custodians, and users at least annually. M13. 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. These measures would be more effective if they aligned in numbering with the requirements. E.g.: R 8 – M 8.0, M 8.1, etc. R1. The Responsible Entity shall have a defined process that maintains a current list of designated personnel responsible for authorizing systems suitable for the production environment. R2. 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. M14. The Responsible Entity shall have a defined process that maintains a current list of designated personnel responsible to authorize access to Critical Cyber Assets to reflect any change in status that affects the designated personnel's ability to authorize access to those Critical Cyber Assets. M15. The list of designated personnel responsible to authorize access to Critical Cyber Assets shall identify each designated person by name, title, business phone, business address, date of designation, and list of systems/applications they are responsible to authorize access for. The list of authorizers shall be reviewed for accuracy at least annually. M16. 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. M17. The Responsible Entity shall ensure that any authorized change in user access to Critical Cyber Assets is documented. Documentation shall be reviewed at least annually to ensure compliance with entities' documented access control processes. M18. The Responsible Entity shall review user access rights to confirm access is still required at least annually. D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.3.1 Written cyber security policy; 1.3.2 The name, title, business address, and business phone number of the current designated senior management official and the date of his or her designation. 1.3.3 Documentation of justification for any deviations or exemptions. 1.3.4 Documented review results of this standard and mitigation strategies for the information security protection program. Review results will be kept for a minimum of 3 years. 1.3.5 The list of approving authorities for access to critical cyber information assets. 1.3.6 The name(s) of the designated approving authority(s) responsible for authorizing systems suitable for production. 1.4. Additional Compliance Information Not specified 2. Levels of Non-Compliance 2.1. Level 1:	

2.1.1 A current senior management official was not designated for less than 30 calendar days during a calendar year; or 2.1.2 A written cyber security policy exists but has not been reviewed in the last calendar year, or 2.1.3 Deviations from requirements or written cyber security policy are not documented within 30 calendar days of the deviation, or exception, or 2.1.4 An information security protection program exists but has not been reviewed in the last calendar year, or 2.1.5 Processes to protect information associated with Critical Cyber Assets have not been reviewed in the last calendar year. 2.2. Level 2: 2.2.1 A current senior management official was not designated for 30 or more calendar days, but less than 60 calendar days during a calendar year, or 2.2.2 Access to critical cyber information has not been assessed within the last calendar year, or 2.2.3 An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or 2.2.4 The list of designated personnel responsible to authorize access to critical cyber information has not been kept current and has not been reviewed within the last calendar year. 2.3. Level 3: 2.3.1 A current senior management official was not designated for 60 or more calendar days, but less than 90 calendar days during a calendar year, or 2.3.2 Deviations to policy are not documented or authorized by the current senior management official or delegate responsible for the cyber security program, or 2.3.3 Roles and/or responsibilities are not clearly and distinctly defined, or Controls for the testing and assessment of new or replacement systems and software patches/changes have not been identified or the list of designated approving authorities is not maintained and up to date. 2.4. Level 4: 2.4.1 A current senior management official was not designated for more than 90 calendar days during a calendar year; or 2.4.2 No cyber security policy exists, or	

2.4.3 No information security program exists, or 2.4.4 Roles and responsibilities have not been defined, or 2.4.5 Executive management has not been engaged in the cyber security program, or 2.4.6 No corporate governance program exists, or 2.4.7 Access authorizations have not been reviewed within the last calendar year, or 2.4.8 There is no authorizing authority to validate systems that are to be promoted to production, or 2.4.9 The list of designated personnel responsible to authorize access to logical or physical Critical Cyber Assets does not exist or, 2.4.10 Access revocations/changes are not authorized and/or documented. E. Regional Differences 1. None Version History	

Personnel & Training

A. Introduction 1. Title: Cyber Security - Personnel & Training 2. Number: CIP-004-1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. Personnel having authorized 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. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP-002-1. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP-002-1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP-002-1. 5. (Proposed) Effective Date: October 1, 2005 B. Requirements Responsible Entity shall comply with the following requirements of this standard: R1. Awareness - The Responsible Entity shall develop, maintain and document its security awareness program to ensure personnel subject to the standard receive on-going reinforcement in sound security practices. R2. Training - The Responsible Entity shall develop and maintain a company specific cyber security-training program that will be reviewed annually. This program will ensure that all personnel having authorized 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.	

R3. Records - The Responsible Entity shall prepare and maintain records to document training, awareness reinforcement, and background screening of all personnel having authorized access to Critical Cyber Assets and shall be provided for authorized inspection upon request.

R4. Personnel Risk Assessment - The Responsible Entity shall subject all personnel having access to Critical Cyber Assets, including contrac I lors and service vendors, to a documented company personnel risk assessment process prior to peing granted authorized access to Critical Assets.

C. Measures

MI. Awareness -The Responsible Entity shall develop and maintain awareness programs designed to maintain and promote sound security pr~ctices in the application of the standards, to include security awareness reinforcement using orie or more of the following mechanisms on at least a quarterly basis:

MIJ Direct communications (e.g., em4ils, memos, computer based training, etc.);

M1.2 Security reminders (e.g., posters, ~intranet, brochures, etc.);

M1.3 Management support (e.g., prese#tations, all-hands meetings, etc.).

M2. Training - The Responsible Entity shall develop and maintain a company-specific cyber security annual training program that includes, at a minimum, the following required items:

M2.1 The cyber security policy;

M2.2 Physical and electronic access controls to Critical Cyber Assets;

M2.3 The proper release of Critical Cyber Asset information;

M2.4 Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

M3. Records - The Responsible Entity shall develop and maintain records to adequately document compliance with this standard.

M3.1 The Responsible Entity shall maintain documentation of all personnel who have access to Critical Cyber Assets and the date of completion of their training.

M3.2 The Responsible Entity shall maintain documentation that it has reviewed and updated its training program annually.

M4. Personnel Risk Assessment - The Responsible Entity shall: M4.1 Maintain a list of all authorized personnel with access to Critical Cyber Assets, including their specific electronio and physical access rights to Critical Cyber Assets within the security perimeter(s). 1, M4.2 Review the document referred t In measure M4.1 of this standard quarterly, and update the listing within seven c endar days of any substantive change of personnel. M4.3 Physical and electronic access revocation must be completed within 24 hours for any personnel terminated for cause and seven calendar days for any personnel who have a change in status where they are not allowed access to Critical Cyber Assets (e.g., resignation, suspension, transfer, requiring escorted access, etc.). M4.4 The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel prior to being granted authorized 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 identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check is required. Entities may conduct more detailed reviews, as perinitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position. M4.5 The Responsible Entity shall ensure that adverse employment actions are consistent with the Responsible Entity's legal and human resources practices for hiring and retention of employees or contractors. M4.6 The Responsible Entity shall conduct update screenings at least every five years or for cause. D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years, and personnel risk assessment documents for the duration of employee	

employment. Contractor and service vendor records will be maintained for the duration of their engagement. 1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 Document(s) for compliance, training, awareness and screening; 1.4.2 Records of changes to access authorization lists verifying that changes were made within prescribed time frames; 1.4.3 Supporting documentation (e.g., checklists, access request/authorization documents); 1.4.4 Verification that quarterly and annual security awareness have been conducted; 1.4.5 Verification that personnel risk assessments are being conducted. 2. Levels of Non-Compliance 2.1. Level 1: 2.1.1 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 2.1.2 One instance of personnel termination (employee, contractor or service provider) in which the access control list was not updated within 24 hours for cause or seven calendar days for other personnel changes; or 2.1.3 Personnel risk assessment program exists, but not properly documented, or 2.1.4 Training program exists, ' but~ records of training either do not exist or reveal some key personnel were not trainod as required; or 2.1.5 Awareness program exists, but not applied consistently or with the minimum of quarterly reinforcement. 2.2. Level 2: 2.2.1 Access control document(s) exist, but have not been updated or reviewed for more than six months but less than 12 months; or 2.2.2 More than one but not more than five instances of personnel tennination (employee, contractor or service vendor) in which the access control list was not updated within seven calendar days or 24 hours if termination for cause; or 2.2.3 Training program exists, but doesn't not cover one of the specific items identified, or	

2.2.4 Awareness program does not exist or is not implemented, or 2.2.5 Personnel risk assessment program exists, but is not consistently applied. 2.3. Level 3: 2.3.1 Access control list exists, but does not include service vendors; and contractors or 2.3.2 More than five instances of personnel termination (employee, contractor or service vendor) in which the access control list was not updated within seven business days or 24 hours if termination for cause; or 2.3.3 A personnel risk assessment program does not exist; or 2.3.4 Training documents exist, but do not cover two or more of the specified items. 2.4. Level 4: 2.4.1 Access control rights list doos not exist; or 2.4.2 No training program exists ~ddressing Critical Cyber Assets. E. Regional Differences 1. None Version History	

Introduction

1. Title: Cyber Security - Electronic Security

2. Number: CIP-005-1

3. Purpose: This standard is intended to ensure that appropriate cyber security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality andvulnerability of the assets needed to manage grid reliability, and the risks to which they areexposed.

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.

4. Applicability

When used in within the text of this standard, "Responsible Entity" shall mean:

4.1. Reliability Coordinator
4.2. Balancing Authority
4.3. Interchange Authority
4.4. Transmission Service Provider
4.5. Transmission Owner
4.6. Transmission Operator
4.7. Generator Owner
4.8. Generator Operator
4.9. Load Serving Entity

4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities.

Applicable entities that comply with Standard CIP-002-1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard.

B. Requirements
R1. Electronic Security Perimeter - The

Physical Security

A. Introduction 1. Title: Cyber Security - Physical Security 2. Number: CIP-006-1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. Business and operational requirements fot the availability and reliability of Critical Cyber Assets dictate the need to physically sec these assets. In order to protect these assets, it is necessary to identify the Physical Security Perimeter(s) (nearest six-wall boundary) within which these Cyber Assets reside. 4. Applicability When used in within the text of this stan*, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP-002-1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP-002-1. 5. (Proposed) Effective Date: October 1, 2005 B. Requirements R1. Security Plan: The Responsible Entity sh~ll document its implementation of the following requirements in its physical security plan.1 i RM. The identification of the Physical Security Perimeters(s) and the development of a defense strategy to protect the physical perimeter within which Critical Cyber Assets reside and all access points to th ~se perimeter(s). R1.2. The implementation of the necessary measures	

to control access at all access points of these perimeter(s) and the Critical Assets within them.

R1.3. Implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the Critical Cyber Assets.

R2. 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) following an industry or government, generally accepted, risk assessment procedure.

R3. 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.

R4. Logging physical access: The Responsible Entity shall implement the technical and procedural mechanisms for logging physical access.

R5. Maintenance and testing: The Responsible Entity shall implement a 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.

R6. Documents for configuration, processes, tools, and procedures: The Responsible Entity shall maintain the specified documentation concerning its implementation of its Physical Security Plan.

C. Measures

M1. Documentation Review and Maintenance. : The Responsible Entity shall review and update its physical security plan at least annually or within 90 days of modification to the perimeter or physical security methods.

M2. 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).

M3. 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 cardholder 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 Enclosure	A cage/safe/cabinet system that controls physical access to the Critical Cyber Asset (for environments where the nearest six-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 all physical access point through the Physical Security Perimeter. The documentation shall identify and describe, at a minimum, the access request, authorization, and revocation process implemented for that control, and a periodic review process for verifying authorization rights, in accordance with management policies and controls defined in Standard CIP-003-1, and on-going supporting documentation.

M4. 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 or point of facility access.
Alarm Systems	A system that indicates a door or gate has been opened without authorization. These alarms must report back to a central

		monitoring station. Examples include card key alarm systems, 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 describe processes to review records for unauthorized access. The Responsible Entity shall have a process for creating unauthorized access reports.

M5. 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 or remote verification
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 intain documentation identifying the methods for logging physical access. This documentat ion shall identify supporting procedures to verify that the logging tools and procedures are f4,nc :ioning and being used as designed. Physical access logs shall be retained for at least 90 clays.

M6. Maintenance and testing of physical security systems: The Responsible Entity shall perform and document maintenance and testing on physical security systems annually. This documentation shall be maintained for a Oeriod of one year.

D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep document revisions and other security event-related data including unauthorized access reports for three calendar years. The Responsible Entity shall keep audit records for 90 days. The compliance monitor shall keep audit records for three years. The perfon-riance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years. 1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 The Physical Security Plan 1.4.2 Document(s) for configurat~on, processes, tools, and procedures as described in this standard. 1.4.3 Records of physical access to Critical Cyber Assets (e.g., manual access logs, automated access logs). 1.4.4 Supporting documentation (e.g., checklists, access request/authorization documents) 1.4.5 Verification that necessary updates were made at least annually or within 90 days of a modification. 2. Levels of Non-Compliance 2.1. Level 1: 2.1.1 Document(s) exist, but have not been updated or reviewed within the last 90 days and/or 2.1.2 Access control, monitoring and logging exists, but aggregate interruptions in system availability over a calendar year exist for more than seven days, but less than 1 month. 2.2. Level 2:	

2.2.1 Document(s) exist, but have not been updated or reviewed in the last 6 months and/or 2.2.2 Access control, monitoring,,nd logging exists, but aggregate interruptions in system availability over a c lendar year exist for more than one month, but less than three months. 2.3. Level 3: 2.3.1 Document(s) exist, but have! not been updated or reviewed in the last 12 months and/or 2.3.2 Access control, monitoring and logging exists, but aggregate interruptions in system availability over a c4lendar year exist for more than three months. 2.4. Level 4: 2.4.1 No access control, or no monitoring, or no logging of access exists. E. Regional Differences 1. None Version History	

Systems Security Management

Introduction 1. Title: Cyber Security – Systems Security Management 2. Number: CIP-007-1 3. Purpose: This standard is intended to ensure that the appropriate cyber security is in place, recoznizing the difference of each entity in the operation of the grid, the criticality and vunerability of the assets needed to manage the grid reliability and the risks to which they are exposed. 4. Applicability when used within the text of this standard, "Responsible Entity" shall mean: 4.1 Reliability Coordinator 4.2 Balancing Authority 4.3 Interchange Authority 4.4 Transmission Service Provider 4.5 Transmission Owner 4.6 Transmission Operator 4.7 Generator Owner 4.8 Generator Operator 4.9 Load Serving Entity 4.10 Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission: therefore, compliance to the requirements of this stanard will not apply to these facilities. Applicable entities that comply with Standard CIP-	

002-1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying witht his stahdard. Any reference in the Standard to Dritical Cyber Assets applies to those assets identified through compliance with Standard CIP-002-1 5 (Proposed) Effective Date B. Requirements R1. Test Procedures -Attended Facilities: I information security test procedures to au all new systems and significant changps t Responsible Entity shall ensure that signi patches, cumulative service packs, new releases, 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 controllod non-production environment. All testing shall be performed in a manner that precludes adversely affecting the production system and operation. The Responsible Entity shall document full detail of the test environment. The Responsible Entity shall verify that all changes to Critioal Cyber Assets were successfully tested for known security vulnerabilities prior to being rolleii into production, on a controlled non-production system. R2. Test Procedures - Unattended Facilities: ~he Responsible Entity shall not store test documentation, security procedures, and a0ceptance procedures at an unattended facility but at another secured attended facility. The Responsible Entity shall conduct security test procedures for Critical Cyber Assets at the unattended facility on a controlled non-production environment located at another secure attended facility. R3. Account and Password Management: TheResponsible Entity shall establish an account password management program to provide for access authentication, audit ability of user activity, and minimize the risk to unauthotized system access by compromised account passwords. The Responsible Entity shall establish, implement, and docurnent end user account (administrator, system, and individual) management that include but are not limited to: R3.1. Strong Passwords: In the absence of more sophisticated authentication methods that are stronger than passwords and don't require a password, (e.g., multi-factor access	

controls, certificates, or bio-metoc), the Responsible Entity shall use accounts that have a strong password. For exat alpha, numeric, and special charE allowed by the existing technolo risk-based frequency to reduce tt aple, a password consisting of a combination of cters with a minimum of six characters to the extent gy. Passwords shall be changed periodically per a .e risk of password cracking. Attended: The Responsible Entity shall have a I hult accounts, e.g., administrator or guest. The [, disabling, or renaming of these accounts where must remain, passwords shall be changed prior to Where technically supported, individual accounts shall be used (in contrast to a group account). Where individual accounts are not supported, the Responsible Entit~ shall have a policy for managing the appropriate use of grouo accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of staff changes, e.g., change in assignment or exit. R3.5. Access Reviews - Unattended: The Responsible Entity shall maintain and periodically review records of approved physical access and the cyber related work performed on Cyber Assets at unattended facilities. R3.6. Acceptable Use: The Responsible Entity shall have a policy implemented to manage the scope and acceptable use of the administrator and other generic account privileges for both attended and unattended facilities. The policy shall support a compliance audit of all account usage to and individually named person, i.e., individually named user accounts, or, personal regist~ation for any generic accounts in order to establish accountability of usage. R4. Security Patch Management: The Respon management program for tracking, ev4lua patches and upgrades to critical cyber sec R4.1. The Responsible Entity shall eva individual situation, e.g. using a and excessive patching. R4.2. The Responsible Entity shall C~er available for each Critical er management processes shall be u for not installing the patch. R4.3. In the case where installationi of' use and document a con R5. Integrity Software	

R5.1. The Responsible Entity shall used Integrity Software on all Critical Cyber Assets that are connected to a wide-area network, the Internet, or to another device that is connected to a network (e.g., prii1ter), to prevent, limit, and/or mitigate the introduction, exposure and distribution of malicious software (mal-ware) to other Cyber Assets within the Electronic Security Perimeter. R5.2. The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the Integrity Software implementation and upgrades. R5.3. In the case where integrity software is not used, e.g., operational incompatibility or not available for a particular computer platform, the Responsible Entity shall use and document a compensating measure(s). R5.4 Where repetitious application of software updates are necessary, such as at unattended facilities, the responsible Entity shall perform integrity verification prior to each site specific installation in order to prevent manual dissemination of malware. R6. Identification of Vulnerabilities and Resp R6.1. The Responsible Entity shalt pei includes: R6.1.1. A diagnostic review o R6.1.2. Scanning for open Po R6.1.3. Factory default accounts R6.1.4. Security patch and anti-virus version levels R6.2. The Responsible Entity shall implement a documented management action plan to remediate vulnerabilities and shortcomings, if any, identified in the assessment. R6.3. For unattended facilities that cont i Critical Cyber Assets, the Responsible Entity shall perform a limited vulnerability assessment prior to each upgrade as possible given the technical capability of the Cyber Assets. R7. Retention of Systems Logs: Using monitoring systems and/or procedures either internal and/or external to Critical Cyber Assets, the RespOnsible Entity shall ensure it is possible to	Syntax: repetitive (better word) Grammar: is necessary R5.4. This is a confusing point. Not sure what this is trying to achieve.

create an audit trail from logs of security-related events affecting the Critical Cyber Assets. The Responsible Entity must determine its own logging strategy to fulfill the requirement. R7.1. The Responsible Entity shall retain said log data for a period of ninety (90) calendar 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) calendar years in an exportable format, for possible use in fiu-ther event analysis. R7.2. In lieu of automatically generated logs at unattended facilities, the Responsible Entity shall collect and retain the physical access and change records of users at each approved access session, or at a minimum annually. R8. Change Control and Configuration Management R8.1. 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 shall includo, change management procedures that at a minimum provide testing, modification aud~t trails, problem identification, a back out and recovery process shall modificati~ns fail, and ultimately ensure the overall integrity of the Critical Cyber Assets.	
R8.2. The Responsible Entity shall ensure the controlled development or test environment for Cyber Assets residing in unattended facilities are not at the unattended facility. The Change Control Process for Cyber Assets at unattended facilities shall prevent the inadvertent dissemination of faulty or compromised software to multiple unattended sites R9. Disabling Unused Host Ports/Services: The Responsible Entity shall enable only those ports/services required for normal and emergency operations of Critical Cyber Assets. All other ports/services, including those used for testing purposes, must be disabled prior to production usage. R10. Operating Status Monitoring Tools: For maintaining situational awareness, the Responsible Entity shall ensure Critical Cyber Assets U~ sed for operating critical infrastructure are included or augmented with automated and/or process tools, where practical, to monitor operating state, utilization and performance, and cyber security events experienced by the Critical Cyber Assets themselves, and issue alarms for specified	R8.2 Why not say that all controlled development and test environments should be located in controlled sites. We disagree with the premise that unattended sites present an additional degree of risk when appropriately secured.

indications, as implemented. For Critical Cyber Assets in use at unattended facilities that are not capable of being electronically monitored remotely, the Repponsible Entity shall review and document pertinent metrics manually during routine access/sorvice to said equipment. R1 1. Back up and Recovery: The Responsible Entity shall back up on a regular basis, where technically feasible, information and data that is resident or required by Cyber Assets used to manage critical electric infrastructure. The back up must be stored in a remote or hardened site some distance away from the Critical Cyber Assets. Information stored on computer media for a prolonged period of time shall be tested at least annually to ensure that the information is recoverable. For unattended facilities, back-up and recovery materials can be effectively tested at central test facility and shall not be tested on site. C. Measures M1. Test Procedures: For all Critical Cyber Assets, the Responsible Entity shall maintain records of test procedures, results, and acceptance of successful completion. M2. Account and Password Management: The Responsible Entity shall maintain a documented password policy and record of semi-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. Review access permissions within 24 hours for any personnel terminated for cause and seven calendar days for any personnel who have a change n status where they are not allowed access to Critical Cyber Assets (e.g., resignation, suspension, transfer, requiring escorted access, etc.). N13. 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, approval for installation, compensating measures, and installation date. M4. Integrity Software: The Responsible Entity's change control documentation shall include a record of all integrity software installations including: M4.1 Version level actively in use M4.2 Installation date	

M4.3 Or provide documentation for other compensating measures taken M5. Identification of Vulnerabilities and Responses: N15.1 The Responsible Entity shall maintain documentation identif~ing the organizational, technical and procedural controls, including tools and procedures for monitoring the critical cyber environment for vulnerabilities. M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation. plans for all vulnerabilities and/or shortcomings that are found. M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities. M6. Retention of Logs: M6.1 The Responsible Entity shall maintain documentation that indexes location, content, and retention schedule of all log data captured from the Critical Cyber Assets. M6.2 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. M7. Change Control and Configuration Management: M7.1 The Responsible Entity shall maintain documentation identifying the controls, including tools and procedures, for managing change to and testing of Critical Cyber Assets. M7.2 The documentation shall verify that all the Responsible Entity follows a methodical approach for managing change to their Critical Cyber Assets. M8. Disabling Unused Host Ports/Services: The Responsible Entity shall disable unused ports and services, and maintain documentation of status/configuration of all ports and services available on Critical Cyber Assets. M9. Operating Status Monitoring Tools: The Responsible Entity shall maintain documentation identifying organizational, technical, and procedural controls, including tools and procedures for monitoring operating state, utilization, and performance of Critical Cyber Assets. M10. Back-up and Recovery:	

M10.1 The Responsible Entity shall maintain documentation that index location, content, and retention schedule of all Critical Cyber Assets' information backup data and tapes. M10.2 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. M10.3 The documentation shall verify that the Responsible Entity is capable of recovering from the failure or compromise of Critical Cyber Asset. D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years. 1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 Document(s) for configuration, processes, tools and procedures as described in this standard. 1.4.2 System log files as described in measure M6. 1.4.3 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.). 2. Levels of Non-Compliance 2.1. Level 1: Document(s) exist, but does not cover up to two of the specific items identified	

and/or the document has not been reviewed or updated in the last 12 months. 2.2. Level 2: Document(s) exist, but does not have three of the specific items identified and/or 2.2.1 A gap in the reviews for the following items exists: 2.2.1.1 Access Reviews (semi-annually for attended facilities, periodically for unattended facilities). 2.2.1.2 Security Patch Management (monthly) 2.2.1.3 Integrity Software (monthly) 2.2.2 Retention of system logs exists, but a gap of greater than three days but less than seven days exists. 2.3. Level 3: 2.3.1 Document(s) exist, but more than three of the items specified are not covered. 2.3.2 Test Procedures: Document(s) exist, but documentation verifying that changes to Critical Cyber Assets tested is incomplete or changes to Critical Cyber Assets were not tested. 2.3.3 Account and Password Management: Document(s) exist, but documentation veritiing accounts and passwords comply with the policy does not exist. 2.3.4 Security Patch Management: Document exists, but records of security patch installations are incomplete. 2.3.5 Integrity Software: Documentation exists, but verification that all Critical Cyber Assets are being kept up to date on anti-virus software or that compensating measures are being taken does not exist. 2.3.6 Identification of Vulnerabilities and Responses: 2.3.6.1 Document exists, but annual vulnerability assessment was not completed and/or 2.3.6.2 Documentation verit(ing that the entity is taking appropriate actions to remediate potential vulnerabilities does not exist. 2.3.7 Retention of Logs (operator, application, intrusion detection): A gap in the logs of greater than 7 days exists.	

2.3.8 Disabling Unused Host Ports/Services: Docurnents(s) exist, but a record of regular audits does not exist. 2.3.9 Change Control and Configuration Management: N/A 2.3.10 Operating Status Monitoring Tools: N/A 2.3.11 Backup and Recovery: Document exists, but record of annual restoration verification exercise does not exist. 2.4. Level 4: No documentation exists. E. Regional Differences 1. None Version History	

A. Introduction 1. Title: Cyber Security - Incident Response Planning 2. Number: CIP-008-1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. Security measures designed to protect Critical Cyber Assets from intrusion, disruption or other forms of compromise must be monitored on a continuous basis. This standard requires responsible entities to define the procedures that must be followed when Cyber Security Incidents are identified. This standard requires: • Developing and maintaining of documented procedures, • Classification of incidents, • Actions to be taken, and • Reporting of Incident. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP-002-1. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP-002-1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. 5. (Proposed) Effective Date: October 1, 2005 B. Requirements	

R1. The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate and/or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items: R2. Incident Classification: The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents. R3. Cyber Security 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. R4. Cyber Security Incident Reporting: The Responsible Entity shall report all Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center ES ISAC in accordance with the Indications, Analysis & Warning Program (IAW) Standard Operating Procedure (SOP). The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. C. Measures Ml. The Responsible Entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and Cyber Security Incident reporting requirements at least annually or within 90 calendar days of known changes. M2. The Responsible Entity shall retain records in addition to requirements defined in Standard CIP-007-1, requirement R7 (Retention of Systems Logs) of Cyber Security Incidents for three calendar years. D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe	

The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years. 1.4. Additional Compliance Information 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: 1.4.1 System and application log file entries, 1.4.2 Video, and/or physical access records, 1.4.3 Documented records of investigations and analysis performed, 1.4.4 Records of any action taken including any recovery actions initiated. 1.4.5 Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC. 2. Levels of Non-Compliance 2.1. Level 1: 2.1.1 Documentation exists, but has not been updated with known changes within 90 calendar days. 2.2. Level 2: 2.2.1 Incident response documentation exists, but has not been updated or reviewed in the last 12 months and/or 2.2.2 Records related to Cyber Security Incidents are not maintained for three years or are incomplete. 2.3. Level 3: 2.3.1 Incident response documentation exists but is incomplete and/or 2.3.2 Cyber Security Incidents have occurred but were not reported to the ES ISAC 2.4. Level 4: No documentation exists.	

E. Regional Differences 1. None Version History	

Recovery Plans

A. Introduction 1. Title: Cyber Security - Recovery Plans 2. Number: CIP-009-1 Purpose: This standard is intended to ensure that appropriate cyber 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. 3. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 3.1. Reliability Coordinator 3.2. Balancing Authority 3.3. Interchange Authority 3.4. Transmission Service Provider 3.5. Transmission Owner 3.6. Transmission Operator 3.7. Generator Owner 3.8. Generator Operator 3.9. Load Serving Entity 3.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP-002-1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP-002-1. 4. (Proposed) Effective Date: October 1, 2005 B. Requirements R1. The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan(s) at least annually. R2. The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan. R3. The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that effects the protection of Critical Cyber Assets. R4. Recovery plan(s) and any updates or	

changes shall be communicated to personnel responsible for their operation or responsibility for such Critical Cyber Asset within seven (7) calendar days of development or modification. R5. The Responsible Entity shall develop training and awareness for its recovery plan(s) that follow the requirements set forth in Standard CIP-004-1 - Personnel and Training. C. Measures M1. The Responsible Entity shall document its Recovery Plan(s) and maintain records of all exercises or drills for at least three (3) years. M2. The Responsible Entity shall document its Recovery Plan(s) and maintain records of all exerci~es or drills for at least three (3) years. M3. The Responsible Entity shall review and update if needed, its response to events of varying duration and severity annually or as necessary. M4. The Responsible Entity shall review and update recovery plan(s) annually. M5. The Responsible Entity shall conduct drills at least every three (3) years and keep attendance records to its Recovery Plan(s) training. D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall make the documents described in this standard available for inspection by the compliance monitor upon request. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years. 1.4. Additional Compliance Information Not specified. 2. Levels of Non-Compliance 2.1. Level 1: Recovery plan(s) exist, but	

have not been reviewed or updated in the last calendar year. 2.2. Level 2: Recovery plan(s) have not been reviewed, exercised, or training performed. 2.3. Level 3: Recovery plan(s) address neither the types of events that are necessary nor any specific roles and responsibilities. 2.4. Level 4: No recovery plan(s) exist. E. Regional Differences 1. None Version History	

Implementation Plan
for Cyber Security Standards
CIP-002-1 through CIP-009-1

The intent of the proposed NERC cyber security standard is to ensure that all entities responsible for the reliability of the bulk electric systems of North America identify and protect critical cyber assets that control or could impact the reliability of the bulk electric systems. This implementation plan is based on the following assumptions; Cyber Security Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP006-1, CIP-007-1, CIP-008-1, and CIP-009-1 are approved by the ballot body and the NERC Board of Trustees no later than September 1, 2005. The NERC Functional Model is implemented in concert with the passage of the Version 0 standards. Entities have registered to the NERC Functional Model. Cyber Security Standards CIP-002-1 through CIP-009-1 become effective October 1, 2005. To provide time for responsible entities to examine their policies and procedures, to assemble the necessary documentation, and to meet the requirements of these standards, compliance assessment will begin starting in 2006. Implementation Schedule Beginning with the first quarter of 2006, NERC and its Regions will develop self-certification forms as part of their compliance and enforcement programs. The Regions will distribute these forms to the applicable functional entities within their respective Regions. Regions may ask other entities to provide self-certification forms if they believe they are performing one of the	As a general comment, we feel that the implementation timetable is too rigorous. It does not align with corporate budgets nor take into consideration the magnitude of the effort to go from NERC 1200 to CIP 002-009. We believe that entities should be requested to certify they will remain compliant with NERC 1200 indefinitely and that 2006 be a planning and budget year for CIP 002-006 implementation with 2007 requiring compliance.

functions identified in the standard. In such cases, the completion of a self-certification form by those other entities will be voluntary. All applicable entities will complete and submit the appropriate Regional self-certification forms, indicating their compliance, or degree of non-compliance, to the requirements of these standards. These self-certification forms will be submitted to the appropriate NERC Regional Reliability Council, which will hold the individual responses as confidential. It will be the responsibility of the Regional Compliance Manager to summarize the results of the self-certification and provide that summary to the NERC Compliance Program. Responsibility for compliance with these standards remains with the "Responsible Entity". The following table identifies when entities must be Auditably Compliant (AC) or Substantially Compliant (SC) with a requirement. Auditably Compliant means the entity meets the full intent of the requirement and can prove compliance to an auditor. The intent of the proposed NERC cyber security standard is to ensure that all entities responsible for the reliability of the bulk electric systems of North America identify and protect critical cyber assets that control or could impact the reliability of the bulk electric systems. This implementation plan is based on the following assumptions; Cyber Security Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP006-1, CIP-007-1, CIP-008-1, and CIP-009-1 are approved by the ballot body and the NERC Board of Trustees no later than September 1, 2005. The NERC Functional Model is implemented in concert with the passage of	

the Version 0 standards. Entities have registered to the NERC Functional Model. Cyber Security Standards CIP-002-1 through CIP-009-1 become effective October 1, 2005. To provide time for responsible entities to examine their policies and procedures, to assemble the necessary documentation, and to meet the requirements of these standards, compliance assessment will begin starting in 2006. Implementation Schedule Beginning with the first quarter of 2006, NERC and its Regions will develop self-certification forms as part of their compliance and enforcement programs. The Regions will distribute these forms to the applicable functional entities within their respective Regions. Regions may ask` other entities to provide self-certification forms if they believe they are performing one of the functions identified in the standard. In such cases, the completion of a self-certification form by those other entities will be voluntary. All applicable entities will complete and submit the appropriate Regional self-certification forms, indicating their compliance, or degree of non-compliance, to the requirements of these standards. These self-certification forms will be submitted to the appropriate NERC Regional Reliability Council, which will hold the individual responses as confidential. It will be the responsibility of the Regional Compliance Manager to summarize the results of the self-certification and provide that summary to the NERC Compliance Program. Responsibility for compliance with these standards remains with the “Responsible Entity”. The following table identifies when entities	

must be Auditably Compliant (AC) or Substantially Compliant (SC) with a requirement. Auditably Compliant means the entity meets the full intent of the requirement and can prove compliance to an auditor. Substantially Compliant means an entity has begun the process to become compliant with a requirement, but is not yet Auditably Compliant. The table has two sections for each standard. The first section defines the implementation schedule for Balancing Authorities (BA) and Reliability Coordinators (RC). The second section defines the implementation schedule for Interchange Authorities (IA), Transmission Providers (TP), Transmission Owners (TO), Transmission Operators (TOP), Generation Owners (GO), Generation Operators (GOP) and Load Serving Entities (LSE).	

Compliance Schedule for Standards CIP-002-1 through CIP-009-1

	1st Qtr 2006		1st Qtr 2007		2008 & Beyond	
Re	Control Center	Other Facilities	Control Center	Other Facilities	Control Center	Other Facilities

Standard CIP-002-1 – Critical Cyber Assets BA & RC						
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
Standard CIP-002-1 – Critical Cyber Assets IA, TP, TO, TOP, GO, GOP, LSE						
F	SC	SC	AC	AC	AC	AC
F	SC	SC	AC	AC	AC	AC
F	SC	SC	AC	AC	AC	AC
F	SC	SC	AC	AC	AC	AC
Standard CIP-003-1 – Security Management Controls						
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
Standard CIP-003-1 – Security Management Controls						
F	SC	SC	AC	AC	AC	AC
F	SC	SC	AC	AC	AC	AC
F	SC	SC	AC	AC	AC	AC
F	SC	SC	AC	AC	AC	AC
F	SC	SC	AC	AC	AC	AC
Standard CIP-004-1 – Personnel & Training BA & RC						
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC
F	AC	SC	AC	AC	AC	AC

	1st Qtr 2006		1st Qtr 2007		2008 & Beyond	
Requirement	Control	Other Facilities	Control	Other Facilities	Control	Other Facilities
R4	SC	SC	SC	SC	AC	AC
Standard CIP-004-1 – Personnel & Training IA, TP, TO, TOP, GO, GOP, LSE						
R1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	SC	SC	AC	AC
Standard CIP-005-1 – Electronic Security BA & RC						
R1	AC	SC	AC	AC	AC	AC
R2	AC	SC	AC	AC	AC	AC
R3	AC	SC	AC	AC	AC	AC
R4	AC	SC	AC	AC	AC	AC
R5	AC	SC	AC	AC	AC	AC
R6	AC	SC	AC	AC	AC	AC
Standard CIP-005-1 – Electronic Security IA, TP, TO, TOP, GO, GOP, LSE						
R1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	AC	AC	AC	AC
R5	SC	SC	AC	AC	AC	AC
R6	SC	SC	AC	AC	AC	AC
Standard CIP-006-1 – Physical Security BA & RC						
R1	AC	SC	AC	AC	AC	AC
R2	AC	SC	AC	AC	AC	AC
R3	AC	SC	AC	AC	AC	AC
R4	AC	SC	AC	AC	AC	AC
R5	AC	SC	AC	AC	AC	AC
R6	AC	SC	AC	AC	AC	AC
Standard CIP-006-1 – Physical Security IA, TP, TO, TOP, GO, GOP, LSE						
R1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	AC	AC	AC	AC
R5	SC	SC	AC	AC	AC	AC
R6	SC	SC	AC	AC	AC	AC
Standard CIP-007-1 – Systems Security Management						

	1st Qtr 2006		1st Qtr 2007		2008 & Beyond	
COMM	Control	Other Facilit	Control	Other Facilit	Control	Other Facilit
R4	AC	SC	AC	AC	AC	AC
R5	AC	SC	AC	AC	AC	AC
Standard CIP-009-1 – Recovery Plans IA, TP, TO, TOP, GO, GOP, LSE						
1	SC	SC	AC	AC	AC	AC
R2	SC	SC	AC	AC	AC	AC
R3	SC	SC	AC	AC	AC	AC
R4	SC	SC	AC	AC	AC	AC
R5	SC	SC	AC	AC	AC	AC

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: **Jerry Litteer**			
Organization: **INL**			
Telephone: **(208) 526-9117**			
Email: **Gerald.litteer@inl.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	X	8 - Small Electricity End Users
☐	SPP	☐	9 - Federal, State, Provincial Regulatory or other Government Entities
☐	WECC		
X	NA - Not Applicable		

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

Group Name: **Idaho National Laboratory**

Lead Contact: Jerry Litteer

Contact Organization: Cyber Security

Contact Segment:

Contact Telephone: 208.526.9117

Contact Email: Gerald.litteer@inl.gov

Additional Member Name	Additional Member Organization	Region*	Segment*
Rita Wells	INL	NA	

* 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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Cyber Assets –

Cyber Security Incident –

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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?

X No

If no, please identify revisions necessary to make this clear.
It needs to clarified that the Critical Asset List is designed to help the utilities define what they need in a backup site and also define where spending their security budgets makes sense.

Specifically excluding areas provides an open field for attack (small generators, distribution, and non-routable protocols). The definition of non-routable protocols is difficult to judge. It is problematic to exclude telecommunications from CIP but to include them in the definition of the critical cyber assets.

A) Exclude non-routable protocols: Does one element in a protocol stack (e.g. old DNP) make it non-routable even though it's running on frame relay PSTN? Conversely if running an old serial protocol over a privately owned line (P2P) with concentrators through a router (e.g. serial cards in a router) to handle network traffic for convenience - does the router make it routable?
B) Based on the heavily networked architecture to support the electric grid, excluding the smaller facilities (e.g. not 80% generation) exposes the connecting architectures (i.e. transmission operators).
C) No mention of discrete communications here as being excluded but is excluded in CIP-005-1B R1, discussion of electronic perimeter.

With the advance in new wireless devices, there needs to be some discussion about wireless access points and the possible address the use of wireless devices (Blackberry's, etc.) in restricted areas.

While I have reason to suspect this standard is a step instead of being a final, the comments page indicates final. Adopting a final standard with these exclusions is not advised.

Missing from the levels of non-compliance is – document exists but no compliance issue if limited critical cyber assets identified in which NERC does not agree with the list or justification?

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

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

☐ Yes
X 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.

The CIP standard treats the Process Control (SCADA) network as though it is an island in the middle of the Internet. In fact, the majority (99 %+) of SCADA networks are within the network boundaries of a corporate network. It should be made clear that the corporate network is the first line of defense for the SCADA network. This standard (nor any of the previous standards) incorporates the corporate network security into the overall security of the grid. You can not separate the two.

The numerous yearly reviews that are required throughout the CIP standard should probably be consolidated into a new section of the standard. This would help focus the reviews and facilitate a single yearly security posture review.

Please Enter All Comments in Simple Text Format.

This would also help eliminate forgetting a review that is buried in another part of the standard. At least a summary review log should be included to make sure all is ready.

Missing: There is no mention of comparing the list of authorized users against the production system or accounts. (CIP007 R3.4 – semi-annually) Periodic review of accounts on the production system is essential. No mention of checking the integrity of the operating system (e.g. rootkit) (CIP007 R5 software integrity but no specifics). No mention of reviewing the audit logs for suspicious activity (CIP-005 M5.3 – document review was done but no frequency specified)

R5.3 user access changes due to termination accomplished in a time frame not specified as compared to 24 hours as specified in 1300. CIP-004 M4.3 states 24 hours for termination change of access. These statements are inconsistent. A process should be in place that would monitor AND document what was done during any extended period.

M1. *The Responsible Entity shall maintain its written cyber security policy stating the entity's commitment to protect Critical Cyber Assets.*

This is a fairly weak requirement for a security policy. The policy needs to be viewed on its content not its mere existence. Since the "Guide Lines" are not finalized, the following should be noted. The policy(s) should address: how the corporation enforces the policy, scope of the implementation and coverage, what employee and vendor uses of the network and assets are allowed, what penalties can be imposed, methods of recourse or appeal.
Above all, the policy must: make good business sense, be technically sound and enforceable, be available to employee /vendor and be technically sound and enforceable.

The policy must also be signed by any one with access to the corporate assets (vendor, employee, backup site manager, etc.), whether these assets are part of a control system or not.

With the growing focus on network/data security, it would make sense for the corporation to have a single Security Policy document. This document would be divided into special sections that discuss general IT, SCADA, HIPPA, etc. security policies. This keeps from having conflicting policies that confuse rather than help the overall security posture.

M2 Review of cyber security policy a minimum of 3 years changed from 1 year in 1300. Due to the number of procedural controls a more frequent policy review is suggested.

M13.1 and M13.2 current list of personnel authorized for production, and change control added – better. There is no mention of comparing the list of authorized users against the production system or accounts. Periodic review of accounts on the production system is essential – CIP-007-1 R3.4 mentions semi-annually. It would be ideal if the Password files on the production and test systems were scanned each day to make sure verify the authorized accounts (user + application + system) were the only accounts on the systems.

M18 User access rights confirmed annually instead of ¼ year in 1300. This might be OK if checking against the production system more frequently but that is only ½ year (CIP-007-1 R3.4).

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

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

X 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 Enter All Comments in Simple Text Format.

Does not say security training is tied to employment but infers access to critical cyber assets. Access to critical cyber assets could be a condition of employment. I realize this standard does not want to be prescriptive, but without strong senior management involvement and conditions to employment – security programs fail.

R2. Training

Add the following**:**

R2-a. Additional training should be given as access level increases.

R2-b. All training must include vendors, contractor personnel and others who (for example local backup entities) that have access to the data/system.

R2-c. Training needs to be updated yearly at a minimum or whenever new requirements / access status dictates.

M4.3 changes to 24 hours terminated with cause and 7 days for change in status – still too long.

No mention of what the operator or system administrator training for a suspected incident or trained for expected utilization of the systems and performance indicators.

CIP–005–1 — Cyber Security — Electronic Security

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

X 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.

Overall Missing items include: a) verifying the integrity (on BOTH production and test hosts) of the operating systems (e.g. no rootkits), reviewing file systems for unexpected files, directory structures or accounts. (CIP007 R5 integrity software?), b) excluded discrete communications and c) no review of logs

"In the case of Critical Cyber Assets, the security level assigned to these Electronic Security Perimeters is high." Suggest rewording too subjective.

R1. Discrete communications are excluded. Again this provides an opening for exploit.

R2 Disabling unused Network Ports/Services: a) text says shall enable only, and title should change from Disable to Enable Used Only. While I understand the difficulty in identifying all the ports and services used in these architectures (e.g. OPC) that's the point – you can secure if you don't know.
b) Missing a requirement to remove unused applications, this goes beyond ports and services. Eliminated all unused applications also reduces your patching complexity and unknown or unidentified security risks.

R5. Monitoring Electronic Access Control contains no requirement for frequency of review or alarm timing. Typical issue with logging information is that no body uses it again. Suggest alarm at multiple attempts over a short time period, and daily review of logs to establish trends of activities and identify where future vulnerabilities are likely. Monitoring equipment and activities are useless without reviewing results daily. Having a system that 'watches' the network traffic would pass as monitoring. If the logs are not examined, how do you know your status? This basic requirement is missing throughout the whole standard, not just in CIP-005-1.

M2 change Disabling unused title and text to enable only used.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

M3.1 annual audit of all dial-up modem connections – is way too infrequent.

M5.3 review access records for authorized access – no frequency specified.

Compliance
1.1.2 90 calendar days retention for access logs, firewall logs and intrusion detection logs is way too short given the nature of reluctance to share incidences until can't resolve on own or delay in time of recognition of unauthorized activity.

CIP–006–1 —Cyber Security — Physical Security

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

X 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.

There is no requirement for log review. Suggest alarm at multiple attempts over a short time period, and daily review of logs to establish trends of activities and identify where future vulnerabilities are likely. Monitoring equipment and activities are useless without reviewing results daily. Having a camera system that 'watches' the door traffic would pass as monitoring. If the logs are not examined, how do you know your status? This basic requirement is missing throughout the whole standard, not just in CIP-005-1.

M5 and Compliance 1.1.2 keep audit records for 90 days – too short for low and slow cyber activities which might involve a physical aspect, but compliance monitor shall keep audit records for 3 years.

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

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

X 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.

A concise definition of terms is needed here when talking about the different kinds of patches and software. Especially the term integrity software, is it software to validate the size and contents of a other files or is it anti-virus software, just what do you mean.

R1 Test procedures 'ensure that significant changes include but are not limited to security patches, cumulative service packs, new releases, upgrades or versions to operating systems, applications, database or other third party software, and firmware.' It is way too difficult to discuss all these type of patches together since they affect different functions. There is a need to discuss the testing security patches separate from updates to the application, or vendor software.

"These tests are required to mitigate risk from known vulnerabilities, affecting operating systems…." I think this has to be reworded. The patches are to mitigate risk from known vulnerabilities, and the tests are to ensure no adverse impact to production operations.

"The responsible entity shall verify that all changes to Critical Cyber Assets were successfully tested for known security vulnerabilities…" - way too resource intensive. The patch may be fixing a potential vulnerability that is not in the wild yet. Due to the no time available for patching on these systems, the responsible entity should be able to

identify another mitigation instead of testing and applying a patch immediately. This will enable the entity to wait and see if the patch actually worked as advertised in other industries prior to testing in the non-production environment and applying to a 24-7 real-time environment.

This discussion is confusing and it might be because too many items are being discussed at once. 'Tested for known security vulnerabilities…' might be talking about vulnerability scans – software that will run and look for tens of thousands of known vulnerabilities (e.g. Trojans). It's difficult to imagine running a COTS vulnerability scan on a production SCADA or control system environment – it will kill communications. This type of scan could be run on a non-production environment.

R3 Account and Password Management. This is still an issue with legacy applications that were not designed or implemented for multiple accounts and passwords. Other forms to insure authenticity similar to CIP-005-1 B R4.2 might be required.

R3.1 specifies the 6 character alpha, numeric and special character but only mentions changed periodically. Cyber hackers like to see the specifics to focus their cracker programs. The most important password characteristic is frequency of change, which is not specified.
R3.4. Invalid accounts, regardless of their origin (vendor-guest, expired, etc.) must be disabled immediately and all account actions (enabled or disabled) reviewed weekly. This will insure that non-authorized accounts are swiftly dealt with.

R3.6 This requirement is redundant. This should be completely spelled out in the security policy required in CIP-003-1.

R4 Security Patch Management – Need definition of security patch management vs. integrity software.

R4.1 risk based assessment, so as to avoid un-necessary and excessive patching. This sounds good but the opposite is also valid. Patching a software application that is not applied to the control system but is used inside the security perimeter (e.g. router software) should be tested and done immediately to reduce the exposure if someone penetrated the perimeter. This type of patch should have limited impact on operations.

R4.2 Monthly review of patches up to date is not enough if this is truly a security patch with the need to update signatures.

R5 Integrity software: Most integrity software available is based on the ability to update signatures to the integrity software. These signatures are considered security patches and will not be implemented in a timely fashion if they have to go through the known vulnerability testing as specified in R1.

R5.2 Monthly review of integrity software is not sufficient. Signature based security patches normally are applied a lot more frequently to keep up to date with published exploits.

R5.3 where integrity software is not used, compensating measure – this would be a good place for a discussion on reviewing for unauthorized accounts, reviewing file systems for unrecognized or unexpected files.

R5.4 Unattended facilities shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of mal-ware. This also needs to include the scanning of the media used for updating systems at these facilities.

R6 annually vulnerability assessment that includes scanning for open ports services (CIP005 R2 no time specified) and modems (CIP005-M3.1 annual), factory default accounts, security patch (CIP007 R4.2 monthly) and anti-virus version levels (CIP007 R5.2 monthly). This requirement contradicts with other requirements. Is this in addition to the other requirements?

R7.1 90 day retention of logs will not be long enough for the forensic activity for stealth attacks. Only keep for 3 years if the attack is identified.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

R9 change title to Enabling only used host ports and services.

R10 Issuing of alarms has no specified time. This in conjunction with no frequency for log reviews is worthless. Monitoring the performance and usage is great if you have a trained operator or good system administrator who knows what normally activity based on the outside factors should reflect.

R11 Not only does the media that stores the data have to be tested annually the procedures to restore a system should be tested or exercised annually. This should be combined with CIP-009-1 R1.

M2 24 hour for termination might be too long.

M3 date of testing might not be needed if security patches for applications that reside on the same machine but do not affect the production operations can be installed without testing.

M8 change disabling unused host ports/services in title and text to enable only those explicitly required.

M10.2 Should read 'include tested recovery procedures…'

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?

X 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.

General comment. If there is no requirement in the CIP standard for examining the logs, why is there are requirement to report incidents you do not know about.

M2 those logs are only retained if an incident has been identified in the 90 day window for log retention.

CIP-009-1 – Cyber Security – Recovery Plans

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

X 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.

R1 here's exercise recovery plans at least annually should be coordinated with the test of the backup media (CIP-007 R11).

R3 and R4**.** These two requirements seem to conflict. In any case, the backup recovery plans need to be kept current, tested, and 'as-built'. Waiting for seven days or 90 days may be fatal.

M3. Annually may be to long. Documentation should exist that when a change in the 'system' is made that would affect the recovery plan, the plan is also updated.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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

X

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

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**
☐ **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: ECAR Critical Infrastructure Protection Panel

Lead Contact: Larry Conrad

Contact Organization: Cinergy

Contact Segment: **3**

Contact Telephone: 317.838.2022

Contact Email: Larry.Conrad@Cinergy.com

Additional Member Name	Additional Member Organization	Region*	Segment*
Jack Hobbick	Consumers Energy	**ECAR**	**3**
Don Miller	First Energy	**ECAR**	**1**
Tim Conway	NIPSCO	**ECAR**	**1**
Scott Cunningham	OVEC	**ECAR**	**1**
Keith Fowler	LG&E Energy	**ECAR**	**1**
Grant McDonald	Allegheny Power	**ECAR**	**1**
Thomas Cichowski	Duquesne Light	**ECAR**	**3**
Dan Powell	IP&L	**ECAR**	**1**
Mohammad Mohtati	Vectren	**ECAR**	**1**
Robert Brantley	METC	**ECAR**	**1**
Peter Scussel	ITC	**ECAR**	**1**
Shawn Null	AEP	**ECAR**	**1**
Wayne Jansen	DPL	**ECAR**	**3**
Jim Davis	EKPC	**ECAR**	**1**
Mark Majewski	Detroit Edison	**ECAR**	**3**

* 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.

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.

These comments do not apply to the definitions, but are general comments that are applicable to all of the proposed standards CIP-002 through CIP-009.

- Standardize the periodicity for review so that most requirements have either an annual or a quarterly review period. At present there are varying times for review, which make it difficult to maintain all of the documentation
- Measures should point back to the appropriate requirement. At present it is sometimes difficult to understand which measure points back to which requirement.
- Change the data retention from 3 years to 2 years throughout the document

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.

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.

Section i.d.	Current Language	Recommendation – Change to
B. R.1.1.1.	Control Centers and backup control centers performing the functions of a Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generation Owner, Generation Operator, and Load Service Entities.	System Control Centers and backup control centers performing the functions of a Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generation Owner, Generation Operator, and Load Service Entities.
B. R1.1.3. & R1.1.8	Transmission substations associated with elements monitored as IROL.	While a definition exists of an IROL, some additional explanation may be required to ensure common understanding of how these requirements should be applied.
B. R.1.1.4.	Generating resources under control of a common system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization.	Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization.
C. M5	A signed and dated record of the senior management officer's approval of the list of Critical Assets must be maintained.	A signed and dated record of the senior management officer's approval of the list of Critical Assets must be maintained annually.

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.

Section i.d.	Current Language	Recommendation – Change to
B. R2.1	The Responsible Entity shall identify **all** information, regardless of media type, related to the entity's Critical Cyber Assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible. This includes 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 must be protected as well.	Recommend removing the word "all" and recommend removing the last sentence, which is redundant in the existing language. Change to: The Responsible Entity shall identify information, regardless of media type, related to the entity's Critical Cyber Assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible. The following documents must be protected: Procedures related to critical cyber assets, 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.
D. 2.1.1	A current senior management official was not designated for less than 30 calendar days during a calendar year…	**Recommend deleting item D.2.1.1.** Current language conflicts with Section C.M11, which allows 30 days to update the information. Therefore, failure to designate senior official for less than 30 calendar days is not a violation. Non-Compliance violation D.2.1.1 should be eliminated. C.M11 states: Changes to the current senior management official must be documented within 30 calendar days of the effective date.

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.

Section i.d.	Current Language	Recommendation – Change to
A.3. Purpose	Personnel having authorized 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…	Recommend changing "screening" to "risk assessment" for continuity of intent throughout the document. Change to: Personnel having authorized 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 risk assessment, training, security awareness…
B. R2.	The Responsible Entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will ensure that all personnel having authorized 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 Cyber Assets.	Recommend: Additional wording stating the level of training that personnel receive will be commensurate with their defined roles and responsibilities previously addressed in CIP-003-1, R3. second paragraph. Clarification is needed in the first sentence to specify what needs to be reviewed. Change to: The responsible Entity shall develop and maintain a company specific cyber security training program. The Program and training materials will be reviewed annually. This program will ensure that all personnel having authorized access to Critical Cyber Assets shall be trained annually in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these Critical Cyber Assets. Training will be commensurate with the roles and responsibilities defined in Standard CIO-003-1.
B. R3.	Records – The Responsible Entity shall prepare and maintain records to document training, awareness reinforcement, and background screening of all personnel having authorized access to Critical Cyber Assets and shall be provided for authorized inspection upon request.	Recommend changing "background screening" to "personnel risk assessment", which is the language used in the rest of the document. Recommend correcting grammar in last part of sentence. Change to: Records – The Responsible Entity shall prepare and maintain records to document training, awareness reinforcement, and personnel risk assessment of all personnel having authorized access to Critical Cyber Assets and shall provide records for authorized inspection upon request.

B. R4	Personnel Risk Assessment – The Responsible Entity shall subject all personnel having access to Critical Cyber Assets, including contractors and service vendors, to a documented company personnel risk assessment process prior to be being granted authorized access to Critical Assets.	Recommend striking the word …company… to allow flexibility with the assessment processes that contractors and service vendors may apply. Change to: Personnel Risk Assessment – The Responsible Entity shall subject all personnel having access to Critical Cyber Assets, including contractors and service vendors, to a documented personnel risk assessment process prior to granting them authorized access to Critical Assets.
C.M4.4	The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel prior to being granted authorized 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 identify verification (e.g., Social Security Number verification in the U>S>) 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.	Recommend: Delete the last two sentences so as not to impinge upon existing or developing personnel risk assessment policies and processes that companies may utilize. Minor grammar correction in first sentence. Change to: The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel prior to granting authorized access to Critical Cyber assets in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.
C.M4.6	The Responsible Entity shall conduct update screenings at least every five years or for cause.	Use “personnel risk assessment” rather than “screenings” for continuity throughout the document. Change to: The Responsible Entity shall conduct update personnel risk assessments at least every five years or for cause.
D.1.4.1	Document(s) for compliance, training, awareness, and screening;	Use “personnel risk assessment” rather than “screening” for continuity throughout the document. Change to: Document(s) for compliance, training, awareness, and personnel risk assessments;
D.1.4.4	Verification that quarterly and annual security awareness have been conducted;	In Additional Compliance Information 1.4.4 - Strike the words …and annual… . There is no reference to annual security awareness programs within the Requirements and Measures of this standard. Quarterly basis only, is mentioned in M1. Change to: Verification that quarterly security awareness have been conducted;

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.

Section i.d.	Current Language	Recommendation – Change to
B. R5.	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.	Change to: The responsible Entity shall implement the organizational, technical, and procedural controls, including tools and procedures, to log the following and review in a timely manner: 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 commensurate with the value of the asset.
B R6.	The entity shall conduct a review of these documents at least ever 90 calendar days to ensure accuracy and shall update all documents within 30 calendar days following the implementation of changes.	Change to: The entity shall conduct a review of these documents at least annually to ensure accuracy and shall update all documents within 30 calendar days following the implementation of changes.
D1.3	Data Retention: The Responsible Entity shall keep documents specified in this standard for three calendar years and personnel risk assessment documents for the duration of employee employment. Contractor and service vendor records will be maintained for the duration of their engagement.	Recommendations: Change data retention from three years to two years. This is a general comment which pertains to all of these standards. Also delete the language after the 2 year data retention requirement because it is not appropriate for Electronic Security and pertains to a different section, i.e., personnel risk assessments. Change to: Data Retention: The Responsible Entity shall keep documents specified in this standard for two calendar years.
D.2.1.1.	Document(s) exist, but have not been updated with known changes within the 90 calendar day period and/or,	Change to: Document(s) exist, but have not been updated with known changes within the 30 calendar day period and/or,
D.2.1.2	Access to any Critical Cyber Asset was unmonitored for a period that does not exceed 24 hours.	Change to: Access to any Critical Cyber Asset was not logged for a period that does not exceed 24 hours.

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.

Section i.d.	Current Language	Recommendation – Change to
A.3.	…it is necessary to identify the physical security perimeter(s) (nearest six wall boundary)…	Recommend deleting the word "nearest". Change to: … it is necessary to identify the physical security perimeter(s) (six-wall boundary)…

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.

General Comments
Page numbering needs to be corrected
The terms Attended and Unattended need definitions. One question pertains to a backup site in a facility that is attended during normal business hours but un-attended at other times, is this site attended or unattended?

Section i.d.	Current Language	Recommendation – Change to
B.R1	The Responsible Entity shall document full detail of the test environment. The Responsible Entity shall verify that all changes to Critical Cyber Assets were successfully tested for known security vulnerabilities on a controlled non-production system prior to being rolled into production.	Recommend changing the reference from test environment to test plan. Also include the requirement that if a test environment is not available, a documented backup plan is required. Change to: The Responsible Entity shall document full detail of the test plan. The Responsible Entity shall verify that all changes to Critical Cyber Assets were successfully tested for known security vulnerabilities on a controlled non-production system prior to being rolled into production. If a separate test environment is not available, a documented backup plan is required.
B.R2.	The Responsible Entity shall not store test documentation, security procedures, and acceptance procedures at an unattended facility but at another secured attended facility.	Recommendation: Procedures need to be available at backup centers. Change to: If test documentation, security procedures, and acceptance procedures are needed and stored at unattended facilities such as backup sites, the materials must be kept in a secure/locked location.
B.R3.1	To the extent allowed by the existing technology, a password must consist of a combination of alpha, numeric, and special characters with a minimum of six characters.	Recommendation: Increase minimum password length from six to eight characters unless it is not supported. Change to: To the extent allowed by the existing technology, a password must consist of a combination of alpha, numeric, and special characters with a minimum of eight characters

B.R5.1	The Responsible Entity shall use integrity software on all Critical Cyber Assets that are connected to a wide-area network, the Internet, or to another device that is connected to a network (e.g., printer), to prevent, limit, and/or mitigate the introduction, exposure, and distribution of malicious software (mal-ware) to other Cyber Assets within the Electronic Security Perimeter.	Recommend: The requirements in this section should be qualified with the term "as applicable" due to diversity in software and operating systems utilized throughout the industry. Change to: The Responsible Entity shall use integrity software as applicable on all Critical Cyber Assets that are connected to a wide-area network, the Internet, or to another device that is connected to a network (e.g., printer), to prevent, limit, and/or mitigate the introduction, exposure, and distribution of malicious software (mal-ware) to other Cyber Assets within the Electronic Security Perimeter.
B. R8.2	The Responsible Entity shall ensure that controlled development or test environment for Cyber Assets residing in unattended facilities are not at the unattended facility.	Recommend: Clarification Change to: The Responsible Entity shall insure that controlled environments, which are used to develop or test Cyber Assets that are normally placed at unattended facilities, are not kept at the unattended facility."
		Recommend: Correct the numbering in this section from page 1 of 1 through page 10 of 10 to correct numbering.

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.

Section i.d.	Current Language	Recommendation – Change to
C.M2	The Responsible Entity shall retain records in addition to requirements…for three calendar years.	Change the data retention from 3 years to 2 years throughout the document. This is one of the general comments, which pertain to all of the standards.
D.1.2	The Responsible Entity shall keep data for three (3) calendar years.	
D.1.3.	The Responsible Entity shall keep documents specified in this standard for three calendar years.	
D.1.4	The Responsible Entity shall keep all records related to Cyber Security Incidents for three calendar years.	
D.2.2.2	Records related to Cyber Security Incidents are not maintained for three years…	

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.

Section i.d.	Current Language	Recommendation – Change to
B.R.4	Recovery plan(s) and any updates or changes shall be communicated to personnel responsible for their operation or responsibility for such Critical Cyber Assets within seven (7) calendar days of development or modification.	Recommend: If the changes are administrative in nature and do not affect the actions which need to be taken by individuals, the 7 day time frame is unduly short. Recovery plan(s) and any updates or changes shall be communicated to personnel responsible for their operation or responsibility for such Critical Cyber Assets within thirty (30) calendar days of development or modification.
C.M4	The Responsible Entity shall conduct drills at least even three (3) years and keep attendance records to its Recovery Plan (s) training.	The Responsible Entity shall conduct drills annually and keep attendance records of its Recovery Plan (s) training.

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.

Page #1: Delete the references to self-certification in the Implementation Plan language.

Page #2: We were told that Control Centers would be required to be 'audibly compliant' by 1st quarter of 2006 with those requirements, which were "direct descendent" of Standard 1200. In many cases the Control Centers are expected to be audibly compliant by 1st quarter, but the increase in scope has significantly altered the requirements in CIP-002-1 through CIP-009-1 vs. Standard 1200. For the items listed below, where the scope has increased, we recommend that Control Areas should be given until 1st quarter of 2007 to be 'audibly compliant."

	1st Quarter 2006		Compliance Schedule for CIP-002-1 through CIP-009-1
	Control Center		Comment
CIP-002-1			
R1	AC	Parameters for List of Assets	This requirement is NOT a "direct descendent" of Standard 1200 requirements because the parameters for the requirement are significantly different from Standard 1200. (IROL's, etc.)
R2	AC	Routable protocol/dial up accessibility	This requirement is NOT a "direct descendent" of Standard 1200 requirements because the parameters for the requirement are significantly different from Standard 1200. Differentiations such as routable protocol and dial up accessibility do not exist in Standard 1200.
R4	AC	Approval of list of assets	This requirement is NOT a "direct descendent" of Standard 1200. Approval of the list by senior management is a new requirement.
CIP-003-1			
R2	AC	Categorize ALL information	This requirement is NOT a "direct descendent" of Standard 1200 and goes MUCH farther than Standard 1200. Categorizing ALL of the information regardless of media type, senior management involvement etc. are new requirements.
R3	AC	Roles & Responsibilities	This requirement is NOT a "direct descendent" of Standard 1200. Defining the roles and responsibilities of all parties involved is a new requirement.
R4	AC	Governance Documentation	This requirement is NOT a "direct descendent" of Standard 1200. Documenting a formalized governance process was not required in Standard 1200.
CIP-004-1			
R1	AC	Awareness Program	This requirement is NOT a "direct descendent" of Standard 1200. A separate "Awareness Program" was not required in Standard 1200.
CIP-005-1			
R1	AC	Electronic Perimeter	This requirement is NOT a "direct descendent" of Standard 1200. Because the scope of CIO-005 has been expanded to include access from sub

			stations and generation facilities, the electronic access requirements to the perimeter have been expanded.
R4	AC	Electronic Access Controls	This requirement is NOT a "direct descendent" of Standard 1200. Electronic Access controls to the EMS system will have to be created for substations and for generation facilities.
R5	AC	Monitoring Electronic Access.	This requirement is NOT a "direct descendent" of Standard 1200. Means to monitor access controls to the EMS system will have to be created for substations and for generation facilities.
R6	AC	Documentation	This requirement is NOT a "direct descendent" of Standard 1200. Because the scope of the new permanent standard has been significantly increased, much new documentation is now required over and above Standard 1200 requirements.
CIP-006-1			
R1	AC		
R2	AC	Access Controls following risk assessment	This requirement is NOT a "direct descendent" of Standard 1200. The generally accepted industry or government risk assessment procedure was not required in Standard 1200.
R5	AC	Maintenance & Testing Program	This requirement is NOT a "direct descendent" of Standard 1200. Maintenance and Testing program was not required in Standard 1200.
R6	AC	Documents	This requirement is NOT a "direct descendent" of Standard 1200. Because the scope of the permanent standard has been significantly increased over Standard 1200, additional documentation is required.
CIP-007-1			
R1	AC	Testing & Environment	This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as documenting full detail of the test environment were not part of Standard 1200. Separating requirements for attended vs. un-attended facilities were not part of Standard 1200.
R3	AC	Account & Password Mgt.	This requirement is NOT a "direct descendent" of Standard 1200. The requirements for password management such as strong passwords and the distinction between controls for unattended vs. attended facilities are new to the current version and did not appear in Standard 1200.
R4	AC	Security Patches	This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as the monthly review and the risk based assessment are new requirements in this standard and were not part of Standard 1200.
R5	AC	Integrity Software	This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as the monthly review and the formal change control process for integrity software were not part of Standard 1200.
R7	AC	System Logs	This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as the distinctions for managing logs at unattended facilities were not part of Standard 1200.
R8	AC	Change Control	This requirement is NOT a "direct descendent" of Standard 1200. The scope of the requirements for change control has been expanded over the requirements of Standard 1200. Specifics regarding the assets at unattended facilities were not part of Standard 1200.
R10	AC	Op. Status Monitoring	This requirement is NOT a "direct descendent" of Standard 1200. Operating Status monitoring and performance monitoring tools requirements have been significantly expanded over Standard 11200 requirements.
R11	AC	Backups & Recovery	This requirement is NOT a "direct descendent" of Standard 1200. Items such as the requirement that the backup must be stored in a remote locations and the requirement for annual tests to ensure recoverability are new to this standard.

CIP-008-1			
CIP-009-1			
R4	AC	Notification of changes	This is not a "direct descendent" of Standard 1200. There was no requirement to notify personnel of changes within 7 calendar days of the modification.
R5	AC	Recovery Plan Training	This is not a "direct descendent" of Standard 1200. Standard 1200 did not contain a requirement that all the testing mirror testing defined in current CIP-004 Personnel and Training.

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**
☐ **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.

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?

☒ Yes
☐ 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?

☐ 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 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

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.

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 comments in Question 3 above and Specific comments in attached.

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 comments in Question 3 above and Specific comments in attached

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 comments in Question 3 above and Specific comments in attached

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 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?

☐ 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 comments in Question 3 above and Specific comments in attached

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 comments in Question 3 above and Specific comments in attached

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 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?

☐ Yes

☒ 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 ful 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 previouly) 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.

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAC approves Standard 1300 SAR, draft 1 posting (July 1, 2003)
2. SAC approves Standard 1300 SAR, draft 2 posting (December 1, 2003) 3. SAC appoints Standard 1300 Drafting Team (June 23, 2004) 4. Drafting Team posts draft 1 for comment (September 15, 2004)
5. Drafting Team posts draft 2 of Standard CIP–002–1 (Draft 1, Std 1300, section 1302) (January 17, 2005)

Description of Current Draft:

The current draft reformats Standard 1300, section 1302 into the new NERC Standards format and is to be posted for a 30-day posting period for public review and comment. This draft includes revisions based on public comments received during the posting of Draft 1.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Review comments to draft 2 and revise as needed	February 17, 2005 –March 15, 2005
2. Post Draft 3 for 45-day public comment period	March 15, 2005– April 30, 2005
3. Post Final Draft for 30-day public review, solicit Ballot Body	June 1–30, 2005
4. First ballot of Standard CIP–002–1	July 1–10, 2005
5. Respond to comments, post for recirculation ballot	July 21–31, 2005
6. 30-day posting before board adoption	August 1–31, 2005
7. Board adopts Standard CIP–002–1	September 1, 2005
8. Effective date	October 1, 2005

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data associated with bulk electric system assets.

Critical Asset: 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.

Cyber 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.

Electronic Security Perimeter: 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.

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.

Critical Cyber Assets: Those Cyber Assets essential to the reliable operation of Critical Assets.

Introduction 1. Title: Cyber Security — Critical Cyber Assets 2. Number: CIP–002–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. Business and operational demands for managing and maintaining 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 Responsible Entities identify and protect critical Cyber Assets that support the reliable operation of the bulk electric system. The Critical Assets are identified by the application of a risk-based assessment procedure on the operation of the interconnected bulk electric system. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service provider 4.5.Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. 5. (Proposed) Effective Date: October 1, 2005 Requirements R1.1. Responsible Entities shall identify their Critical Assets using their preferred risk-based assessment. A list	

of Critical Assets is then the basis to identify a list of associated critical Cyber Assets that must be protected by this standard. R1.2. Critical Assets: The Responsible Entity shall identify its Critical Assets. For the purpose of this standard the list of Critical Assets consists of those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a detrimental impact on the reliability or operability of the electric grid and critical operating functions and tasks affecting the interconnected bulk electric system such as, but not limited to: monitoring and control, load and frequency control, emergency actions, contingency analysis, special protection systems, power plant control, substation control and real-time information exchange. Those Critical Assets include the following: R1.3. Control centers and backup control centers performing the functions of a Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generation Owner, Generation Operator and Load Serving Entities. R1.4. Systems, equipment and facilities critical to operating functions and tasks supporting control centers and backup control centers such as telemetering, monitoring and control, automatic generation control, real-time power system modeling and real-time inter-utility data exchange. R1.5. Transmission substations associated with elements monitored as Interconnection Reliability Operating Limits (IROL) R1.6. Generating resources under control of a common system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. R1.7. Generation control centers having control of generating resources that when summed meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. R1.8. Systems, equipment and facilities critical to System Restoration, including Blackstart generators and substations associated with transmission lines used for initial system restoration. R1.9. Systems, equipment and facilities critical to automatic load shedding under control of a common system capable of load shedding 300 MW or greater. R1.10. Special Protection Systems whose misoperation can negatively affect elements associated with an IROL.	

R1.11. Additional Critical Assets: The Responsible Entity shall utilize a risk-based assessment to identify any additional Critical Assets. The risk-based assessment documentation must include a description of the assessment including the determining criteria and evaluation procedure. R1.12. The Responsible Entity shall identify the critical Cyber Assets associated with each Critical Asset listed in section R1. For the purpose of this standard, Critical Cyber Assets will be limited to those Cyber Assets having the following characteristics: R1.13. The Cyber Asset uses a routable protocol, or R1.14. The Cyber Asset is dial-up accessible. R1.15. Dial-up accessible Critical Cyber Assets which do not use a routable protocol require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter R1.16. Any other Cyber Asset within the same Electronic Security Perimeter as identified Critical Cyber Assets must be protected to ensure the security of the Critical Cyber Assets. R1.17. A member of senior management must approve the list of Critical Assets and the list of Critical Cyber Assets. C. Measures M1. The Responsible Entity shall maintain its approved list of Critical Assets as identified in R1. M2. The Responsible Entity shall maintain documentation depicting the risk-based assessment used to identify its Critical Assets in R1. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure. M3. The Responsible Entity shall maintain its approved list of Critical Cyber Assets as identified under Requirement R2 and all other Cyber Assets as identified under Requirement R3. M4. The Responsible Entity shall review, and as necessary, update the documentation referenced in M1, M2, and M3 at least annually, or within 30 calendar days of the addition of, removal of, or modification to any Critical Asset or critical Cyber Asset. M5. A signed and dated record of the senior management officer's approval of the list of Critical Assets must be maintained. M6. A signed and dated record of the senior management officer's approval of the list of Critical Cyber Assets must be maintained.	

D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe Verify annually that necessary updates were made within 30 calendar days of asset additions, deletions or modifications. The performance-reset period shall be one (1) calendar year. The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. 1.3. Data Retention The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.3.1 Documentation of the approved list of Critical Assets, 1.3.2. Documentation depicting the risk-based methodology used to identify its Critical Assets. The document or set of documents shall include a description of the methodology including the determining criteria and evaluation procedure. 1.3.3. Documentation of approved list of Critical Cyber Assets, and 1.3.4 Documentation of the senior management official's approval of both the Critical Asset list and the critical Cyber Asset list. 1.4 Additional Compliance Information: Not Specified Levels of Non-Compliance Level 1: The required documents exist, but have been updated with known changes within thirty (30) calendar days. Level 2: The required documents exist, but have not been approved, updated or reviewed in the last calendar year. Level 3: One or more document(s) missing. Level 4: No Documents exist. E. Regional Differences 1. None Version History	in the "Requirements" section of the Standard.

Introduction 1. Title: Cyber Security Management controls 2. Number: CIP–003–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. 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. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2.balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. 5. (Proposed) Effective Date: October 1, 2005 B. Requirements	
R1. 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 controls. R2. The Responsible Entity shall document and implement a program for the protection of critical information associated with Critical Cyber Assets R1. The Responsible Entity shall identify all information, regardless of media type, related to the entities Critical Cyber Assets whose compromise could	Renumbering of these requirements is necessary.

impact the reliability and/or availability of the bulk electric system for which the entity is responsible. This includes 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.	The last sentence in "this" R1 should be deleted as it is redundant.
R2. The Responsible Entity shall categorize information related to Critical Cyber Assets to aid personnel with access to this information in determining what information can be disclosed to unauthorized personnel; as well as the relative sensitivity of information that should not be disclosed outside of the entity without proper authorization. R3. Responsible Entities must identify the information access controls related to Critical Cyber Assets based on classification level as defined by the individual entity. R3. The Responsible Entity shall assign a member of senior management with responsibility for leading and managing the entity's implementation and adherence of the cyber security standard. This person, or their designated delegate, must authorize any deviation or exception from the requirements of this standard. Any such deviation or exception and its authorization must be documented.	The words "from the requirements of this standard" should be replaced by "from the requirements of the NERC CIP series of standards".
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 categorized in Requirement R2 of this standard. R4. 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. This governance process must include: R4. 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 prior to the system being promoted to operate in a production environment.	This sentence is redundant and should be deleted: Roles and responsibilities shall also be defined for the access, use, and handling of critical information as identified and categorized in Requirement R2 of this standard.

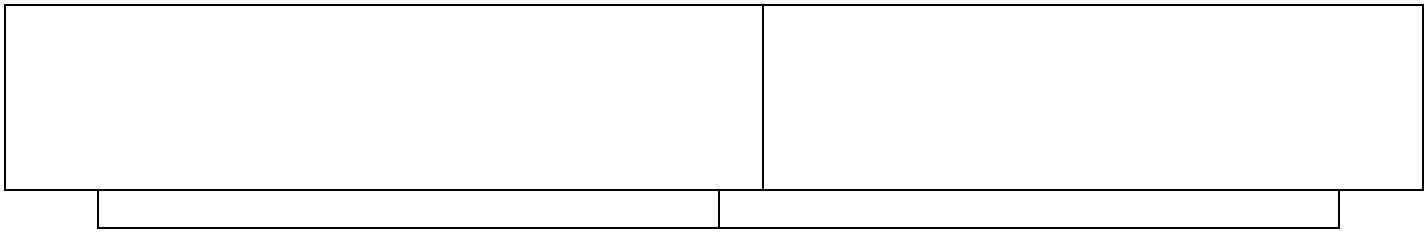
R5. The Responsible Entity shall establish a Change Control Process that provides a controlled environment for modifying all hardware and software for Critical Cyber Assets. The process should include change management procedures that at a minimum provide testing, modification audit trails, problem identification, a back out and recovery process should modifications fail, and ultimately ensure the overall integrity of the Critical Cyber Assets.	In R5, the phrase, "and ultimately ensure the overall integrity of the Critical Cyber Assets." is superfluous and should be deleted.
R5. The Responsible Entity shall institute and document a process for management of access to information associated with Critical Cyber Assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible.	This second instance of R5 is redundant and should be deleted as it is stated in R2.
R6. 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.	
R7. 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.	
R8. Responsible Entities shall define and document procedures to ensure that modification, suspension, or termination of user access to Critical Cyber Assets is accomplished in a time frame that ensures Critical Cyber Assets are not put at significant risk. All access revocations/changes must be authorized and documented.	
C. Measures	
M1. The Responsible Entity shall maintain its written cyber security policy stating the entity's commitment to protect Critical Cyber Assets.	
M2. The Responsible Entity shall review the cyber security policy as often as determined by the entity with a minimum review period not to exceed three years.	
M3. The Responsible Entity shall maintain documentation of any deviations or exemptions authorized by the current senior management official responsible for the cyber security program.	
M4. 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.	
M5. The Responsible Entity shall review the information security protection program at least	Remove sections M5 & M6 because they are scope creep and are covered in M7.

annually. M6. The Responsible Entity shall perform an assessment of the information security protection program to ensure compliance with the documented processes at least annually. M7. The Responsible Entity shall document the procedures used to secure the information that has been identified as critical cyber information according to the categorization level assigned to that information. M8. The Responsible Entity shall assess the critical cyber information identification and categorization procedures to ensure compliance with the documented processes at least annually. M9. The Responsible Entity shall maintain in its policy the defined roles and responsibilities for the handling of critical cyber information. M10. The current senior management official responsible for the cyber security program shall be identified by name, title, business phone, business address, and date of designation. M11. Changes to the current senior management official must be documented within 30 calendar days of the effective date. M12. The Responsible Entity shall review the roles and responsibilities of Critical Cyber Asset owners, custodians, and users at least annually. M13. 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. M13.1. The Responsible Entity shall have a defined process that maintains a current list of designated personnel responsible for authorizing systems suitable for the production environment. M13.2. 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. M14. The Responsible Entity shall have a defined process that maintains a current list of designated personnel responsible to authorize access to Critical Cyber Assets to reflect any change in status that affects the designated personnel's ability to authorize access to those Critical Cyber Assets.	Furthermore, it is unclear what is meant by, "information security protection program" as no requirement to establish such a program has been specified. Suggest "procedures" in M7 and M8 be changed to "controls". M 10 is too prescriptive. Name, Title and Date of Designation are adequate here. Maintaining the other information is too onerous and does not provide any value. M13.1 is a duplicate of M 12 M13.2 – There is not a requirement for Change Management in this standard. This text should be moved to the requirements section. M14 – Delete the phrase, "to reflect any change in status that affects the designated personnel's ability to authorize access to those Critical Cyber Assets" as it is redundant and confusing.

M15. The list of designated personnel responsible to authorize access to Critical Cyber Assets shall identify each designated person by name, title, business phone, business address, date of designation, and list of systems/applications they are responsible to authorize access for. The list of authorizers shall be reviewed for accuracy at least annually.	M15 – same comment as M10
M16. 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.	See general comment on establishing review frequency based on risk considerations rather than prescribing an arbitrary frequency.
M17. The Responsible Entity shall ensure that any authorized change in user access to Critical Cyber Assets is documented. Documentation shall be reviewed at least annually to ensure compliance with entities' documented access control processes. M18. The Responsible Entity shall review user access rights to confirm access is still required at least annually.	M17 and M18 should be deleted. They duplicate measures 4.1 and 4.2 of CIP 004.
D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.3.1 Written cyber security policy; 1.3.2 The name, title, business address, and business phone number of the current designated senior management official and the date of his or her designation. 1.3.3 Documentation of justification for any deviations or exemptions.	
1.3.4 Documented review results of this standard and mitigation strategies for the information security protection program. Review results will be kept for a minimum of 3 years.	1.3.4 – The need to establish a strategy has not been established as a requirement. If this is required, it should be moved to a requirements section and the term defined.
1.3.5 The list of approving authorities for access to critical cyber information assets. 1.3.6 The name(s) of the designated approving authority(s) responsible for authorizing systems suitable	

for production. 1.4. Additional Compliance Information: Not specified 2. Levels of Non Compliance 2.1 Level 1: 2.1.1 A current senior management official was not designated for less than 30 calendar days during a calendar year; or 2.1.2 A written cyber security policy exists but has not been reviewed in the last calendar year, or 2.1.3 Deviations from requirements or written cyber security policy are not documented within 30 calendar days of the deviation, or exception, or 2.1.4 An information security protection program exists but has not been reviewed in the last calendar year, or 2.1.5 Processes to protect information associated with Critical Cyber Assets have not been reviewed in the last calendar year. 2.2. Level 2: 2.2.1 A current senior management official was not designated for 30 or more calendar days, but less than 60 calendar days during a calendar year, or 2.2.2 Access to critical cyber information has not been assessed within the last calendar year, or 2.2.3 An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or 2.2.4 The list of designated personnel responsible to authorize access to critical cyber information has not been kept current and has not been reviewed within the last calendar year. 2.3. Level 3: 2.3.1 A current senior management official was not designated for 60 or more calendar days, but less than 90 calendar days during a calendar year, or 2.3.2 Deviations to policy are not documented or authorized by the current senior management official or delegate responsible for the cyber security program, or 2.3.3 Roles and/or responsibilities are not clearly and distinctly defined, or	
2.3.4 Controls for the testing and assessment of new or replacement systems and software patches/changes have not been identified or the list of designated approving authorities is not maintained and up to date. .4. Level 4: 2.4.1 A current senior management official was not designated for more than 90 calendar days during a calendar year; or 2.4.2 No cyber security policy exists, or	Failure to have a formal process to validate and promote systems to production (level 2 non-compliance) is equivalent to having no controls for testing and assessment of new or replacement systems (level 3 non-compliance).

2.4.3 No information security program exists, or 2.4.4 Roles and responsibilities have not been defined, or 2.4.5 Executive management has not been engaged in the cyber security program, or 2.4.6 No corporate governance program exists, or 2.4.7 Access authorizations have not been reviewed within the last calendar year, or 2.4.6 No corporate governance program exists, or 2.4.7 Access authorizations have not been reviewed within the last calendar year, or 2.4.8 There is no authorizing authority to validate systems that are to be promoted to production, or 2.4.9 The list of designated personnel responsible to authorize access to logical or physical Critical Cyber Assets does not exist or, 2.4.10 Access revocations/changes are not authorized and/or documented. E. Regional Differences 1. None Version History	2.4.7 is redundant and confusing. Failure to review access authorizations within a year is stated in 2.2.2 as leading to Level 2 non-compliance. Substantially greater care needs to be taken to ensure that the conditions leading to the various levels of non-compliance are a mutually exclusive set. This is not the case at present. This is very confusing and leads to an inability to understand which level an entity that is not in full compliance should certify to.



Personnel & Training

Introduction 1. Title: Cyber Security — Personnel & Training 2. Number: CIP–004–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. Personnel having authorized 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. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 5.(Proposed) Effective Date: October 1, 2005 B. Requirements Responsible Entity shall comply with the following requirements of this standard R1. Awareness — The Responsible Entity shall	

develop, maintain and document its security awareness program to ensure personnel subject to the standard receive on-going reinforcement in sound security practices. R2. Training — The Responsible Entity shall develop and maintain a company specific cyber security-training program that will be reviewed annually. This program will ensure that all personnel having authorized 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. R3. Records — The Responsible Entity shall prepare and maintain records to document training, awareness reinforcement, and background screening of all personnel having authorized access to Critical Cyber Assets and shall be provided for authorized inspection upon request. R4. Personnel Risk Assessment — The Responsible Entity shall subject all personnel having access to Critical Cyber Assets, including contractors and service vendors, to a documented company personnel risk assessment process prior to being granted authorized access to Critical Assets. C. Measures M1. 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: M1.1 Direct communications (e.g., emails, memos, computer based training, etc.); M1.2 Security reminders (e.g., posters, intranet, brochures, etc.); M1.3 Management support (e.g., presentations, all-hands meetings, etc.). M2. Training — The Responsible Entity shall develop and maintain a company-specific cyber security annual training program that includes, at a minimum, the following required items: M2.1 The cyber security policy; M2.2 Physical and elctronic access controls to Critical Cyber Assets; M2.3 The proper release of Critical Cyber Assetn	In R2, reword the last phrase to read, “and *management of* sensitive information surrounding these critical *cyber* assets.”

formation; M2.4 Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident. M3. Records — The Responsible Entity shall develop and maintain records to adequately document compliance with this standard. M3.1 The Responsible Entity shall maintain documentation of all personnel who have access to Critical Cyber Assets and the date of completion of their training. M3.2 The Responsible Entity shall maintain documentation that it has reviewed and updated its training program annually. M4. Personnel Risk Assessment — The Responsible Entity shall: M4.1 Maintain a list of all authorized personnel with access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets within the security perimeter(s). M4.2 Review the document referred to in measure M4.1 of this standard quarterly, and update the listing within seven calendar days of any substantive change of personnel. M4.3 Physical and electronic access revocation must be completed within 24 hours for any personnel terminated for cause and seven calendar days for any personnel who have a change in status where they are not allowed access to Critical Cyber Assets (e.g., resignation, suspension, transfer, requiring escorted access, etc.). M4.4 The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel prior to being granted authorized 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 identity verification (e.g., Social Security Number verification in the U.S.) 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. M4.5 The Responsible Entity shall ensure that adverse employment actions are consistent with the Responsible Entity's legal and human resources practices for hiring and retention of employees or	M2.4 – this is a new requirement and there is no matching requirement in this standard. M3.1 partially duplicates CIP-003 which speaks of requirements to maintain a list of personnel with access to critical cyber assets. Please remove the duplication as it can lead to confusion and duplication of effort. M4.1, 4.2, 4.3 are redundant as they are covered in CIP 003.

contractors. M4.6 The Responsible Entity shall conduct update screenings at least every five years or for cause.	M4.6 – this should refer to risk assessment as in R4 rather than screenings. The specification of an arbitrary 5 year update is not consistent with the requirement (R4) which states that a risk based approach shall be used.
D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years, and personnel risk assessment documents for the duration of employee employment. Contractor and service vendor records will be maintained for the duration of their engagement. 1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 Document(s) for compliance, training, awareness and screening; 1.4.2 Records of changes to access authorization lists verifying that changes were made within prescribed time frames; 1.4.3 Supporting documentation (e.g., checklists, access request/authorization documents); 1.4.4 Verification that quarterly and annual security awareness have been conducted; 1.4.5 Verification that personnel risk assessments are being conducted 2. Levels on Non-Compliance 2.1.1 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 2.1.2 One instance of personnel termination (employee, contractor or service provider) in which the access control list was not updated within 24 hours for cause or seven calendar days for other personnel changes; or 2.1.3 Personnel risk assessment program exists, but	1.3 establishes a new requirement (to retain personnel risk assessment documentation) for the duration of employment. This is inconsistent with 1.2 above. Requirements should not be established in the Compliance section of the standard.

not properly documented, or 2.1.4 Training program exists, but records of training either do not exist or reveal some key personnel were not trained as required; or 2.1.5 Awareness program exists, but not applied consistently or with the minimum of quarterly reinforcement. 2.2. Level 2: 2.2.1 Access control document(s) exist, but have not been updated or reviewed for more than six months but less than 12 months; or 2.2.2 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 seven calendar days or 24 hours if termination for cause; or 2.2.3 Training program exists, but doesn't not cover one of the specific items identified, or 2.2.4 Awareness program does not exist or is not implemented, or 2.2.5 Personnel risk assessment program exists, but is not consistently applied. 2.3. Level 3: 2.3.1 Access control list exists, but does not include service vendors; and contractors or 2.3.2 More than five instances of personnel termination (employee, contractor or service vendor) in which the access control list was not updated within seven business days or 24 hours if termination for cause; or 2.3.3 A personnel risk assessment program does not exist; or 2.3.4 Training documents exist, but do not cover two or more of the specified items. .4. Level 4: 2.4.1 Access control rights list does not exist; or 2.4.2 No training program exists addressing Critical Cyber Assets E. Regional Defences: None Version History:	The wording of 2.1.5 suggests that reinforcing the awareness program with the minimum quarterly frequency is indicative of level 1 non-compliance. This is inappropriate. The wording requires revision. 2.3.1 – Please include a matching requirement or delete this paragraph.

Introduction 1. Title: Cyber Security — Electronic Security 2. Number: CIP–005–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. 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. Applicability When used in within the text of this standard, “Responsible Entity” shall mean 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities.	The reference to “critical assets” should be changed to “Critical Cyber Assets”

Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1 5. (Proposed) Effective Date: October 1, 2005 B. Requirements	
R1. 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 nonCritical Cyber Assets within the defined Electronic Security Perimeter, these non-Critical Cyber Assets must comply with the requirements of this standard.	R1 – delete the first sentence. Repeating the term Electronic Security Perimeters is redundant as it is defined in the definitions section above. The rest of the paragraph is helpful but should not be contained in a requirements statement. Could be moved to the Electronic Security Perimeter definition or to an FAQ.
R2. Disabling unused Network Ports/Services: The Responsible Entity shall enable only those ports/services required for normal and emergency operations of Critical Cyber Assets. All other ports/services, including those used for testing purposes, must be disabled prior to production usage.	The wording of R2 fails to contemplate that having ports/services open for testing purposes may be required for an entity to "operate normally"
R3. The Responsible Entity shall secure dial-up modem connections. Where remote activation of dial-up connectivity via SCADA activated relays from the security or control center is technically feasible, dial-up equipment at unattended facilities shall be physically deactivated when not in approved use and remotely activated upon approval of activation. In all other cases, the Responsible Entity shall implement procedural or technical measures to ensure authenticity of the accessing device and/or application.	R3 – attended or unattended is irrelevant to security in this paragraph.
R4. Electronic Access Controls — The Responsible Entity shall implement the organizational, technical and procedural controls to permit or deny logical access at all	R4 – The phrase "and the Critical Cyber Assets within the Electronic Security Perimeter(s)." is confusing given that this

electronic access points to the Electronic Security Perimeter(s) and the Critical Cyber Assets within the Electronic Security Perimeter(s).	standard refers to Electronic Security Perimeter.
R4.1. These Electronic Security Perimeter access controls shall implement an access control model, which denies access by default unless explicit access permissions are specified.	R4.2 – Did y'all mean "remote access" or really "external interactive logical access"? Please clarify.
R4.2. 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. These strong procedural or technical measures shall include at least one of the following measures: Two-factor authentication Digital certificates Out-of-band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication One time use passwords	R4.2 – Suggest that indicating "Strong procedural or technical controls" is all that is required. R4.2 – this is too prescriptive for a standard. Would be better as a guideline because technology changes so rapidly.
In dial-up access, automatic number identification (ANI) to augment static user id and password authentication In dial-up access, call back to augment static user id and password authentication	R4.3 – should be removed. This is not a security measure but a legal support measure.
R4.3. Where technically feasible, electronic access control devices shall display an appropriate use banner upon interactive access attempts.	
R5. 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.	R5 – Monitoring authorized access should be replaced with logging authorized access.
R6. Documentation Review and Maintenance - The Responsible Entity shall ensure that all documentation by this standard reflect current configurations and processes. The entity shall conduct a review of these documents at least every 90 calendar days to ensure accuracy and shall update all documents within 30 calendar days following the implementation of changes.	R6. We could find no requirements for the creation of any documents in the "Requirements" section of this standard.
C. Measures M1. Electronic Security Perimeter — The Responsible	M1 establishes a new requirement to

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 entity shall ensure that all systems hosting Critical Cyber Assets have been identified and are within the Electronic Security Perimeter(s) documented. M2. Disabling unused Network Ports/Services: The Responsible Entity shall disable unused ports and services, and maintain documentation of status/configuration of all ports and services available on Critical Cyber Assets. M3. Dial-up Modems: M3.1 The Responsible Entity shall maintain a documented policy for securing dial-up modem connections to Critical Cyber Assets, and a record of an annual audit of all dial-up modem connections and ports against the policy and documented configuration. M3.2 The documentation shall verify that the Responsible Entity has taken the appropriate actions to secure dial-up access to all Critical Cyber Assets. M4. Electronic Access Controls M4.1 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). M4.2 For each control, the document or set of documents shall identify and describe, at a minimum, M1.4.2 The access request and authorization process implemented for that control, M2.4.2 The authentication methods used, and M3.4.2 A periodic review process for authorization rights, in accordance with management policies and controls defined in Standard CIP–003–1, and ongoing supporting documentation (e.g. access request and authorization documents, review checklists) verifying that these have been implemented. M5. Monitoring Electronic Access Control — The Responsible Entity shall maintain a document or set of documents to identify and describe: M5.1 Organizational, technical and procedural controls, including tools and procedures, for monitoring electronic (logical) access. M5.2 Supporting documents, including access records and logs, to verify that the tools and procedures are	document interconnected critical cyber assets within the security perimeter which is not reflected in the Requirements. M2, M3.1 and M3.2 establish new requirements which are not covered in the Requirements section. M5.2 – this appears to be the same as CIP 007, R7/M6.

functioning and being used as designed. M5.3 Processes, procedures and technical controls implemented to review 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. Documents that record these reviews shall be identified.	
M6. Documentation Review and Maintenance: — The Responsible Entity shall review the documents referenced in this standard at least annually and shall update these documents within 30 calendar days of the modification of the network or controls.	M6 contradicts R6 of this standard.
D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization	
1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep document revisions and security incident related data (such as unauthorized access reports) for three (3) 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 calendar days. The compliance monitor shall keep audit records for three years. The performance-reset period shall be one (1) calendar year.	1.2 there is an inconsistency with CIP 007 R 7.1.
1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years, and personnel risk assessment documents for the duration of employee employment. Contractor and service vendor records will be maintained for the duration of their engagement.	1.3 establishes a requirement (new to this standard) to retain personnel risk assessment documents. This requirement neither belongs in this section, nor does it belong in this standard. See also comments on CIP-004-1
1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 Document(s) for configuration, processes, tools and procedures as described in this standard; 1.4.2 Records of electronic access to Critical Cyber Assets (e.g. access logs, intrusion detection logs) 1.4.3 Supporting documentation (e.g. checklists, access request/authorization documents)	
1.4.4 Verification that necessary updates were made at least annually or within 90 calendar days of a modification	1.4.4 – Not consistent with requirements or measures.
2. Levels of Non-Compliance 2.1 Level 1:	

2.1.1 Document(s) exist, but have not been updated with known changes within the 90calendar day period and/or, 2.1.2 Access to any Critical Cyber Asset was unmonitored for a period that does not exceed 24 hours. 2.2. Level 2: 2.2.1 Document(s) exist, but have not been updated or reviewed in the last 12 months and/or, 2.2.2 Monitoring is in place, but a gap in the access records exists for one calendar day or more but for less than seven calendar days. 2.3. Level 3: 2.3.1 Electronic Security Perimeter: Document exists, but no verification that all critical assets are within the perimeter(s) described or, 2.3.2 Disabling Unused Network Ports/Services: Documents(s) exist, but a record of regular audits does not exist. 2.3.3 Electronic Access Controls: 2.3.3.1 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 2.3.3.2 Required documents exist, but records for some transactions are missing. 2.3.4 Electronic Access Monitoring: 2.3.4.1 Access not monitored to any Critical Cyber Asset for one week or more; or 2.3.4.2 Access records reveal access by personnel not approved on the access control list. 2.4. Level 4: 2.4.1 No document or no monitoring of access exists E. Regional Differences 1: None Version History	2.1.2 – This is not a realistic requirement as it deals mainly with the reliability and availability of monitoring systems. A better measure would be to verify that the monitoring processes are in place or the failure of a monitoring process was corrected within 24 hours. 2.3.2 – The word audit establishes a new requirement and has specific connotations. The word regular is un-measurable. A better expression would be “record of [time period] validations or assessments”. 2.3.3 – Delete this section because it is not measurable.

A. Introduction

1. Title: Cyber Security — Physical Security 2. Number: CIP–006–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. 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) (nearest six-wall boundary) within which these Cyber Assets reside.	Delete reference to the nearest six-wall boundary from the discussion on "Physical Security Perimeter", as the term "Physical Security Perimeter" is already defined. Alternatively, include the concept in the definition.
4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 5. (Proposed) Effective Date: October 1, 2005 Requirements R1. Security Plan: The Responsible Entity shall document its implementation of the following requirements in its physical security plan. R1.1. The identification of the Physical Security Perimeters(s) and the development of a defense strategy to protect the physical perimeter within	In R1, it is not clear what a physical security plan is. Better phraseology might be, "the Responsible Entity shall develop a physical security plan which shall document the following:". In R1.1 Please delete the phrase, "and the development of a defence strategy". It is unclear what is meant by the phrase and how one documents the implementation of the

which Critical Cyber Assets reside and all access points to these perimeter(s). R1.2. The implementation of the necessary measures to control access at all access points of these perimeter(s) and the Critical Assets within them. R1.3. Implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the Critical Cyber Assets. R2. 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) following an industry or government, generally accepted, risk assessment procedure. R3. 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. R4. Logging physical access: The Responsible Entity shall implement the technical and procedural mechanisms for logging physical access. R5. Maintenance and testing: The Responsible Entity shall implement a 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. R6. Documents for configuration, processes, tools, and procedures: The Responsible Entity shall maintain the specified documentation concerning its implementation of its Physical Security Plan. C. Measures M1. Documentation Review and Maintenance: The Responsible Entity shall review and update its physical security plan at least annually or within 90 days of modification to the perimeter or physical security methods. M2. 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). M3. Physical Access Controls: The Responsible Entity shall implement one or more of the following	development of a strategy. In R.1.2 Delete the phrase "and the critical assets within them". Controlling access to the Physical Security Perimeter will adequately control physical access to the Critical *Cyber* Assets and is consistent with R2 below In R1.3, Delete the phrase "and the critical assets within them. Monitoring access to the Physical Security Perimeter will adequately control physical access to the Critical *Cyber* Assets and is consistent with R2 below In R3, reword as. "for monitoring physical access *to the Physical Security Perimeter*….." In R4, reword as. "for loging physical access *to the Physical Security Perimeter*….." R6 – Duplicates R1. M1 – 90 days is not found in the requirements section. Replace "modification " by "significant modification" M3 – this is too prescriptive and does not respect changing technologies. The addition of

physical access methods: Card Key: A means of electronic access where the access rights of the cardholder are pre-defined in a computer database. Access rights may differ from one perimeter to another. Special Locks / Security Officers / Security Enclosure: These may include locks with non-reproducible keys, magnetic locks that must open remotely or by a Man-trap. Personnel responsible for controlling physical access 24 hours a day. These personnel shall reside on-site or at a central monitoring station. A cage/safe/cabinet system that controls physical access to the Critical Cyber Asset (for environments where the nearest six-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 all physical access point through the Physical Security Perimeter. The documentation shall identify and describe, at a minimum, the access request, authorization, and revocation process implemented for that control, and a periodic review process for verifying authorization rights, in accordance with management policies and controls defined in Standard CIP–003–1, and on-going supporting documentation. M4. 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 or point of facility access.	the words “or equivalent” would make this section better. The term “Security Officers” is confusing and should be changed to “Security Personnel”. The paragraph beginning “In addition” defines requirements that are redundant. The requirement to to maintain a physical security plan (R1 and maybe R6) and the requirement to keep it up to date as established in M1 effectively cover all of the ground that the text in this paragraph covers. In addition, requirements for maintaining documentation describing the access request, authorization, and review process are specified in CIP-003. There is no need to refer to those requirements in CIP-006. M4. This is redundant. These requirements are

Alarm Systems	A system that indicates a door or gate has been opened without authorization. These alarms must report back to a central monitoring station. Examples include card key alarm systems, 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 describe processes to review records for unauthorized access. The Responsible Entity shall have a process for creating unauthorized access reports.

M5. 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 Computerized Logging	A log book or sign-in sheet or other record of physical access accompanied by human observation or remote verification 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.

M6. Maintenance and testing of physical security systems: 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.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

Regional Reliability Organization

referred to in R1 and M1. Furthermore, this is too prescriptive and does not respect changing technologies. The addition of the words “or equivalent” would make this section better.

The paragraph beginning “In addition” defines requirements that are redundant. The requirement to maintain a physical security plan (R1 and maybe R6) and the requirement to keep it up to date as established in M1 effectively cover all of the ground that the text in this paragraph covers.

The paragraph beginning “In addition” defines requirements that are redundant – see similar comments on M3 and M4..

1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep document revisions and other security event-related data including unauthorized access reports for three calendar years. The Responsible Entity shall keep audit records for 90 days. The compliance monitor shall keep audit records for three years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years. 1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 The Physical Security Plan 1.4.2 Document(s) for configuration, processes, tools, and procedures as described in this standard. 1.4.3 Records of physical access to Critical Cyber Assets (e.g., manual access logs, automated access logs). 1.4.4 Supporting documentation (e.g., checklists, access request/authorization documents) 1.4.5 Verification that necessary updates were made at least annually or within 90 days of a modification. 2. Levels of Non-Compliance 2.1. Level 1: 2.1.1 Document(s) exist, but have not been updated or reviewed within the last 90 days and/or 2.1.2 Access control, monitoring and logging exists, but aggregate interruptions in system availability over a calendar year exist for more than seven days, but less than 1 month. 2.2. Level 2: 2.2.1 Document(s) exist, but have not been updated or reviewed in the last 6 months and/or 2.2.2 Access control, monitoring and logging exists, but aggregate interruptions in system availability over a calendar year exist for more than one month, but less than three months. 2.3. Level 3: 2.3.1 Document(s) exist, but have not been updated or reviewed in the last 12 months and/or 2.3.2 Access control, monitoring and logging exists, but aggregate interruptions in system availability	1.2 establishes requirements that appear to be inconsistent with M5. 1.3 If the documents referred to are video records, then the requirement for 3 years data storage is excessive, unless the documents relate to a significant security incident. 2.1.1 Not consistent with M1.

over a calendar year exist for more than three months. 2.4. Level 4: 2.4.1 No access control, or no monitoring, or no logging of access exists. E. Regional Differences 1. None Version History	2.2.1 Requires more stringent compliance than level 1 compliance, which would be perverse.

1. Title: Cyber Security — Systems Security Management 2. Number: CIP–007–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. A System Security Management Program is necessary to minimize or prevent the risk of failure or compromise from misuse or malicious cyber activity. 4. Applicability When used within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. While there are significant differences between attended and unattended facilities that contain Critical Cyber Assets, the requirements below will apply to both unless specifically differentiated. R1. Test Procedures — Attended Facilities: The Responsible Entity shall use documented information security test procedures to augment functional test and acceptance procedures for all new systems and significant changes to existing	This standard is a prime example of the need for a technical writer's review of the standards. It is much more prescriptive than the rest and demonstrates the lack of homogeneity across the standards. R1 – Delete. This requirement is well covered in CIP 003, R4 and R5

critical cyber security assets. The Responsible Entity shall ensure that significant changes include but are not limited to security patches, cumulative service packs, new releases, 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 non-production environment. All testing shall be performed in a manner that precludes adversely affecting the production system and operation. The Responsible Entity shall document full detail of the test environment. The Responsible Entity shall verify that all changes to Critical Cyber Assets were successfully tested for known security vulnerabilities prior to being rolled into production, on a controlled non-production system.	The last sentence of R1 is redundant given the preceeding two paragraphs. The need for the requirement as stated is unclear. The second paragraph above states that tests are required to mitigate risks from known vulnerabilities. If the vulnerabilitiy is known, either a patch exists or it does not. If a patch does not exist, testing will surely reveal a vulnerabilitity, and the Responsible Entity is no further ahead. If a patch does exist, the only test that is necessary is to establish that the patch has been installed. Furthermore, testing on a "controlled, non-production system, is not always possible or practical. In many cases it may be necessary to roll patches out onto a small subset of the production environment, assess impact, and then decide whether to proceed with more complete patch roll-out or whether to withdraw the
R2. Test Procedures – Unattended Facilities: The Responsible Entity shall not store test documentation, security procedures, and acceptance procedures at an unattended facility but at another secured attended facility. The Responsible Entity shall conduct security test procedures for Critical Cyber Assets at the unattended facility on a controlled non-production environment located at another secure attended facility.	R2 – Delete. This requirement is well covered in CIP 003, R4 and R5 The need to preclude storage of documentation at an unattended site is unclear. Storage of documentation at a suitably secured unattended site should not be precluded, and indeed, can be an important part of a disaster recovery plan.. As worded, this requirement precludes remote testing. Suitably configured remote testing can

	be done securely, and should not be precluded. It is not always possible or practical to conduct testing on a non-production environment The meaning of the term "unattended facilities" is not clear. Does this include unmanned facilities which are subject to 24x7 monitoring to which personnel can be quickly dispatched if necessary?
R3. Account and Password Management: The Responsible Entity shall 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 shall establish, implement, and document end user account (administrator, system, and individual) management that include but are not limited to: R3.1. Strong Passwords: In the absence of more sophisticated authentication methods that are stronger than passwords and don't require a password, (e.g., multi-factor access controls, certificates, or bio-metric), the Responsible Entity shall use accounts that have a strong password. For example, a password consisting of a combination of alpha, numeric, and special characters with a minimum of six characters to the extent allowed by the existing technology. Passwords shall be changed periodically per a risk-based frequency to reduce the risk of password cracking. R3.2. Generic Account Management – Attended: The Responsible Entity shall have a process for managing factory default accounts, e.g., administrator or guest. The process shall include the removal, disabling, or renaming of these accounts where possible. For those accounts that must remain, passwords shall be changed prior to putting any system into service. Where technically supported, individual accounts shall be used (in contrast to a group account). Where individual accounts are not supported, the Responsible Entity shall have a policy for managing the appropriate use of group accounts that limits access to only	R3 – use "account management" instead of "establish an account password management program" R3 – "by compromised account passwords" should be struck as unnecessary. R3 – "that include but are not limited to:" should say "that must meet at a minimum: In R3.1, it is inappropriate to have "For example" text in a requirement. This would be better included in the FAQ. The concept of "strong password" is vague and will change over time. This standard fails to define the term in a way that is meaningful and lasting. 'Strong passwords" should be used where permitted by the existing technology.

those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of staff changes, e.g., change in assignment or exit. R3.3. Generic Account Management – Unattended: For unattended facilities, the Responsible Entity shall ensure the physical access to Cyber Assets by approved users is authorized by a control or security center operator on an instance-by-instance basis. R3.4. Access Reviews – Attended: The Responsible Entity shall ensure a designated approver reviews access to Critical Cyber Assets, e.g., computer and/or network accounts and access R3.5. Access Reviews — Unattended: The Responsible Entity shall maintain and periodically review records of approved physical access and the cyber related work performed on Cyber Assets at unattended facilities. R3.6. Acceptable Use: The Responsible Entity shall have a policy implemented to manage the scope	R3.3 is covered in CIP 006. It should not be necessary for a human operator to approve physical access to an unattended facility on an instance by instance basis. Suitably configured automated access controls provide sufficient assurance that only authorized personnel can enter. R3.4 and R3.5 are covered by CIP 003, 005 and 006. Specification of access control and monitoring requirements in multiple standards is either redundant or leads to contradiction and confusion,
R3.5. Access Reviews — Unattended: The Responsible Entity shall maintain and periodically review records of approved physical access and the cyber related work performed on Cyber Assets at unattended facilities. R3.6. Acceptable Use: The Responsible Entity shall have a policy implemented to manage the scope and acceptable use of the administrator and other generic account privileges for both attended and unattended facilities. The policy shall support a compliance 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. R4. Security Patch Management: The Responsible Entity shall establish a formal security patch management program for tracking, evaluating, testing, and installation of applicable security patches and upgrades to critical cyber security assets. R4.1. The Responsible Entity shall evaluate all patches and upgrades for applicability to the individual situation, e.g. using a risk based	R 4 – “critical cyber security assets.” Security should be deleted. R4.1 – Should read “all relevant patches” R4.2 & R4.3 – this requirement is too

assessment, so as to avoid un-necessary and excessive patching. R4.2. The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch. R4.3. In the case where installation of the patch is not possible, the Responsible Entity shall use and document a compensating measure(s).	prescriptive. A better requirement would be for the company to have a patch management policy and procedure based on its own environment.
R5. Integrity Software R5.1. The Responsible Entity shall use Integrity Software on all Critical Cyber Assets that are connected to a wide-area network, the Internet, or to another device that is connected to a network (e.g., printer), to prevent, limit, and/or mitigate the introduction, exposure and distribution of malicious software (malware) to other Cyber Assets within the Electronic Security Perimeter.	R5.1 – The term "Integrity Software" is confusing, and should be defined. In addition, this section is unclear and would be better if written as follows: "The Responsible Entity shall use means to monitor and protect the integrity of data including software associated with critical cyber assets e.g.: technology, processes/procedures, software." to prevent, limit, and/or mitigate the introduction, exposure and distribution of malicious software (malware) to other Cyber Assets within the Electronic Security Perimeter.
R5.2. The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the Integrity Software implementation and upgrades.	R5.2 – The need to perform a monthly review of "integrity software available" is unclear and appears to be far too prescriptive. Is the intent really to reviw monthly which new sotware has hit the market? The requirement for formal change control should be deleted as it is covered elsewhere.
R5.3. In the case where integrity software is not used, e.g., operational incompatibility or not available for a particular computer platform, the Responsible Entity shall use and document a compensating measure(s). R5.4. Where repetitious application of software updates are necessary, such as at unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of mal-ware.	R 5.3 correctly contemplates that "integrity software" may not be available for all platforms. Requirement R5.1 should be reworded accordingly, since its current wording would lead to non-compliance in cases where integrity software is not available. In R5.4, the use of the word "repetitious" is confusing, as is the reference to unattended facilities. Suggest possible rewording to, "Where remote installation of software updates is required, the Responsible Entity shall ensure the integrity of the software being installed prior

	to initiating remote installation in order to prevent manual dissemination of mal-ware.
R6. Identification of Vulnerabilities and Responses R6.1. The Responsible Entity shall perform a vulnerability assessment at least annually that includes: R6.1.1. A diagnostic review of the access points to the Electronic Security Perimeter R6.1.2. Scanning for open ports/services and modems	In R6, the required frequency and scope of vulnerability assessments should be established by the responsible entity based on a risk assessment, rather than being prescribed in the standard.
R6.1.3. Factory default accounts R6.1.4. Security patch and anti-virus version levels	Requirements 6.1.3 and 6.1.4 lack verbs.
R6.2. The Responsible Entity shall implement a documented management action plan to remediate vulnerabilities and shortcomings, if any, identified in the assessment.	
R6.3. For unattended facilities that contain Critical Cyber Assets, the Responsible Entity shall perform a limited vulnerability assessment prior to each upgrade as possible given the technical capability of the Cyber Assets.	The intent of requirement R6.3 is unclear. It is not feasible or necessary to perform vulnerability assessments for an entire unattended facility at the same frequency as software is updated and patches are applied.
R7. Retention of Systems Logs: Using monitoring systems and/or procedures either internal and/or external to Critical Cyber Assets, the Responsible Entity shall ensure it is possible to create an audit trail from logs of security-related events affecting the Critical Cyber Assets. The Responsible Entity must determine its own logging strategy to fulfill the requirement. R7.1. The Responsible Entity shall retain said log data for a period of ninety (90) calendar 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) calendar years in an exportable format, for possible use in further event analysis. R7.2. In lieu of automatically generated logs at unattended facilities, the Responsible Entity shall collect and retain the physical access and change records of users at each approved access session, or at a minimum annually.	R7 – The last sentence gives the entities the responsibility to determine their own logging strategy but R7.1 and R7.2 are contrary and prescriptive and should be deleted.
R8. Change Control and Configuration Management R8.1. The Responsible Entity shall establish a Change Control Process that provides a controlled environment for modifying all hardware and	R8 – Should be deleted as it is well covered in CIP 003.

software for Critical Cyber Assets. The process shall include change management procedures that at a minimum provide testing, modification audit trails, problem identification, a back out and recovery process shall modifications fail, and ultimately ensure the overall integrity of the Critical Cyber Assets. R8.2. The Responsible Entity shall ensure the controlled development or test environment for Cyber Assets residing in unattended facilities are not at the unattended facility. The Change Control Process for Cyber Assets at unattended facilities shall prevent the inadvertent dissemination of faulty or compromised software to multiple unattended sites.	
R9. Disabling Unused Host Ports/Services: The Responsible Entity shall enable only those ports/services required for normal and emergency operations of Critical Cyber Assets. All other ports/services, including those used for testing purposes, must be disabled prior to production usage.	R9 – Should be deleted as it is well covered in CIP 005.
R10. Operating Status Monitoring Tools: For maintaining situational awareness, the Responsible Entity shall ensure Critical Cyber Assets used for operating critical infrastructure are included or augmented with automated and/or process tools, where practical, to monitor operating state, utilization and performance, and cyber security events experienced by the Critical Cyber Assets themselves, and issue alarms for specified indications, as implemented. For Critical Cyber Assets in use at unattended facilities that are not capable of being electronically monitored remotely, the Responsible Entity shall review and document pertinent metrics manually during routine access/service to said equipment	In R10, pertinent to what? Pertinent to current operating status, Outage rates, utilization, others?
R11. Back up and Recovery: The Responsible Entity shall back up on a regular basis, where technically feasible, information and data that is resident or required by Cyber Assets used to manage critical electric infrastructure. The back up must be stored in a remote or hardened site some distance away from the Critical Cyber Assets. Information stored on computer media for a prolonged period of time shall be tested at least	R11 – The last sentence “For unattended facilities, back-up and recovery materials can be effectively tested at central test facility and shall not be tested on site.” should be removed and the rest of this section moved to CIP 009. The reference to “critical assets used to manage critical electric infrastructure” should be a reference to critical cyber assets. Delete the

annually to ensure that the information is recoverable. For unattended facilities, back-up and recovery materials can be effectively tested at central test facility and shall not be tested on site. C. Measures M1. Test Procedures: For all Critical Cyber Assets, the Responsible Entity shall maintain records of test procedures, results, and acceptance of successful completion.	words “at least annually” from the third sentence. The need for the final sentence is unclear. The sentence should be deleted.
M2. Account and Password Management: The Responsible Entity shall maintain a documented password policy and record of semi-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. Review access permissions within 24 hours for any personnel terminated for cause and seven calendar days for any personnel who have a change in status where they are not allowed access to Critical Cyber Assets (e.g., resignation, suspension, transfer, requiring escorted access, etc.).	M2. – Remove “record of semi-annual audit of this policy” as is contrary to R3.1 and is overly prescriptive, particularly given the stated requirement that passwords should change on a frequency based on assessed risk. The requirement that all passwords comply with the policy in order to attain full compliance is not realistic. The measure should be that remedial measures are taken within 7 days for passwords found to be non-compliant
M3. 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, approval for installation, compensating measures, and installation date. M4. Integrity Software: The Responsible Entity’s change control documentation shall include a record of all integrity software installations including: M4.1 Version level actively in use M4.2 Installation date M4.3 Or provide documentation for other compensating measures taken M5. Identification of Vulnerabilities and Responses: M5.1 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. M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found. M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to	M3 - The reference to change control should be deleted as it is dealt with in CIP-003 In M1 to M10.3, Please align measurements to

address the potential vulnerabilities. M6. Retention of Logs: M6.1 The Responsible Entity shall maintain documentation that indexes location, content, and retention schedule of all log data captured from the Critical Cyber Assets. M6.2 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. M7. Change Control and Configuration Management M7.1 The Responsible Entity shall maintain documentation identifying the controls, including tools and procedures, for managing change to and testing of Critical Cyber Assets. M7.2 The documentation shall verify that all the Responsible Entity follows a methodical approach for managing change to their Critical Cyber Assets.	requirements. Measures should be directly related to the Requirement statements, and should not impose additional requirements for success.
M8. Disabling Unused Host Ports/Services: The Responsible Entity shall disable unused ports and services, and maintain documentation of status/configuration of all ports and services available on Critical Cyber Assets. M9. Operating Status Monitoring Tools: The Responsible Entity shall maintain documentation identifying organizational, technical, and procedural controls, including tools and procedures for monitoring operating state, utilization, and performance of Critical Cyber Assets.	M8 identifies redundant requirements. Change control is adequately addressed in CIP-003.
M10. Back-up and Recovery: M10.1 The Responsible Entity shall maintain documentation that index location, content, and retention schedule of all Critical Cyber Assets' information backup data and tapes. M10.2 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.	M10.1. Replace backup data and tapes with backup media.
M10.3 The documentation shall verify that the Responsible Entity is capable of recovering from the failure or compromise of Critical Cyber Asset. D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset	Delete M10.3 as it should be covered under CIP-009.

Timeframe The Responsible Entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years. 1.4. Additional Compliance Information The Responsible Entity shall make the following available for inspection by the compliance monitor upon request: 1.4.1 Document(s) for configuration, processes, tools and procedures as described in this standard. 1.4.2 System log files as described in measure M6. 1.4.3 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.). 2. Levels of Non-Compliance	
2.1. Level 1: Document(s) exist, but does not cover up to two of the specific items identified and/or the document has not been reviewed or updated in the last 12 months. 2.2. Level 2: Document(s) exist, but does not have three of the specific items identified and/or 2.2.1 A gap in the reviews for the following items exists: 2.2.1.1 Access Reviews (semi-annually for attended facilities, periodically for unattended facilities). 2.2.1.2 Security Patch Management (monthly) 2.2.1.3 Integrity Software (monthly) 2.2.2 Retention of system logs exists, but a gap of greater than three days but less than seven days exists. 2.3. Level 3:	Section 2.1 introduces a new requirement – that documentation be reviewed and updated within 12 months. If this is, indeed, a requirement, it should be specified in the Requirements section. For some documents (eg. policies or processes for reviewing factory accounts, or patch management process documentation) annual revision is not required.
2.3.1 Document(s) exist, but more than three of the items specified are not covered. 2.3.2 Test Procedures: Document(s) exist, but documentation verifying that changes to Critical Cyber Assets tested is incomplete or changes to Critical Cyber Assets were not tested. 2.3.3 Account and Password Management: Document(s) exist, but documentation verifying accounts and passwords comply with the policy	What are items 2.3.2 to 2.3.11 intended to mean? Are these the documents referred to in 2.3.1 or are they additional conditions which could lead to Level 3 certification? Are these logical Or or logical AND conditions?

does not exist. 2.3.4 Security Patch Management: Document exists, but records of security patch installations are incomplete. 2.3.5 Integrity Software: Documentation exists, but verification that all Critical Cyber Assets are being kept up to date on anti-virus software or that compensating measures are being taken does not exist. 2.3.6 Identification of Vulnerabilities and Responses: 2.3.6.1 Document exists, but annual vulnerability assessment was not completed and/or 2.3.6.2 Documentation verifying that the entity is taking appropriate actions to remediate potential vulnerabilities does not exist. 2.3.7 Retention of Logs (operator, application, intrusion detection): A gap in the logs of greater than 7 days exists. 2.3.8 Disabling Unused Host Ports/Services: Documents(s) exist, but a record of regular audits does not exist. 2.3.9 Change Control and Configuration Management: N/A 2.3.10 Operating Status Monitoring Tools: N/A 2.3.11 Backup and Recovery: Document exists, but record of annual restoration verification exercise does not exist. 2.4. Level 4: No Documentation exists E. Regional Differences 1. None Version History	

1. Title: Cyber Security — Incident Response Planning 2. Number: CIP–008–1 3. Purpose: This standard is intended to ensure that appropriate cyber 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. Security measures designed to protect Critical Cyber Assets from intrusion, disruption or other forms of compromise must be monitored on a continuous basis. This standard requires responsible entities to define the procedures that must be followed when Cyber Security Incidents are identified. This standard requires: Developing and maintaining of documented procedures, Classification of incidents, Actions to be taken, and Reporting of Incident. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. 4. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 4.1. Reliability Coordinator 4.2. Balancing Authority 4.3. Interchange Authority 4.4. Transmission Service Provider 4.5. Transmission Owner 4.6. Transmission Operator 4.7. Generator Owner 4.8. Generator Operator 4.9. Load Serving Entity 4.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP–002–1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard.	The references to "incidents" should say cyber security incidents.

(Proposed Effective Date: October 1, 2005 . Requirements R1. The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate and/or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items: R2. Incident Classification: The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents. R3. Cyber Security 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. R4. Cyber Security Incident Reporting: The Responsible Entity shall report all Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center ES ISAC in accordance with the Indications, Analysis & Warning Program (IAW) Standard Operating Procedure (SOP). The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. C. Measures M1. The Responsible Entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and Cyber Security Incident reporting requirements at least annually or within 90 calendar days of known changes M2. The Responsible Entity shall retain records in addition to requirements defined in Standard CIP-007-1, requirement R7 (Retention of Systems Logs) of Cyber Security Incidents for three calendar years. D. Compliance 1. Compliance Monitoring Process	In R1, replace the word, “accuracy” by “adequacy”. Measure M1 is worded poorly. The various documents may require periodic review, but surely that documentation does not need to define incident classification at least annually. As worded, M1 and M2 introduce new requirements that should be noted in the requirements section.

1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep documents specified in this standard for three calendar years. 1.4. Additional Compliance Information 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: 1.4.1 System and application log file entrie 1.4.2 Video, and/or physical access records, 1.4.3 Documented records of investigations and analysis performed, 1.4.4 Records of any action taken including any recovery actions initiated. 1.4.5 Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC. 2. Levels of Non-Compliance 2.1.Level 1 2.1.1 Documentation exists, but has not been updated with known changes within 90 calendar days. 2.2. Level 2: 2.2.1 Incident response documentation exists, but has not been updated or reviewed in the last 12 months and/or 2.2.2 Records related to Cyber Security Incidents are not maintained for three years or are incomplete. 2.3. Level 3: 2.3.1 Incident response documentation exists but is incomplete and/or 2.3.2 Cyber Security Incidents have occurred but were not reported to the ES ISAC 2.4. Level 4: No documentation exists. E. Regional Differences 1. None Version History	In 1.4.1, it should only be required to retain log file entries relevant to the specific cyber security incidents, not all logs. In 4.2, it should only be required to retain records where relevant to specific incidents In 1.4., the reference to all cyber security incidents is redundant given the rest of Section D1.4. 2.1.1 should read “Documentation necessary to show compliance with M1 exists, but has not been updated with known changes within 90 calendar days of known changes. In 2.2.1, it appears that the reference to “incident response documentation is actually a reference to the Cyber Security Incident Response **Plan** mentioned in R1. If so, the wording must be clarified, as otherwise the reference could be interpreted to be a reference to incident response records defined in Section C, item M2 and in Section D subsection 1.4 2.4 should be reworded as, “ a documented Cyber Security Incident Response Plan does not exist.”

1. Title:Cyber Security — Recovery Plans 2. Number: CIP–009–1 Purpose: This standard is intended to ensure that appropriate cyber 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. 3. Applicability When used in within the text of this standard, "Responsible Entity" shall mean: 3.1. Reliability Coordinator 3.2. Balancing Authority 3.3. Interchange Authority 3.4.Transmission Service Provider 3.5.Transmission Owner 3.6. Transmission Operator 3.7. Generator Owner 3.8. Generator Operator 3.9. Load Serving Entity 3.10. Nuclear facilities are regulated by the NRC or the Canadian Nuclear Safety Commission; therefore, compliance to the requirements of this standard will not apply to these facilities. Applicable entities that comply with Standard CIP-002-1 and as a result identify that they have no Critical Cyber Assets, are exempt from complying with this standard. Any reference in this Standard to Critical Cyber Assets applies to those assets identified through compliance with Standard CIP–002–1. (Proposed) Effective Date: October 1, 2005 Requirements R1. The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan(s) at least annually. R2. The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan. R3. The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that effects the protection of Critical Cyber Assets R4. Recovery plan(s) and any updates or changes shall be communicated to personnel responsible for their operation or responsibility for such Critical Cyber Asset within seven (7) calendar	Though it may seem self-evident, the standard should not take as a given that all entities share the same understanding of what is required in a viable, "Recovery Plan". This standard should define the term, or at least provide guidance as to what is intended. This is particularly important as the "levels of non-compliance" portion of the standard suggests mandatory contents of the recovery plan (such as "types of events that are necessary") without ever defining these. R1. Overly prescriptive. The minimum test frequency schedule should be based on a risk-based assessment and evidence kept that this testing frequency is respected. In R3, reword to state, "The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan".

days of development or modification. R5. The Responsible Entity shall develop training and awareness for its recovery plan(s) that follow the requirements set forth in Standard CIP–004–1 — Personnel and Training. C. Measures M1. The Responsible Entity shall document its Recovery Plan(s) and maintain records of all exercises or drills for at least three (3) years. M2. The Responsible Entity shall document its Recovery Plan(s) and maintain records of all exercises or drills for at least three (3) years. M3. The Responsible Entity shall review and update if needed, its response to events of varying duration and severity annually or as necessary. M4. The Responsible Entity shall review and update recovery plan(s) annually. M5. The Responsible Entity shall conduct drills at least every three (3) years and keep attendance records to its Recovery Plan(s) training D. Compliance 1. Compliance Monitoring Process 1.1. Compliance Monitoring Responsibility Regional Reliability Organization 1.2. Compliance Monitoring Period and Reset Timeframe The Responsible Entity shall make the documents described in this standard available for inspection by the compliance monitor upon request. The performance-reset period shall be one (1) calendar year. 1.3. Data Retention The Responsible Entity shall keep data for three calendar years. The compliance monitor shall keep audit records for three years. 1.4 Additional Compliance Information: Not Specified 2. Levels of Non-Compliance 2.1 Level 1: Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year. 2.2 Level 2: Recovery plan(s) have not been reviewed, exercised, or training performed. 2.3 Level 3: Recovery plan(s) address neither the type of events that are necessary nor	M1 and M2 should be merged. M3 and M4 are repetitive and should be merged. M4 contradicts R3. M5 is not consistent with R1 and needs to be clarified. 2. This compliance section will not work and should be revisited. For example, a plan that has not been reviewed will contradict both level 1 and level 2. An entity which neither updated its recovery plan in the past year, nor exercised it, nor included in it the types of “events that are necessary” could legitimately claim any of level 1, 2 or 3 non-compliance.

any specific roles and responsibilities. 2.4. Level 4L No recovery plan(s) exists. E. Regional Differences: None	Level 3 identifies a new requirement that should be identified in the requirements or measures section.

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:	**William J. Smith**		
Organization:	**Allegheny Power**		
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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Allegheny Power agrees with the definitions.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

R2.3 - This section doesn't adequately take into account the substation environment. If someone accesses the physical perimeter of a substation, they would be able to cause an outage if sufficiently motivated regardless of the kinds of cyber precautions undertaken. The reason for physically protecting critical cyber assets located at substations is to reduce the risk to other critical cyber assets. Allegheny Power acknowledges that physical access to a critical cyber asset may also put other critical cyber assets within the same local electronic security perimeter at risk. Given the access controls placed on electronic security perimeters, however, physical access to a critical cyber asset in one local electronic security perimeter does not create a significant risk to critical cyber assets in other local electronic security perimeters. The standard should recognize that an adequate electronic security perimeter, in certain physical environments, is sufficient in regards to protecting critical cyber assets. CIP-002-1 R2.3 should be modified as follows:
Critical Cyber Assets located at substations in which the local electronic security perimeter and its associated access points are completely contained within the substation control building require only an electronic security perimeter for the remote access without the associated physical security perimeter.
Requirements R1.1.1 through R1.1.9 are too prescriptive given the risk management approach to identifying critical cyber assets. They should be removed from the standard, and at most, be part of the FAQ as an answer to the question: What kinds of assets should I consider in my risk-based assessment?

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

General Comment – Confusion throughout this section in terms of understanding the difference between critical **information** about the Critical Cyber Asset (floor plans, etc.) vs. critical information emanating from the asset that is vulnerable to attack or acquisition by a hacker. Is the Standard asking us to categorize only the first type, or both? Allegheny Power believes the Standard's intent is to protect the information ABOUT the Critical Cyber Asset. Can you please clarify?

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

The purpose states that personnel having authorized access to Critical Cyber Assets are required to have a higher level of screening, etc… than personnel not provided access. This is too prescriptive given the entity's responsibility to develop its own training program.
M4.4 - Reference to company personnel is confusing and should be clarified. Appears to imply that only employees need to have a personnel risk assessment while the implication of the standard is that all personnel (employee, contractor, vendor) who have unescorted access to critical cyber assets must have a personnel risk assessment completed.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

R4.2 – The specific procedural and technical measures are too prescriptive and don't allow for future technology advances. They should be removed from the standard and placed in the FAQ document as examples of strong procedural and technical measures.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

R4 – The requirement of testing installed patches to ensure that they address a particular vulnerability is unreasonable. Vulnerabilities are most often identified by system vendors and may not be readily reproduced by system administrators. The reference to testing should be removed.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

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:	Jim Hansen	
Organization:	Seattle City Light	
Telephone:	206-706-0165	
Email:	james.hansen@seattle.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.

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.

1. The definition of Cyber Assets should be clarified to specifically exclude communication links connecting electronic perimeters. You could add the sentence: For the purpose of this standard, communications links connecting discrete electronic permiters are excluded. 2. The term 'Authorized Access' is used in CIP-004,005, and 006 but not defined here. Please add a definition for this term, and specifically describe whether it is intended to mean authorized electronic access, physical access, or both. This would help us understand the intent of these sections. It may be appropriate to spell out physical or electronic (or both) where appropriate in the standard. Training requirements for staff granted authorized physical access but not electronic access would be different than staff granted both for example. If this term means physical access, it would be helpful if exemptions (such as escorted visitors) or any special circumstances were identified.

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.

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.

1. CIP-002 to 009: Please tie measures to the pertinent requirements. This will assist us in insuring our compliance with these standards. 2. CIP-002 to 009: Please match compliance levels to specific measures. This will assist us in insuring we are aware of our current level of compliance. 3. CIP-002 to 009: There are overlaps and inconsistencies in some cases since different groups within the drafting team wrote these standards. For example in CIP-005 M5.1 Organizational controls are part of the measurement in this section but are already specified and measured in CIP-003. We recommend that a professional technical writer who can correct these problems in order to avoid causing confusion and unnecessary expense review these standards in total. 4. R1.1.1: The word 'performing' in the first sentence might be interpreted to mean 'actively performing'. This generally does not apply to backup control centers. If applied litterally, then backup control centers would not fall under this requirement unless they were actively performing one of the critical functions listed here. We believe the intent is to monitor these facilities 7x24 whether they are active or not. We suggest that the wording be changed to 'Control centers and backup control centers that, when operational, perform the functions of -' 5. R1.1.2: The use of the phrase 'such as', in this section, when taken together with the last sentence of R1.1 causes us some confusion. Do the authors intend to allow Responsible Entities to apply their risk-based assessment to identify which of these functions are critical to the operation of the control centers or is this a perscriptive list? If the latter, then the phrase 'such as' should be changed to 'shall include'. If not, then the phrase should be changed to 'for example' and it should be made clear that systems performing certain of these functions may not be critical to the operation of the control center. For example, control centers that are not transmission service providers may not need to include cyber assets running real-time power system modelling. Also, depending on the type of data being exchanged, inclusion of inter-utility data exchange may not be appropriate. 6. R1 and R2: It would helpful if a flow chart were provided that would provide the industry with a consistent approach to applying R1 and R2. 7. R1.1.3: The phrase associated with in the first sentence extends beyond equipment within the IROL transfer path. This requirement should state that anything not in the direct transfer path is excluded. Responsible Entities applying their risk-based assessment would identify anything outside the path that might impact the transfer path. 8. R1.1.7 Please tie the requirement to a specific criteria rather than 300 MW. 9. R2: A clarification was made during the conference call, and later confirmed during our WECC EMSWG meeting, that Cyber Assets using a routable protocol would not be considered Critical Cyber Assets if these assets were electronically isolated. In other words, there were no routable or dial-up electronic access points to the system. The requirements in this section do not state this however. The requirements need to be clarified to include this point. We suggest modifying R2.1 to state: The Cyber Asset uses a routable protocol for access from outside the electronic security perimeter. This will exclude power plants and substations that use a network of Cyber Assets to provide governor control, data acquisition, etc. but are connected outside their electronic perimeter by RTU protocol communications only. It would also exclude Cyber Assets in control centers and backup control centers that have no external electronic perimeter access points using a routable protocol or dial-up modem. 10. R4 Please clarify that senior management are not required to sign a detailed list of Critical Assets and Critical Cyber Assets. For example, we should be able to identify our control center and EMS system as critical assets and cyber assets respectively without providing

management with a detailed list of all of the critical equipment in each. 11. M5-6 should require annual review by senior staff. Signature and review on change would usually require daily or weekly review. 12. Compliance should be numbered in the same fashion as Requirementss (Rn) and Measures (Mn). example: R1.1, M1, C1.1.2. This would make it easier to refer to particular sections of the standard from documents and programs we develop for compliance. 13. Please remove the use of 'shall' in measures. 'Shall' should appear in the Requirements section only. For example in CIP-005 M1 – 'The Responsible Entity shall maintain' should be changed to 'The Responsible Entity maintains'.

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.

1. CIP-002 to 009: Please tie measures to the pertinent requirements. This will assist us in insuring our compliance with these standards. 2. CIP-002 to 009: Please match compliance levels to specific measures. This will assist us in insuring we are aware of our current level of compliance. 3. CIP-002 to 009: There are overlaps and inconsistencies in some cases since different groups within the drafting team wrote these standards. For example in CIP-005 M5.1 Organizational controls are part of the measurement in this section but are already specified and measured in CIP-003. We recommend that a professional technical writer who can correct these problems in order to avoid causing confusion and unnecessary expense review these standards in total. 4. M5-10: Is there a difference between the Cyber Security Program in M10 and the information security protection program in M5? We're getting confused between the Cyber Security Policy, the Cyber Security Program, information protection security program, Cyber Security Standard (mentioned in R2.3), etc. Ideally, we'd like the standard to contain easy to identify documents that we can uniquevicollay relate to between requirements, measures, and compliance. In general this standard is will written but we believe could be cleaned up in order to minimze confusion. 5. D 2.1.1: There is no way to avoid at least level 1 non compliance the way this is written. For instance, a Responsibility Entity with a senior management official designated 100% of the time meets the criteria of a senior management official was not designated for less than 30 calendar days. It should be recognized that staff may decide to leave and it may take several days to appoint someone as acting senior management, or appoint alternative senior management. We suggest that this be changed to 20 or more but less than 30.

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.

1. CIP-002 to 009: Please tie measures to the pertinent requirements. This will assist us in insuring our compliance with these standards. 2. CIP-002 to 009: Please match compliance levels to specific measures. This will assist us in insuring we are aware of our current level of compliance. 3. CIP-002 to 009: There are overlaps and inconsistencies in some cases since different groups within the drafting team wrote these standards. For example in CIP-005 M5.1 Organizational controls are part of the measurement in this section but are already specified and measured in CIP-003. We recommend that a professional technical writer who can correct these problems in order to avoid causing confusion and unnecessary expense review these standards in total. 4. Throughout this section the term ‘authorized access’ is used. It is particularly critical to us that this term be clarified (physical or electronic access or both) throughout this section as stated in CIP-002 comments. Please ensure that the use of this term matches the definition if it is added to definitions. 5. R4 and M4.4: Both contain the phrase 'prior to'. Please clarify how existing staff should be handled. We specifically do not want to prohibit existing staff from having access while we are performing the required assessments. 6. R1, M1 and D2.1.5 use the term 'reinforcement' however there is no suggestion within the standard of what would meet NERC's minimum standard of awareness reinforcement. In the measure, e-mails are listed for example without indicating what the content should be. It may have been the drafting team's intent to leave this up to the companies to apply, however, in the interest of ensuring that we comply with the intent, it would be ideal to either specifically state in the compliance section that the content of awareness communications is totally up to the company and any content guarantees compliance, or state specific minimum content.

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.

1. CIP-002 to 009: Please tie measures to the pertinent requirements. This will assist us in insuring our compliance with these standards. 2. CIP-002 to 009: Please match compliance levels to specific measures. This will assist us in insuring we are aware of our current level of compliance. 3. CIP-002 to 009: There are overlaps and inconsistencies in some cases since different groups within the drafting team wrote these standards. For example in CIP-005 M5.1 Organizational controls are part of the measurement in this section but are already specified and measured in CIP-003. We recommend that a professional technical writer who can correct these problems in order to avoid causing confusion and unnecessary expense review these standards in total. 4. Throughout this section the term 'authorized access' is used. It is particularly critical to us that this term be clarified (physical or electronic access or both) throughout this section as stated in CIP-002 comments. Please ensure that the use of this term matches the definition if it is added to definitions. 5. R1 - There is a variety of equipment and software typically used in electronic security perimeter access control. We believe that this is what was intended by the word 'logical' in this section. Can you state this more clearly and also ensure that associated measures and compliance levels incorporate the concept that the electronic access point can be this group of hardware and software used to secure the perimeter? In some cases, a single system may be used in more than one logical perimeter. For example, a router may be used to implement level 1 and 2 security and a variety of target machines may implement other levels. 6. Please remove the use of 'shall' in measures. 'Shall' should appear in the Requirements section only. For example, M1 – 'The Responsible Entity shall maintain' should be changed to 'The Responsible Entity maintains'. 7. R3 – 'unattended' usually has no bearing on securing and being aware of dial-in access. Should this second sentence read '…dial-up equipment shall be…' instead? 8. R4.2 - Should the word 'logical' in the first sentence be removed? 9. R4.2 The measures would be more clear if specific examples were included. 10. R5 Please include 'where technically feasible' as this is not always possible with existing systems. 11. R5 'Monitoring' implies active notification 7x24 when the events specified occur. In the case of Authorized Access, 'Logging' for audit purposes is important, however active notification is not. For unauthorized access attempts, (internally or at electronic perimeter(s)) active monitoring should be used. Please modify R5 to remove the requirement for monitoring authorized access. 12. R4 appears to be written with human access rather than software access to systems. Either can be 'interactive'. We have numerous interactions with specific computers using specific ports and protocols in various DMZ's outside of the electronic security perimeter of our EMS. A variety of methods are used to ensure that logins are never presented to anyone who could gain access to these systems outside the security perimeter and attempt unauthorized access. For example, a custom program receiving XML data delivered by another program across a normally unused port will reject any message that does not match the schema. While it is possible that someone could send a bogus XML data set complying with the schema. The damage would be limited to overwriting data that we could easily recover without threatening the reliability of the grid. The bullets in R4.2 do not cover any of these methods

however we believe they effectively limit access through our electronic security perimeter. Would you please split R4 into two requirements? One governing login access or access on defined ports, and the other programmatic access using specialized application software and interfaces on non-standard ports? Also, we believe that login access into a security perimeter should be encrypted when possible in order to ensure integrity and privacy. Networks outside of the perimeter could allow network traffic to be captured and viewed (exposing ip addresses, ports, user id and passwords) or even captured and modified in transit. 13. M4 and 5 also appear to have been written with login access in mind. If you split R4 into two requirements as requested above, can you also create separate measures? It is not necessary to log authorized programmatic access for example when thousands of transactions using different sessions are conducted each hour. 14. M1 Since this standard focuses on Cyber Security, the document described in M1 should be limited to contain only the Electronic Security Perimeter(s). The remainder of the sentence should be struck as it is outside the scope of this SAR, increases the cost of compliance, and does nothing to increase Cyber Security.

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.

1. In R1.1, the development of a defense strategy is dependent on what we are trying to physically defend against. For example, do the authors expect us to defend against casual access, unauthorized access via stealthy break-in, armed attack, aerial attack, explosion, terrorist assault teams? The measures do not refer to the defense strategy. Please state more specifically what is intended by this term. 2. In M4, regarding CCTV, what are the retention requirements for the video images?

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.

1. R1. In the second paragraph, please clarify that a non-production environment can be a production system that has been removed from production mode. This covers the case where non-production testing is not possible, on obsolete equipment for example, while achieving the goal of this section that is to ensure that testing is done safely. 2. R1 requires that we add another layer of tests to our existing test procedures, testing that a vendor's security patches for known security vulnerabilities work correctly. This causes us several problems. First, we have Solaris Unix systems from Sun. Sun tests their patches prior to releasing them (just as Microsoft is starting to do). We install necessary patches and then verify that the patches were installed correctly. We believe that the vendor should be held accountable for ensuring their security patches actually remove the vulnerability. If damages resulted from the patch not correcting the vulnerability, then the vendor would be held liable. Second, the cost of testing, in both human and financial resources is high. The new CIP standards are already creating a significant increase in resource utilization. We believe it would increase security for us to concentrate our resources on more critical security issues. Third, we do not believe that requiring the industry to test the security patches from vendors is effective in increasing security. Pressure is already placed on the vendors when the computer user industry finds that a security patch does not correct the problem. The operating system vendors have significantly increased their quality assurance testing as a result. If this requirement is not removed from the standard, we will be forced to vote 'no' on CIP-007. 3. R2 should be reworded. We suggest 'The Responsible Entity shall store test documentation, security procedures, and acceptance procedures for Critical Cyber Assets located at unattended facilities at a facility that is staffed 7x24. These documents must not be stored in a facility that is unattended at any time.' The second sentence should be removed since it would be possible to conduct security test procedures at the unattended facility simply by going there and conducing tests on a non-production environment located at that facility. The location of the non-production test environment is not something that should be specified. 4. R3. Entities should be required to 'perform account management to provide for access authentication…' or 'follow an account management program' rather than 'establish an account password management program'. Our program already exists and generic programs that meet these requirements are specified in standard security documents. 5. R3.1 change 'shall use accounts that have a strong password' to 'shall require and utilize strong passwords'. 6. R4.2 requires a monthly review of available security patches. Our vendor provides us with critical security alerts tat we respond to immediately. Our normal cycle for non-critical security patches is to review and download them every 6 months because it takes at least a month to adequately test our EMS applications. Given the other

measures employed on our electronic security perimeter in conjunction with the security alert program, we believe that a monthly review requirement is much too frequent. We request that this sentence be struck. 7. In R5, we take 'Integrity Software' to mean that set of software commonly called 'anti-virus software'. Is that the intent or is something else meant? In either case, can you clarify with specific examples or more common terminology? 8. R5.1 We believe the drafting team intended for this integrity software to be run on all Critical Cyber Assets within the Electronic Security Perimeter. However R5.1 does not clearly state this requirement. 9. R6.3 Doesn't this apply to all facilities? 10. R11. As stated in comment 3 above, the location of the non-production test environment is not something that should be specified in any of the CIP standards. Please remove the last sentence so that we can test at an unattended facility if we happen to have a test environment there. 11. M2 typo 'n'. 12. M10 in general should consider the use of other backup media. Specifically, 'backup data and tapes', and 'backup data', should be replaced with 'backup media'.

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.

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.

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.

We like the implementation timeline matrix however it is tied to a specific date rather than the date of adoption of the standard. If the standard isn't adopted until the fourth quarter of 2005, then we are left with very little time to implement. Implementation of the plan in anticipation of a successful ballot without a ratified standard to refer to would be probelmatic if not impossible. We would like the implementation plan to tie its first due date to 6 months after the standard is adopted with all other dates changing, as in a gant chart.

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:	Western Area Power Administration (contact Laurent Webber)	
Organization:	Western Area Power Administration	
Telephone:	720-962-7216	
Email:	webber@wapa.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.

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 a Cyber Security Incident is extensive enough to include common events such as port scans or automated programs that attack databases and Web servers. Having to report such events within 60 minutes is an unreasonable requirement. The definition of a Cyber Security Incident must be more clear as to what must be reported or the requirement must allow each company to define Cyber Security Incident in the context of their systems. Suggest adding the phrase (is known or suspected to be of malicious origin) to the definition.

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.
R1.1.1 through R1.1.8 eliminate the risk-based assessment process for much of the electrical system. They instead define an inclusion list regardless of the risk-based assessment process. These requirements belong more correctly in the potential impact definitions for each security objective in a risk-based assessment process such as that described in the NERC document FIPS-199. WAPA suggests that the words (Those Critical Assets include the following:) be removed from R1.1. R1.1.1 through R1.1.8 be moved to an Appendix A and that R1.1.9 be reworded to say: (Critical Assets: The Responsible Entity shall utilize a risk-based assessment to identify any Critical Assets. The risk-based assessment documentation must include a description of the assessment including the determining criteria and evaluation procedure. The risk-based assessment must include the potential impact definitions listed in Appendix A.

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.

It seems that the requirements defined in the NERC Permanent Cyber Security Standard have been drafted individually with no attempt to synchronize the requirements, measures, and compliance between individual CIPs and even within single CIPs. The overall effect of the "Critical Asset" definitions and the cascading requirements in following CIPs must be carefully considered in terms of the onerous burden in cost, personnel, resource allocation, and how these will affect overall reliability. As utilities are required to allocate resources to these onerous Permanent Cyber Security Standards, attention to other critical reliability functions will likely be reduced.
Purpose: The term (critical reliability control functions) is not well defined both in the sense of what is critical and what are the "reliability control functions".
R1.1.2, R1.1.7, R2.1, R2.2, and R3 seem to require that Critical Assets be defined down to the component level. This, combined with the requirements and measures listed in this and other CIPs (i.e. CIP-003-R3, CIP-005-M1 CIP-004-M3, CIP-004-M4, CIP-004-4.3, CIP-004-M4.4, CIP-005-R5, CIP-006, CIP-007-R5, CIP-009) creates a cascading requirement that would lead to huge lists of every device and result in an undue burden of documentation, testing, and tracking of individual Intelligent Electronic Devices (IEDs). It must be made clear that the listing of critical assets and critical cyber assets does not extend down to the component level.
WAPA suggests that R1.1 be revised to include the sentence, (Critical assets, critical cyber assets, and associated risk-based assessments, security plans and lists may be identified at a system level rather than a component level.)
R1.1.3 and R1.1.8 create a cascading effect with the requirement to include (elements monitored as…IROL) and (elements associated with an IROL.) These would be better worded as: [R1.1.3. Transmission substations in the direct electrical path of elements monitored as Interconnection Reliability Operating Limits (IROL)] and [R1.1.8. Special Protection Systems protecting elements monitored as IROL.]
R1.1.5 would include generating resources of about 2000 MW, and R1.1.7 includes load shedding of 300 MW. This seems to be a wide discrepancy in the amount of electrical power defined as critical.
R1.1.6 creates a cascading effect with the requirement to include (substations associated with transmission lines used for initial system restoration.) It would be better worded, (substations in the electrical path of transmission lines used for initial system restoration.)

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.

Combine CIP-003 and CIP-007 into one requirement for security controls, testing, and validation.
R2.1: The sentence, (This includes 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,) more correctly belongs as a definition of (Critical Information).
R2.1: The last sentence, (These documents must be protected as well,) seems unnecessary.
R4.1: It is not clear what the term (assessment) refers to here. The balance of the requirement refers only to testing. Remove the word assessment from the first sentence because it is not clear to what degree or how individual utilities are to assess new or replacement systems and software patches/changes. If this is meant to give utilities leeway in determining which patches are appropriate for installation, state so clearly.

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.

R1 and M1: The training requirements in R2 are adequate. As such R1 can be eliminated.
R1 and M1: Documenting and maintaining awareness training quarterly and retaining such records for 3 years is overkill. Awareness training is in place at WAPA, but retaining documentation of every employee's attendance, every email, every poster, and other awareness actions is overkill. Measures are important, but there should be a reasonable limit on the documentation requirements. The requirement to retain documentation of awareness training should be eliminated.
The measures of CIP-004 do not map well to the requirements; in fact the measures add additional requirements. One example is M4.6 which requires updated screenings every 5 years or for cause. This is not part of the requirements and should be eliminated.
M4.2: This measure implies additional requirements for communication and notification between companies that share access to Critical Cyber Assets (substations?). Such communication and notification of personnel actions between companies are not defined elsewhere. If it is the intention of this standard to require inter-company communications to this level, it must be clearly defined in the requirements.
M4.3: This measure adds requirements that are not defined in the requirements section. This additional requirement has a cascading effect because many interconnecting-company employees have authorized access to WAPA substations. The communications between interconnecting utilities has been primarily operations-based. This requirement will result in inter-utility administrative and personnel-based communications at a level never imagined. If this is the desired result it should be clearly stated. Otherwise it must be clearly stated in the requirements section that this applies only to employees of each Responsible Entity.
M4.4: The second sentence includes additional requirements (identity verification and 7 year criminal check) that are not listed in the requirements of this standard. These should be eliminated from the measures, since they are not part of the requirements or the compliance sections.

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.

R3 unattended facilities should be more clearly defined. An attended facility implies personnel on duty 24X7. A facility only (attended) 8 hours a day should still be defined as unattended.
R4.2 The term (external interactive logical access) should be better defined or explained.
R4.2: Since measures have special meaning in the CIPs, the last word before the bulleted list, (measures:), should be changed to (methods:).
R5 and M5: Requiring monitoring of authorized access for all Critical Cyber Assets within the perimeter creates a cascading and unreasonable requirement. If Critical Cyber Assets includes individual intelligent electronic devices, as it seems in CIP-002, the addition of thousands of expensive monitoring systems and log review and retention will crush most utilities. A reasonable requirement would be to apply this only to the electronic perimeter. In addition, clarify the 24x7 requirement. Does 24x7 apply to the log collection or does a person have to monitor 24x7?
R6: 90 day document reviews are overkill; annual review is adequate.
Compliance 1.4.1 seems too vague. It should more clearly list the documents to be made available for inspection.

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.

Purpose: Does the reference to a six-wall-boundary mean that this does not apply to outdoor assets, as found in substations and communication sites. Does it apply to the control buildings at substations and the radio building at communication sites? This will be very extensive, expensive, and cascading requirement to apply to all substations and microwave or fiber communication sites that are related to IROL. Again this relates to the definition of Critical Cyber Assets.

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.

Can we test one device after upgrade or must we test every device. For instance if a firmware upgrade is tested on one SEL relay, can identical devices be upgraded and rolled out to production without a full test based on the fact that complete testing was done on identical devices?
Changing passwords on thousands of devices is a daunting and near impossible task. Frequency of password changes may impact reliability and safety by denying access to critical support personnel during emergencies. For instance if a password change is done, but emergency response personnel forget to keep the new list with them at all times, they could be unable to access systems during emergencies.
R5 This section requiring integrity software should be eliminated for the following reasons. It is not clear what is meant by (Integrity Software). The term can be interpreted to be simple check-sum programs, anti-virus software, or sophisticated configuration management systems. This uncertainty, along with the potential problems detailed below, indicate that this requirement is poorly formulated and should be eliminated. Any software beyond what is needed for an application may negatively impact reliability. During times of intense activity some systems have been hard pressed to process information at a rate commensurate with real-time data acquisition, display, and system control. Integrity software can be resource intensive and may negatively impact reliability at the most critical times. This requirement needs more study of the potential impacts before it can be included in a NERC Standard.
R5.3: States that compensating measures shall be used, but without a clear understanding of what integrity software is, how can we know what adequate compensating measures are? Again, this is a poorly defined requirement and should be removed.

R6.1.2 should include scanning for WiFi devices including client probes and wireless access points.

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.

The definition of a Cyber Security Incident is extensive enough to include common events such as port scans or automated programs that attack databases and Web servers. Having to report such events within 60 minutes is an unreasonable requirement. The definition of a Cyber Security Incident must be more clear as to what must be reported or the requirement must allow each company to define Cyber Security Incident in the context of their systems. Suggest adding the phrase (is known or suspected to be of malicious origin) to the definition.

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.

R1: Must individual recovery plans exist and be exercised for every Critical Cyber Asset or is it adequate to have a single recovery plan for many similar assets? This is answered in the FAQ document.
R4: This seems to be a conflicting requirement with CIP-003 R1-R3. CIP-003 requires the protection of Recovery Plans, while CIP-009 R4 requires the distribution of Recovery Plans. While it may be possible to meet both requirements, it will require careful coordination between the protection procedures and the distribution procedures. Such inter-related requirements should be identified with references to each other and careful consideration of the coordination effects.

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.

The Auditably Compliant criteria for BA & RC Control Centers should be delayed another year. Substantial Compliance must be considered adequate for the first year. There is uncertainty as to the volume of documentation and the resources required to comply with the Cyber Security Standard. Given that the Standard is adopted by September 2005 the Implementation Plan calls for Control Centers to be Audit Compliant by 1st Quarter 2006. That is only 3 months and those months include some major holidays. It is absolutely unreasonable to allow only 3 months to evaluate the new Cyber Security Standard, assess compliance, define cyber and physical boundaries, install physical access controls, install physical monitoring devices, generate an undetermined amount of documentation, perform numerous background checks, choose and implement numerous cyber monitoring and auditing tools, and a multitude of other tasks.

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:	Howard 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.

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.

Cyber security incident. Remove "or was an attempt to compromise" from the definition. If this is kept in the definition, you need to quantify what is considered as an "attempt". A virus that is properly quarantined? A port scan on the outside that is properly blocked by the firewall?

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.

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.

Remove R1.1.9. You cover this with R1.1.1-8. Change reporting period for asset changes from 30 days to 90 days. Clarify weather senior manager needs to sign offon changes to assets. Because this standard has been expanded to include control areas in generating stations and transmission substations, the senior manager responsible will more than likely be multiple people, based on business area. This should be reflected in all parts of the standard. Why identify critical assets and manage them if they are not cyber and subject to this standard?

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.

This standard overlaps 007. Examples are R4.1,4.2, M13.1, 13.2. Combine or eliminate the redundancies. Remove section 2.3.4.

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.

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.

Do the same requirements apply if the dial-up connections are used to monitor equipment only and do not permit control or modification of equipment?

The Cyber Security Standard refers to Routable OSI-Open Systems Communications vs Non-Routable communications (Master/Slave communications). Will security at the Modem Dial-up Access point be needed if OSI communications i.e. DNP Networking is used?

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.

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.

Strong passwords, R3.1: minimum password length of 6 characters does not constitute a strong password. Security best practice and software vendors (even Microsoft) recomend a minimum of 8 characters. Keep alpha, numbers and special characters.Section R6.1, change verbage to annual vulnerability assessment to be conducted by a third party consultant..

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.

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.

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.

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 the 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**
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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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 devided 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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

———Critical Cyber Assets: In response to a previous comment the drafting team wrote: "For the purposes of this standard, criticality is defined by the magnitude of vulnerability . . ."

Although this makes clear that vulnerability is a key element of the concept of Critical Cyber Assets, the current definition does not contain even an implied reference to vulnerability. We believe that the term should be Vulnerable Critical Cyber Assets. The definition should be "those cyber assets essential to the reliable operation of Critical Assets that are most vulnerable to malicious attack as determined by a risk based assessment methodology". As currently defined the document is internally inconsistent: the definition itself refers only to the criticality of the assets, while the text of CIP002-1R2 focuses on vulnerability.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

———No. This draft applies an arbitrary criteria to identifying critical cyber assets (use of routable protocol). While this criteria is one relevant factor in conducting an assessment, it is far from the most important and its role in the standard as a determining factor prevents a utility from using a reasonable assessment methodology. CIP-002-1 gives this factor far too much weight and results in widely disparate systems being treated the same with respect to documentation and audit requirements. For example, a system which uses X.25 on an isolated link with no connection to an external network is treated exactly the same as a SCADA network based solely on the use of the public Internet without firewalls. These two networks have huge differences in risk profiles, but the current standard requires us to treat them the same. At the same time the standard excludes unencrypted radio SCADA transmissions which carry substantial security risks. The singling out of the use of a routable protocol also has the unfortunate impact of discouraging utilities from modernizing their communications infrastructure. The standard imposes a very expensive documentation and audit requirement on systems using routable protocols. The standard thus increases the cost of providing communication to more devices within substations and hence discourages utilities from implementing such systems. This is quite unfortunate because providing better information about system status is a key component of our efforts to improve system efficiency and reliability.

The standard should list the use of routable protocols along with other more important factors (such as whether the system is exposed to public networks and whether information could be monitored by a member of the general public) as factors to be included in an appropriate assessment methodology. If you are determined to include a rigid "routable protocol" criteria it should at least be amended to be "a routable protocol with exposure to a public network".

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

———No. The internal inconsistencies of the definition of Critical Cyber assets make it impractical to vote on at this time. We believe that the issue of the arbitrary criteria of the use of a routable protocol has been partially hidden by the inconsistent definitions of Critical Cyber Assets. We believe that it is a central issue of the document and that a ballot is inappropriate until a thorough discussion of this issue takes place. Requiring a substantially higher level of documentation and audit for systems using advanced protocols discourages system modernization and will lead to a delay in making more data and control available to system operators. Hence these standards which are intended to make our systems more secure may have the opposite effect.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

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.

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.

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:	Kenneth A. Goldsmith	
Organization:	Alliant Energy	
Telephone:	319-786-4167	
Email:	kengoldsmith@alliantenergy.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.

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.

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.

Under measures M3, should state 'shall maintain its approved list of Critical Cyber Assets as identified under Requirement R2 …

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.

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.

Remove overlapping requirements, measurements and non-compliance from CIP-003.
Requirements R4.1 is redundant with CIP-007 R1, R2
R4.2 is redundant with CIP-007 R8, R8.1 and R8.2.
R5.2 is redundant with CIP-007 R3.4.
M13.2 is redundant with CIP-007 M7, M7.1, M7.2
Levels of Non-Compliance 2.2.2, 2.2.3, 2.3.4, 2.4.7 and 2.4.8 are redundant with CIP007.
Measurements M13.1 - move to CIP007
Levels of non-compliance
2.3.3 clearly and distinctly defined - how do you measure
2.4.5 - Executive management engagement cannot be measured, remove from document

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.

Reword Levels of non-compliance 2.1.2, 2.2.2, 2.3.2 … in which the access was not revoked (rather than access control list updated)

2.1.4 The concept of "Key Personnel" is unclear. This term is not defined. This is the only place where the term is used

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.

Remove overlaps:

Requirement R2 is same as CIP007 R9

Measurement M2 same as CIP007 M8

Level of non-compliance 2.3.2 same as CIP007 2.3.8

R5 - should state …for monitoring unauthorized access (rather than authorized)

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.

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.

see CIP003 and CIP005 for redundancy

Level 3 compliance - much too severe. Suggest:
Remove 2.3.1 - same as 2.2
Move 2.3.2, 2.3.6.1, 2.3.7, 2.3.8, 2.3.11 to Level 2

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.

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.

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.

The timeframe for full compliance should be extended to 1st quarter 2008. NERC should develop a training program to ensure companies understand the requirements and implement appropriately. This training program should be rolled out in late 2005, early 2006. That will allow companies time to work through any issues and implement by 3/31/08.

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:	Randy Schimka	
Organization:	San Diego Gas and Electric Co	
Telephone:	619-725-8627	
Email:	rschimka@semprautilities.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.

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.

1. Cyber Assets - This definition refers to a communications network. Our understanding is that a separate standard will cover telecommunications networks at some future time. We suggest a qualifying statement up front in this section that lists certain assumptions, such as 'for the purpose of this standard, communications networks are excluded' or something similar. 2. Due to the amount of debate in the community about what sort of assets should be classified as Critical Cyber, we feel that some examples of various types of Cyber Assets and Critical Cyber Assets and additional documentation like a decision tree or flow chart (perhaps in the FAQ document) would help clarify the types of assets that qualify as Critical Cyber Assets and provide ideas that the community could use and compare our own efforts against. 3. We also suggest including a revised definition for the term 'authorized access' that includes both physical and electric access.

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.

Many of the questions we've heard discussed about this standard revolve around the issue of identifying Critical Cyber Assets. Some clean examples of what qualify as Critical Cyber Assets, perhaps in the FAQ document, would go a long way towards clarifying some of the questions with respect to this definition.

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.

1. Introduction / Purpose - In the second paragraph, the phrase 'loss or compromise of these assets' is used. We suggest that it be changed to something like 'loss of availability or compromise of the asset integrity.' 2. Requirements - R1.1 - The phrase 'such as, but not limited to' should be replaced with something like 'shall include, but should not be limited to.' 3. R1.1.3 - Please provide more examples or references about Transmission substations, elements, and IROL. There has been some confusion about how this affects the declaration of certain substation assets as critical cyber assets. 4. R1.1.4 - In WECC, the largest generator is 4,000 MW. So using the 80% criteria presented in this section would mean that a 3,200 MW threshold value would exclude most, if not all, of the generation in our region from having to comply with this standard. It doesn't make sense to apply this Cyber Security standard to our Control Centers and EMS systems and some substation equipment while many generating plants in the region would simply not have to comply. Is this relatively high threshold what was really meant by the drafting team for including (or excluding) generation plants? 5. R1.1.7 - Please identify what the specific criteria is for this section beyond the 300 MW figure that is discussed. 6. R2 - While providing a simple definition and an easy way to differentiate what should be included in Security efforts vs. not included (routable protocol vs. non-routable protocol), this section or the FAQ would benefit from further definition. 7. R4 - This list of critical cyber assets can change periodically, so what is the frequency that the senior management signature is required? We recommend no more frequently than once per year. 8. M5 and M6 - Both of these sections add the word 'officer' to the Senior Management designation. Please define the intent of the approval required. We feel that this would most likely be delegated from the Senior VP down to a Director or Manager level in our organization. 9. We suggest that matching compliance levels with specific measurements and requirements will help ensure consistent compliance. 10. Perhaps a flow chart or other visual aid example would be helpful for organizations in applying their situations to R1 and R2.

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.

1. We think it would be helpful for the Requirements and Measures sections to have a one-for-one correlation to make the compliance process easier to organize and manage. 2. Compliance section 2.1.1 - Senior management officials may change during the year, but this section seems to indicate non-compliance if a senior management official position is not occupied or designated for even 1 day during a transition. This wording seems to be in conflict with section M11. 3. M5 reference - Information Security Protection Program, M10 reference - Cyber Security Program, etc. Different terminology is used through the document to refer to the same Security programs as noted above. Please update naming conventions to make more consistent and easier to follow.

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.

1. CIP-004 refers several times to 'personnel' or 'authorized personnel' when discussing assessments, but doesn't really address how to handle the many vendors and contractors that need access to our critical cyber assets to perform maintenance and other tasks. Please consider providing guidelines for these external but necessary folks. 2. If the term 'personnel' is referring to internal employees as well as external vendors and contractors, we see difficulties in holding external vendor and contractor employees to our own internal standards for background checks and assessments. For example, is the drafting team expecting that we would conduct the same type of background checks on regular employees who work on the EMS and associated systems everyday vs. a Facilities contract electrician that gets access to the critical cyber asset space a few days per year to install new circuits or to perform maintenance? There are probably a dozen different examples of contractors and maintenance workers that visit just once or twice per year to perform maintenance in our critical cyber asset areas where it may be impractical to escort them for 5-8 hours during their work. What suggestions does the drafting team have for handling these types of visitors? 3. Please clarify the term 'authorized access' with respect to electronic or physical access, as there are differences in those types of access that should be handled independently. 4. Please provide examples in CIP-004 or in the FAQ document that outline acceptable examples of Awareness communication.

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.

1. General comment - We'd like to see a definition or differentiation made between different types of attended or unattended sites. Some sites have no permanent personnel assigned as their primary work location, but are staffed 3-4 days per week for 4-6 hours per day for maintenance or development work, as well as associated security personnel or other Facility tradespeople doing work in and around the facility. We would call that type of facility 'attended' unless directed otherwise. 2. R3 - The requirements for securing modem connections are different for attended vs. unattended sites. Should this be the case? In our view, unsecure modem connections can make a system vulnerable, no matter whether a site is attended or unattended. 2. R3 - We strongly recommend that an electronic access system be used to control dial up access instead of relying on operations personnel to issue a control to the device and then shutting off access later. The electronic system should use access rosters, two-factored authentication, and logging through the use of a secure server. The benefits of this system are immediate updating, more accurage control, and electronic logging. 4. R5 - The discussion of monitoring electronic access and detecting unauthorized access 24x7 should be more fully defined. What response is required in the event of an unauthorized access, especially after normal business hours? 5. M1 - We suggest removing 'and to the interconnected environment(s)' 6. R6 and M6 - There is a discrepancy between these sections for the timeframes required. Annual documentation review is preferred. 7. R4.2 - We don't think the modem dial-back requirement is particularly effective against hackers. We suggest that the dial back requirement be dropped and replaced with a requirement to utilize electronic handshakes, certificates, or keys to establish a secure connection. 8. R5 - We suggest adding "where technically feasible" in this section since many existing systems don't have these capabilities.

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.

1. Compliance Section - Please add language in the compliance section to address the requirements for archiving the closed circuit or video images discussed in M4 and M5. Any time duration beyond that of just a few days is going to require specific plans to rotate, store, and archive a large amount of video tapes.

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.

1. Introduction - We suggest that the sentence starting with 'A System Security Management program' be modified to include non-malicious activity as well. 2. R1 - Many utilities currently don't install vendor patches and upgrades as they are released by 3rd party vendors (IBM, Sun, HP, etc.) because of the high probability of breaking system functionality. These updates and patches are typically rolled up and installed with a new software release for the control system. We feel that requiring the entity to install these updates and patches as they are released or to take responsibility for testing and certifying these patches and updates is impractical with our current staff and resources. We'd suggest removing references to these items from R1. 2. We'd also like to suggest that this section be modified to include the possibility of using a production system, perhaps at a backup control center, in a non-production mode to accomplish the testing. 3. R2 - The last sentence of this section is not clear. Perhaps a typo exists in the last sentence that reads "shall conduct security test procesures' and should actually read ' shall store security test procesures' ? That would make more sense in the context. 4. We'd like to see some clarification about what the drafting team considers a proper definition for 'attended' versus 'unattended' facilities. 5. R3 - Instead of language in this section that directs the utility to 'establish an

account password management program', isn't the desired result more along the lines of requiring the entity to 'manage account passwords'? 6. R3.1 - Replace the text that reads 'the Responsible Entity shall use accounts that have a strong password' with 'the Responsible Entity shall implement strong passwords.' 7. R3.3 - Again, we'd like to see additional clarification regarding 'unattended facilities.' This subsection becomes unworkable if implemented for our Backup Control Center. 8. R4.2 - While desirable for enhanced system security, many EMS vendors do not support the frequent application of security patches, especially for UNIX Operating systems. Most all of these patches are applied during periodic control system software upgrades, not monthly, due to the fact that many patches break the normal functionality of the tightly coupled EMS software applications and the underlying OS. We would recommend deleting the first sentence of this section. 9. R5.1 This section isn't clear regarding the definition and application of the Integrity software. Is this the same type of software that might also be called "anti-virus software?" Of course, UNIX systems typically don't use anti-virus software like Microsoft platforms would. Some items on our current Critical Cyber Asset list may meet the requirements of this section, but would not have integrity software installed on them. Perhaps this could be clarified with a defining statement that refers to the application of Integrity software with respect to the perimeter and defining the type of equipment that requires it versus other types of equipment that do not require it. 10. R6.3 - We don't see the need for this section and would recommend that it be deleted. 11. R7.2 - We'd suggest deleting this section as it extends beyond the boundary of practicality. 12. R11 - The last sentence of this section should be removed. We see no reason why backup and recovery materials cannot be adequately tested at a normally unattended facility. 13. M2 - Fix typo that reads 'change n status' to 'change in status.' 14. M10.1 - Replace text 'backup data and tapes' with 'backup media.'

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.

Ready for ballot with minor changes - 1) Introduction - Title should be: Cyber Security - Incident Reporting and Response Planning. 2) R1 - 'periodic reviews' should be defined. An annual review would be preferred.

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.

R4 - The seven calendar day requirement in this section will be difficult to implement in a few instances, such as with substations that have Critical Cyber Assets. Typically, a large work force works in, on, and around these types of facilities. Communicating a high quality updated recovery plan to all personnel within 7 calendar days of modification could prove to be a daunting task. Our suggestion is something more reasonable such as 30 calendar days.

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.

1. The schedule for ballot and the eventual implementation of this draft is a few short months for organizations to achieve substantial and/or auditable compliance (estimating an October 2005 implementation date and a March 31, 2006 substantial compliance date). There are many new items in this draft vs. the existing 1200 standard that would have to be drafted, implemented, and reviewed in training with affected personnel. We believe the only way that we'll be ready with compliance in the schedule presented in this draft is to start implementation before the balloting passes, with the risk that certain items may not make it into the final standard. We believe that there should be at least an additional 3-6 months in the implementation plan to be reasonable. 2. General Comments - Requirements should be clearly correlated with Measures and Compliance in the various sections. Some of the sections seem to have been drafted with this in mind, while others have not. For consistency's sake, we believe there should be a one-for-one correspondence between Requirements and Measures. 3. General Comments - Since the sections of the standard have been drafted by separate teams, there are some inconsistencies between the sections. We recommend that NERC have a professional technical writer review and edit future drafts of these documents to bring a high level of consistency to the process and to help clarify terminology before balloting. 4. There are several occasions in the documents where a reader can interpret the standard one way if thinking in terms of control centers and then another way if thinking in terms of substations, power plants, etc. Is there any way to expand on the language and organization in the documents to make the differentiation clearer between the different types of facilities? We'd all like to see a final product that is concise and brief, but sometimes we struggle with the application or definition of some of these materials. 5. We'd also be interested in learning the drafting team's perspective about the inclusion or exclusion of Distribution Control or other utility SCADA systems as they relate to this standard. Has Distribution or other control systems been left out of the requirements due to prioritization, costs for implementation, or will there perhaps be a phased-in approach where they will be added in later? Is the thought to eventually include Distribution control systems in the NERC standards? It seems impractical to spend this much time, money, and effort on Bulk Power-related assets such as EMS control systems and perhaps substation and power plant assets when a similar amount of damage or havoc can be accomplished from a power system perspective if Distribution SCADA systems were compromised.

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:	Bob Wallace	
Organization:	Ontario Power Generation	
Telephone:	416-592-8297	
Email:	bob.wallace@opg.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.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by <<senior management>> or <<executive management.>> OPG often has need or reason to delegate such tasks. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

OPG feels that there are many incidents that may have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>.

We are concerned that <<suspicious event>> is too broad. We recommend changing the Cyber Security Incident definition to <<Any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.>>

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.
YES

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by <<senior management>> or <<executive management.>> OPG often has need or reason to delegate such tasks. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

The OPG answer to question 2 is YES.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by <<senior management>> or <<executive management.>> OPG often has need or reason to delegate such tasks. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

OPG strongly believes that CIP-002 is not ready for ballot. We believe it is important that this Standard specify that the Critical Assets to be considered are a subset of the Critical Assets as defined in the Definitions section.

Requirements R1.1.1 to R1.1.9, inclusive, are too prescriptive. This list belongs in a FAQ. We feel that cyber security personnel should not maintain a list of non-cyber equipment. Perhaps the FAQ should include a statement that <<the Responsible Entity should use a cross-functional team or other methods that are appropriate for that organization>>.

We suggest the Purpose be altered to

<<
This standard is intended to ensure that appropriate cyber 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.

With the increased use of standard technologies to connect Control Center computer systems to the bulk electrical systems, corporate business systems, and the internet, separation between the critical assets of the bulk electrical system and untrusted infrastructure has been dramatically reduced. This connectivity requires that the Control Center systems put in place a high level of Cyber Security measures to protect the Control Center and bulk electrical system assets.

Business and operational demands for managing and maintaining 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 Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system.

The Critical Cyber Assets are identified by the application of a risk-based assessment procedure on the operation of cyber assets supporting the monitoring and control of the interconnected bulk electric system.
>>

We recommend changing Requirement R4 to <<Member(s) of senior management or designee must approve the list of Critical Assets and the list of Critical Cyber Assets.>>

We recommend changing Measure M5 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Assets must be maintained.>>

We recommend changing Measure M6 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Cyber Assets must be maintained.>>

Please clarify the performance reset period in Compliance 1.2. What is being reset? Why is it being reset?

Recommend that Compliance 1.2 change from 30 days back to the 90 days specified in 1200.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by <<senior management>> or <<executive management.>> OPG often has need or reason to delegate such tasks. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

OPG feels CIP-003 needs a little more work before it is ready for ballot. This answer assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot, for more information see the response to the previous question.

We do not agree with C.M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets. We recommend that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>

Please explain what <<information security protection programs>> C.M5 refers to.

We feel that C.M10 is too prescriptive. The Compliance Submittal is signed by an authorized representative of the Responsible Entity. That commits the Entity to that information. If it is later discovered that person did not have authorization, then the Entity did not submit compliance on time, which makes the Responsible Entity non-compliant. This incents Entities to insure the appropriately documented information is submitted on-time.

We are concerned that C.M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the structure of internal corporate relationships>> too frequently.

We feel that C.M13.1 and C.M.13.2 are overly prescriptive and should be removed.

We question how to document continual engagement by executives. If it cannot be document, then it cannot be measured. We recommend removing <<and that executive level management is continually engaged in the process>> from C.M13.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by <<senior management>> or <<executive management.>> OPG often has need or reason to delegate such tasks. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

OPG feels CIP-004 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

OPG feels this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.

Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.

Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.3 should be deleted since this duplicates Requirement 5.3 in CIP-003.

Measure 4.6 should be modified. The requirement for a regular 5 year update to the security screening is not consistent with Requirement R4, which states that a risk based approach be used. The need for rescreening should be cause only.

Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures

Request for Clarification: One of the issues that has been debated at length is the <<Background Screening>> and <<Risk Assessment>> including criminal records checking. The wording in CIP-004 on pages 4 and 5 seems to have been strengthened. The IMO (IESO), and other companies across Canada, have taken the position that existing staff would be <<grandfathered>>. This document would seem to indicate that grandfathering would not be allowed, unless there was

something in the collective agreement to preclude Background Screening. Can we please have clarification on the issue of grandfathering with respect to Background Screening?

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by <<senior management>>or <<executive management.>> OPG often has need or reason to delegate such tasks. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

OPG feels CIP-005 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

OPG requests clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.

Requirement R4.2's third bullet is not clear. We recommend changing from
<<
Out of band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication.
>>
to
<<
Out of band authentication procedures to augment static user id and password access. (e.g. Access will not be enabled via static user id and password authentication unless a telephone call is received from the entity requesting access. On receipt of the telephone call and after successful procedural authentication of the calling party, an administrator will enable access allowing the entitiy to utilize their static user id and password.)
>>

We believe that Requirement R3 is one of many solutions to securing dial-in access. Other solutions are bullet items under Requirement R4.2. We recommend that Requirement R3 become another bullet item under Requirement R4.2.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by <<senior management>> or <<executive management.>> OPG often has need or reason to delegate such tasks. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

OPG feels CIP-006 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

The term <<nearest six-wall boundary>> is used in the Purpose. This term confuses some people. We recommend using <<bounded by the nearest walls, floor and ceiling>> instead.

Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2.

Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.

Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement.

Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.

Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <<In addition, the Responsible Entity>>.

Measure M4 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <<In addition, the Responsible Entity>>.

Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by <<senior management>> or <<executive management.>> OPG often has need or reason to delegate such tasks. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

OPG feels CIP-007 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Requirement R1 assumes that every Responsible Entity has a test system and test unit for every device. We do not agree with that assumption. We do not agree that every patch on every device needs to be tested. If the same patch is applied to the same device, then it needs to be tested once. If the vendor approves the patch and the Responsible Entity applies that patch to all those devices, then the Responsible Entity has secured those devices for this standard. The main source of these objections is the last paragraph in this requirement. We recommend deleting that paragraph. We recommend changing the second sentence in the previous paragraph from

<<Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment.>>

to

<<Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment, where available.>>

We like the phrase <<as possible given the technical capability of the Critical Cyber Asset>> in Requirement R6.3. Perhaps this phrase should be used in a revised Requirement R1.

Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006.

Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.

Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.

Requirement R3.6 should be modified. The second sentence repeats the first, as such it is unnecessary and may confuse some.

Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>.

Requirement R4.1 is too prescriptive and should be deleted.

The <<monthly review>> in Requirement R4.2 is too presciptive. We recommend changing R4.2 from
<<The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.>>
to
<<The Responsible Entity shall perform a routine review of the security patches available for each Critical Cyber Asset. Formal processes shall be used to document their implementation or the reason for not installing the patch.>>

Add <<where technically feasible>> to the end of Requirement R4.3.

Requirement R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means.

Requirement R5.3 allows exception to R5.1. As such, these Requirements should be combined, otherwise one could be non-compliant with R5.1 and fully compliant with R5.3 while the intent appears to be full compliance with R5.1 and R5.3.

The combined requirement should allow technically feasible alternative solutions.

Change Requirement R5.2 from
<<The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.>>
to
<<Where integrity software is deemed to be technically implementable and has been implemented, the Responsible Entity shall perform a monthly review of the integrity software to ensure that the release level of the integrity software is functionally effective and maintainable for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.>>

We do not agree with <<site-specific installation>> in Requirement 5.4. We recommend changing from
<<Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of malware.>>
to
<<Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each software deployment in order to prevent manual dissemination of malware.>>

Change Requirement R6.1 from
<<The Responsible Entity shall perform a vulnerability assessment at least annually that includes:>>
to
<<The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes;>>

Change Requirement 6.1.3 from
<<Factory default accounts>>

to
<<Scanning for factory default accounts>>

Change Requirement 6.1.4 from
<<Security patches and anti-virus version levels>>
to
<<Assessing security patches and/or anti-virus version levels, as appropriate>>

The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assesssment schedule than an attended facility?

The title of Requirement R7 is too broad. We recommend changing this title from
<<Retention of System Logs>>
to
<<Retention of Appropriate System Logs>>
The last sentence of this requirement says the Responsible Entity determines its logging strategy. We believe this means the Responsible Entity decides which are the appropriate system logs to retain.

Requirement R9 should clarify that it pertains to ports inside the perimeter. Requirement R2 of CIP-005 covers ports at the perimeter.

The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.

Requirement R11 belongs in CIP-009. This requirement should be moved to that standard. This requirement references Critical Assets. That is not correct. It should a requirement for the backup and recovery of Critical Cyber Assets. The requirement starts with <<on a regular basis>>, and the third sentence says <<at least annually>>. The requirement should stipulate one or the other. We recommend removing <<annually>>. The last sentence is unclear and should be deleted.

Change Measure M2. The semi-annual audit is too prescriptive. The requirements recognize that the frequency of password changes should be determined by risk assessment.

<<where applicable>> should be added to the end of Measure 4.3.

Change the Measures M5.1 - M5.3 from
<<M5.1 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.
M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found.
M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities.>>
to
<<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments.
M5.2 The documentation shall include a record of the results of the annual vulnerability assessment.

M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions. >>

Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the perimeter.

Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.

Which Requirement and Measurement is Compliance 2.1 associated with?

Compliance 2.2.1.1 needs to be changed so that it is consistent with changes to the corresponding Requirement(s) and Measure(s). This compliance is restricted to <<inside the perimeter>>. There should be no stated difference in the time frames for attended and unattended facilities.

Clarify if Compliance 2.3 should be read as [2.3.1 or 2.3.2 or 2.3.3 (etc)] OR [2.3.1 and 2.3.2 and 2.3.3 (etc)]. We suggest that all of these standards include a statement regarding compliance levels with multiple items.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by <<senior management>> or <<executive management.>> OPG often has need or reason to delegate such tasks. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

OPG feels CIP-008 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from
<<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>>
to
<<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>>

Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3.

The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows

<<The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.>>

Compliance 1.4 stipulates a requirement that is not in the second posting. We recommend creating a Requirement R2 as follows

<<R2. The Responsible Entity shall keep all records related to each Cyber Security Incident for three calendar years. This includes, where appropriate, but is not limited to the following:
R2.1 - System and application log file entries,
R2.2 - Appropriate physical access records,
R2.3 - Documented records of investigations and analysis performed, as available,
R2.4 - Records of any action taken including any recovery actions initiated.
R2.5 - Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.>>

These changes call for a different Measure M2. <<The Responsible Entity shall retain records for each Cyber Security Incident for three calendar years.>>

We recommend changing Compliance 1.2 from
<<The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance reset period shall be one (1) calendar year.>>
to
<<The compliance monitoring period shall keep be three (3) calendar years. The performance reset period shall be one (1) calendar year.>>

We recommend changing Compliance 1.3 from
<<The Responsible Entity shall keep documents specified in this standard for three calendar years.>>
to
<<The Responsible Entity shall keep all data specified in this standard for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.>>

We recommend changing Compliance 2.1.1 from
<<Documentation exists, but has not been updated with known changes within 90 calendar days.>>
to
<<Documentation necessary to demonstrate compliance with Measure M1 exists, but has not been updated within 90 calendar days of known changes.>>

We recommend changing Compliance 2.2.1 from
<<Incident response documentation exists, but has not been updated or reviewed within the last 12 months>>
to
<<Cyber Security Incident Response Plan documentation exists, but has not been updated or reviewed within the last 12 months>>

We recommend changing Compliance 2.2.2 from

<<Incident response documentation exists but is incomplete>>
to
<<Cyber Security Incident Response Plan documentation exists but is incomplete>>

We request clarification on the threshold for Compliance 2.3.2.

Change Compliance 2.4 from
<<No documentation exists>>
to
<<2.4.1 Cyber Security Incident Response Plan documentation does not exist
2.4.2 Cyber Security Incidents have occurred and none were reported to the ES-ISAC>>

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by <<senior management>> or <<executive management.>> OPG often has need or reason to delegate such tasks. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

OPG feels CIP-009 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

We are not sure how broad this standard is. If this is the Recovery Plans of Critical Cyber Assets from Cyber Security Incidents, then the following comments apply.

Requirements R1 and R2 should be swapped. We recommend changing the first requirement from
<<The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan.>>
to
<<The Responsible Entity shall specify the appropriate response to Cyber Security Incidents of varying duration and severity that would require the activation of a Critical Cyber Asset Recovery Plan.>>

Furthermore, we recommend changing the second requirement from
<<The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan at least annually.>>
to
<<The Responsible Entity shall create recovery plan(s) for those events and assets indentified in R1 and exercise its recovery plan(s) as defined by its risk based assessment.>>

We believe that Requirement R3 has the right intention, but its wording is too broad. We recommend changing from
<<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.>>
to

<<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan(s).>>

Requirement R5 is covered in CIP-004. R5 should be deleted.

We believe that Measures M2 and M3 are duplicates. We recommend deleting Measure M2.

Measure M3 corresponds to Requirement R3. We changed Requirement R3. Measure M3 needs a similar modification from
<<The Responsible Entity shall review and update recovery plan(s) annually.>>
to
<<The Responsible Entity shall review and update recovery plan(s) as prescribed by its risk based assessment.>>

Since Requirement R5 is deleted, the corresponding Measure M4 should be deleted. This is covered in CIP-004.

Compliance 1.3 restates Measure M1. Compliance 1.3 needs different words or should be deleted.

Compliance 2.1 should be changed from
<<Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year>>
to
<<Recovery plan(s) exist, but have not been reviewed or updated, if necessary, in the last calendar year>>

As posted, if a Responsible Entity has not reviewed their recovery plan(s) in the last calendar year, they are Level 1 and Level 2 non-compliant. This is confusing. Also, training is covered in CIP-004. Compliance 2.2 should be changed from
<<Recovery plan(s) have not been reviewed, exercised or training performed.>>
to
<<Recovery plan(s) have not been exercised according to the Responsible Entity's risk based assessment.>>

Compliance 2.3 includes specific roles and responsibilities that are not in the Requirements or the Measures. It is confusing and inappropriate to introduce new requirements in Compliance. The reference to <<types of events that are necessary>> is confusing. This standard specifies no types of events as <<necessary>>.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by <<senior management>> or <<executive management.>> OPG often has need or reason to delegate such tasks. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

OPG feels the Implementation Plan does not allow enough time for compliance. First, these standards have substantial changes from 1200. Significant work effort beyond that required to be compliant with 1200 will be required to be compliant with these standards. In addition, the timeframe in which these standards are to be finalized and approved will conflict with the OPG 2006 budget cycle. The 2005 budget is now set without funds set aside for work efforts beyond 1200 and the budget requirements for the new standards will be a moving target until mid to late summer 2005. For either reason, OPG is concerned that we will not be able to identify, defend and have approved appropriate funding to ensure a solid start to the work efforts in 2006, placing the implementation schedule in jeopardy. We recommend that the 2006 dates change to 2007 dates, the 2007 dates change to 2008 dates, etc.

We are concerned with compliance for substations. Substations are part of the <<Other Facilities>>. We recommend the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.

Clarify what dates the compliance submittal is for. Is the first quarter submittal of 2007 for January 1, 2006 to December 31, 2006? Or is the 2007 submittal as of a year ending on the submittal date? Or is the 2007 submittal what the Entity has as of that submittal date?

If the Functional Model is not implemented according to the Functional Model schedule, what is the impact on the Cyber Security Implementation Plan?

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:	Jerry Freese	
Organization:	American Electric Power	
Telephone:	614-716-2351	
Email:	gsfreese@AEP.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.

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.

Cyber Security Incident - "Electronic" is a proper noun and should be capitalized.

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.

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.

R1 should end with a colon instead of a period.

The purpose of restating R1 in R1.1 as well as the definition of a Critical Asset is not immediately clear. If the definition must remain in the requirement text, it should be consistent with the official definition given at the beginning of the standard (i.e., should contain no additional verbiage). We believe that R1.1 should be eliminated and the "level 3" requirements should be promoted to "level 2"

In R2, "critical Cyber Assets" should be "Critical Cyber Assets" (with a capital "C")

In R2.3, we disagree with this statement. Dialing up to a terminal server doesn't necessarily involve routable protocols, but the remote device may very well have point-to-point connections (i.e. serial) to multiple Critical Cyber Assets. These devices should still be given a physical perimeter. Maybe not the same Physical Security Perimeter found at a control center, but a physical security perimeter nonetheless. Otherwise, this is going to cut down on physical protection of Critical Cyber Assets.

In R3, add "as though they are Critical Cyber Assets" after "must be protected" to require all assets on a critical segment to be protected equally.

In general, we believe that the measures should line up with the requirements.

For both compliance and levels of non-compliance, standardize on quarterly for every review cycle. So, "verify annually that changes are made quarterly."

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.

In R2.2, we believe the word "classify" should be used instead of "categorize."

R2.2 could read: "The Responsible Entity shall classify information related to Critical Cyber Assets in order to determine the relative sensitivity of such information; as well as to aid personnel with authorized access in judging what information can be disclosed to others. "

The second paragraph of R3 should be a separate requirement - not part of R3 or a sub-requirement to R3. This should then map to M12.

In R3 "cyber security standard" is a proper noun, and should be capitalized.

R5.2 belongs with the measures, instead of with the Requirements. Overall, it seems like M14 through M18 should be submeasures of a measure that lines up with R5.

All measures should have quarterly review process.

M13.1 is more of a requirement than a measure. Should this be included in R4.1? Or a separate subrequirement for R4?

In the compliance section, the data should be kept for two years instead of three years. Three years requires storing a huge amount of data for an extra year.

In Compliance 1.3.4, "Documented" should be "Document" and this should be two years instead of three years.

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.

The "titles" are inconsistent - either all requirements in the NERC CIP seriees should have titles, or none should have titles. We believe that all requirements should have titles.

Compliance 1.2 - the data should only be stored for 2 years. Storing the data for an extra year makes an even greater burden.

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.

This CIP has titles - again, we like the titles. All Requirements in CIP should have titles.

Also, this CIP has a good relationship between the requirements and the measures. All off the CIP should use this model - the same number of requirements and measures.

R1 should be broken in to separate subrequirements.

In R4.2, consider removing "ANI" specifically. Refer to Caller ID generally.

R6 - the second half of this requirement is actually a measure. It already exists in M6, so it should probably be removed.

Compliance 1.2 - can this be two years instead of three years?

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.

In R1 this requirement should include the requirement for the Responsible Entity to actually maintain a security plan. It could be worded as follows: "The responsible entity shall develop and document a physical security plan, which at a minimum, includes the following requirements."

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.

There is a page number problem in CIP-007-1.

R1 is actually a few separate requirements mixed together. Can it be split up?

Is "Integrity Software" meant to address detective or protective controls?

R5 is inconsistent because it uses a title as the requirement - what is the requirement? Other requirements that have this problem in CIP-007-1 should also be addressed.

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.

The requirements in CIP-008-1 should be matched up with the measures.

Also, CIP-001-1 may conflict with CIP-008-1.

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.

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.

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 the 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:	**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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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 devided 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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

GENERAL COMMENTS: This form has no place for General Comments. In the future, all such forms should have a place for General Comments. / Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements. / The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.Need to define document vs. record and use them consistently. Typically, a document provides the process or procedural requirements of fulfilling an activity. A record provides proof of what the organization actually did and cannot be altered. Another term that is used interchangeably with the two is "data," which is not a document and not always a "business record". Inadequately stated timeframe requirements for retention and documentation updates. Several instances of inconsistent timeframe requirements. Under Compliance, <<other audit records>> should read <<other auditable records>>. It seems the window for such audits is very tight (90 days). The terms <<compliance monitor>> and <<performance-reset period>> are unclear. / DEFINITIONSWe feel that there are many incidents have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>. Further we feel that it needs to be acknowledged that this definition is broad in its scope as a potential standard NERC definition, and that any more specific interpretation is to be addressed within the scope of individual standards, such as CIP002. ———

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

———YES. However, we feel that it needs to be acknowledged that the Critical Asset definition is broad in its scope as a potential standard NERC definition, and that any more specific interpretation is to be addressed within the scope of individual standards, based on such standards' topics, such as CIP002.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO. GENERAL COMMENTS:The standards CIP002-CIP009 still looks inconsistent in a number of areas: a) Some of the measures and requirements language seems to be similar both in the same section of the standards and across the standards; b) The numbering is still inconsistent; c) 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.The time periods prescribed throughout are still inconsistent across the CIP 002 to 009 standards.If an entity is found not to have properly identified its critical infrastructure in 002, will this mean being scored as non-compliant in the other remaining standards?The standard 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 exists 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.Most references to unattended facilities do not seem to bear relevance on security measures to critical cyber assets and should be reviewed.ISO-NE believes that CIP-002 is not ready for ballot. We believe it is important that it is clarified that the Critical Assets specifically identified are a subset of the Critical Assets as defined in the Definitions section. In the purpose, the words <<would adversely impact>> should be changed to <<would significantly impact>>.Suggest removal of R 1.2 – R 1.10 to the FAQ because these are guidelines and are overly prescriptive rather than allowing the entity to use a risk-based methodology. R.1.11 should be deleted. This will require some adjustment to the requirements and measures throughout the whole section.We recommend changing Requirement R4 to <<Member(s) of senior management or designee must approve the list of Critical Assets and the list of Critical Cyber Assets.>>In MEASURES, This section (in several areas) refers to <<officers>> whereas the other standards refer to <<senior manager>>. We recommend a standard term of <<senior manager or designee>>.Suggest MEASURES refer to a <<significant or material change>>.M4 should be 90 days.We recommend changing Measure M5 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Cyber Assets must be maintained.>>We recommend changing Measure M6 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Cyber Assets must be maintained.>>Please clarify the performance reset period in Compliance 1.2. What is being reset? Why is it being reset?Recommend that Compliance 1.2 change from 30 days back to the 90 days specified in 1200———

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO. ISO-NE feels CIP-003 needs a little more work before it is ready for ballot. The last sentence in R1 should be deleted as it is redundant.R3 the words <<from the requirements of this standard>> should be replaced by <<from the requirements of the NERC CIP series of standards>>. The last sentence of paragraph two is redundant and should be deleted.R4.1-4.2 belongs in CIP007, and should be removed from CIP003.We do not agree with M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets. We recommend that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>Remove sections M5 & M6 because they are scope creep and are covered in M7.Suggest <<procedures>> in M7 and M8 be changed to <<controls>>.M 10 is too prescriptive. Name, Title and Date of Designation are adequate here. Maintaining the other information is too onerous and does not provide any value.We are concerned that M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the structure of internal corporate relationships>> too frequently.We question how to document continual engagement by executives. If it cannot be document, then it cannot be measured. We recommend removing <<and that executive level management is continually engaged in the process>> from M13.M13.1 is a duplicate of M 12M13.2 –This belongs in CIP007 and should be removed.M14 – This statement is redundant - to reflect any change in status that affects the designated personnel's ability to authorize access to those Critical Cyber Assets.M15 – same comment as M10M17 and M18 should be deleted. This measure duplicates measures 4.1 and 4.2 of CIP 004. 1.3.4 – There is no stated requirement for this and should be removed.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO. ISO-NE feels CIP-004 needs more work before it is ready for ballot. ISO-NE feels this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003.Measure 4.6 should be modified. The requirement for a regular 5-year update to the security screening is not consistent with Requirement R4, which states that a risk-based approach be used. The need for re-screening should be cause only.Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures———

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO. ISO-NE feels CIP-005 needs more work before it is ready for ballot.R1 – delete the first sentence. Repeating the term Electronic Security Perimeters is redundant. The rest of the paragraph is helpful but should not be contained in a requirements statement. Could be moved to the Electronic Security Perimeter definition or to an FAQ.ISO-NE requests clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.R3 – attended or unattended is irrelevant to security in this paragraph.We believe that Requirement R3 is one of many solution to securing dial-in access. Other solutions are bullet items under Requirement R4.2. We recommend that Requirement R3 become another bullet item under Requirement R4.2.R4 – The phrase <<and the Critical Cyber Assets within the Electronic Security Perimeter(s).>> is confusing given that this standard refers to Electronic Security Perimeter.R4.2 – Did y'all mean <<remote access>> or really <<external interactive logical access>>? Please clarify.R4.2 – Suggest that indicating <<Strong procedural or technical controls>> is all that is required.R4.2 – this is too prescriptive for a standard. Would be better as a guideline because technology changes so rapidly.R4.3 – should be removed. This is not a security measure but a legal support measure.R5 – Monitoring authorized access should be replaced with logging authorized access.R6. We could find no requirements for the creation of any documents in the requirements section of this standard.M1 establishes a new requirement to document interconnected critical cyber assets within the security perimeter, which is not reflected in the requirements.M2, M3.1 and M3.2 establish new requirements, which are not covered in the requirements section.M5.2 – this appears to be the same as CIP 007, R 7/M6.M6 contradicts R6 of this standard.COMPLIANCE:1.2 there is an inconsistency with CIP 007 R 7.1.1.4.4 – Not consistent with requirements or measures.2.1.2 – This is not a realistic requirement as it deals mainly with the reliability/availability of systems. A better measure would be to verify that the monitoring processes are in place or the failure of a monitoring process was corrected within 24 hours. 2.3.2 – The word audit is a new requirement and has specific connotations. The word regular is un-measurable. A better expression would <<record of [time period] validations or assessments>>.2.1.2 – This is not a realistic requirement as it deals mainly with the reliability/availability of systems. A better measure would be to verify that the monitoring processes are in place or the failure of a monitoring process was corrected within 24 hours. 2.3.2 – The word audit is a new requirement and has specific connotations. The word regular is un-measurable. A better expression would <<record of [time period] validations or assessments>>.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO. ISO-NE feels CIP-006 needs more work before it is ready for ballot. The reference to six-wall boundary is only referenced once, but is confusing. Be more specific as to intent.Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2.Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement.Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement. Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.The term <<Security Officers>> is confusing and should be changed to <<Security Personnel>>.M4. This is redundant. These requirements are referred to in R1 and M1.Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.2.1.1 Not consistent with M1.2.2.1 Requires more stringent compliance than level 1 compliance.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO. ISO-NE feels CIP-007 needs more work before it is ready for ballot. This standard is a prime example of the need for a technical writer's review of the standards. It is much more prescriptive than the rest and demonstrates the lack of homogeneity across the standards. It also needs very serious work to properly align Requirements, Measurements, and Compliance statements.R1 – Delete. This requirement is well covered in CIP 003, R4 and R5R2 – Delete. This requirement is well covered in CIP 003, R4 and R5R3 – use <<account management>> instead of <<establish an account password management program>>R3 – <<by compromised account passwords>> should be struck as unnecessary.R3 – <<that include but are not limited to:>> should say <<that must meet at a minimum:Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006.Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006. Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.Requirement R3.6 should be modified. The second sentence repeats the first, as such it is not necessary and may confuse some.Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>.R4.1 – Should read <<all relevant patches>>R4.2 & R4.3 – this requirement is too prescriptive. A better requirement would be for the company to have a patch management policy and procedure based on its own environment.R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means.R5.1 – This section is unclear and would be better if written as follows: <<The Responsible Entity shall use means to monitor and protect the integrity of data including software associated with critical cyber assets e.g.: technology, processes/procedures, software.>> to prevent, limit, and/or mitigate the introduction, exposure and distribution of malicious software (malware) to other Cyber Assets within the Electronic Security Perimeter.R5.2 - Suggest it be deleted. Covered elsewhere.R5.4 – Where remote installation of software updates is required, the responsible entity shall ensure the integrity of the software being installed prior to initiating remote installation in order to prevent annual dissemination of malware.Change Requirement R6.1 from<<The Responsible Entity shall perform a vulnerability assessment at least annually that includes:>>to<<The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes:>>Change Requirement 6.1.3 from<<Factory default accounts>>to<<Scanning for factory default accounts>>Change Requirement 6.1.4 from<<Security patches and anti-virus version levels>>to<<Assessing security patches and/or anti-virus version levels, as appropriate>>The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assesssment schedule than an attended facility?The title of Requirement R7 is too broad. We recommend changing this title from<<Retention of System Logs>>to<<Retention of Appropriate System Logs>>R7 – The last sentence gives the entities the responsibility to determine their own logging strategy but R7.1 and R7.2 are contrary and prescriptive and should be deleted.R8 – Should be deleted as it is well covered in CIP 003.R9 – Should be deleted as it is well covered in CIP 005.The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.R11 – The last sentence <<For unattended facilities, back-up and

recovery materials can be effectively tested at central test facility and shall not be tested on site.>> should be removed and the rest of this section moved to CIP 009.Please re-align all Measurements with stated Requirements. Remove any measurements that to not coorespond to a stated requirement.M2. – Remove <<record of semi-annual audit of this policy>> as is contrary to R3.1.M3 Remove - The reference to change control is dealt with in CIP 003.Change the Measures M5.1 - M5.3 from<<M5.1 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. M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found. M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities. >>to<<M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments. M5.2 The documentation shall include a record of the results of the annual vulnerability assessment. M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions. >>Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the perimeter.Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.Which Requirement and Measurement is Compliance 2.1 associated with?Compliance 2.2.1.1 needs to be changed so that it is consistent with changes to the corresponding Requirement(s) and Measure(s). This compliance is restricted to <<inside the perimeter>>. There should be no stated difference in the time frames for attended and unattended facilities.Clarify if Compliance 2.3 should be read as [2.3.1 or 2.3.2 or 2.3.3 (etc)] OR [2.3.1 and 2.3.2 and 2.3.3 (etc)]. We suggest that all of these standards include a statement regarding compliance levels with multiple items

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO. ISO-NE feels CIP-008 needs more work before it is ready for ballot. The references to <<incidents>> should say <<cyber security incidents>>.Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from<<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>>to<<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>>Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3.The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows<<The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.>>Compliance 1.4 stipulates a requirement that is not in the second posting. We recommend creating a Requirement R2 as follows<<R2. The Responsible Entity shall keep all records related to each Cyber Security Incident for three calendar years. This includes, where appropriate, but is not limited to the following: R2.1System and application log file entries, R2.2Appropriate physical access records, R2.3Documented records of investigations and analysis performed, as available, R2.4Records of any action taken including any recovery actions initiated. R2.5Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.>>These changes call for a different Measure M2. <<The Responsible Entity shall retain records for each Cyber Security Incident for three calendar years.>>We recommend changing Compliance 1.2 from<<The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance reset period shall be one (1) calendar year.>>to<<The compliance monitoring period shall keep be three (3) calendar years. The performance reset period shall be one (1) calendar year.>>We recommend changing Compliance 1.3 from<<The Responsible Entity shall keep documents specified in this standard for three calendar years.>>to<<The Responsible Entity shall keep all data specified in this standard for three (3) calendar years.The compliance monitor shall keep audit records for three (3) calendar years.>>We recommend changing Compliance 2.1.1 from<<Documentation exists, but has not been updated with known changes with 90 calendar days.>>to<<Documentation necessary to demonstrate compliance with Measure M1 exists, but has not been updated within 90 calendar days of known changes.>>We recommend changing Compliance 2.2.1 from<<Incident response documentation exists, but has not been updated or reviewed within the last 12 months>>to<<Cyber Security Incident Response Plan documentation exists, but has not been updated or reviewed within the last 12 months>>We recommend changing Compliance 2.2.2 from<<Incident response documentation exists but is incomplete>>to<<Cyber Security Incident Response Plan documentation exists but is incomplete>>We request clarification on the threshold for Compliance 2.3.2.Change Compliance 2.4 from<<No documentation exists>>to<<2.4.1 Cyber Security Incident Response Plan documentation does not

exist2.4.2 Cyber Security Incidents have occurred and none were reported to the ES-ISAC>>

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO. ISO-NE feels CIP-009 needs more work before it is ready for ballot. We are not sure how broad this standard is. If this is the Recovery Plans of Critical Cyber Assets from Cyber Security Incidents, then the following comments apply.R1. Overly prescriptive. The minimum test frequency schedule should be based on a risk-based assessment and evidence kept that this testing frequency is respected.We believe that Requirement R3 has the right intention, but its wording is too broad. We recommend changing from<<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.>>to<<The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan(s).>>Requirement R5 is covered in CIP-004. R5 should be deleted.M1 and M2 should be merged.M3 and M4 are repetitive and should be merged.M4 contradicts R3.Since Requirement R5 is deleted, the corresponding Measure M4 should be deleted. This is covered in CIP-004.Compliance 1.3 restates Measure M1. Compliance 1.3 needs different words or should be deleted.2. This compliance section will not work and should be revisited. For example, a plan that has not been reviewed will contradict both level 1 and level 2. Entity which neither updates its recovery plan in the past year, nor exercised nor included in it the types of <<events that are necessary>> could legitimately claim any of level 1, 2 or 3 noncompliance. Level 3 identifies a new requirement that should be identified in the requirements and measures section, or deleted.———

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.

NO. GENERAL COMMENTS:The standard still looks inconsistent in a number of areas: a) Some of the measures and requirements language seems to be similar both in the same section of the standards and across the standards; b) The numbering is still inconsistent; c) 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.The time periods prescribed throughout are still inconsistent across the CIP 002 to 009 standards.If an entity is found not to have properly identified its critical infrastructure in 002, will this mean being scored as non-compliant in the other remaining standards?The standard 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 exists 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. Most references to unattended facilities do not seem to bear relevance on security measures to critical cyber assets and should be reviewed. SPECIFIC TO IMPLEMENTATION: Since the standard will not become official before October 1, 2005, it is not realistic to expect an acceptable level of auditable compliance in Q1 2006. Specifically: a) NERC CIP 002-009 is much deeper and wider than NERC 1200 and will require a significant compliance effort; b) No budgeting can typically be done until the standards are confirmed and solidified; c) 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 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.Change 2006 to 2007 (and successive columns) and change from auditably to substantially compliant. A good requirement would be to require a corporate implementation plan for compliance 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: The entity must identify the dates when the document retention processes must begin to be compliant with the standard.———

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:	John Currier(seg 5), Ron Donahey(seg3), Jose Quintas(seg 6), Paul Davis (seg 1)	
Organization:	Tampa Electric	
Telephone:	813-225-5287 Paul McClay	
Email:	PFMCCLAY@TECOENERGY.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.

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 preface to the this section should reference the NERC Glossary of Terms. There does not appear to be a Reliablity Standards Glossary of Terms.

"Exceptions" and "deviations" are used throughout the standards, and while described as different in the answer to Tampa Electric's previous comments (deviations are where you meet part but not all of standard; exception is where you meet no parts of the standard), neither the standard nor the FAQ differentiates the terms. Question 4 in the FAQ describes documenting both in the same manner.

The following are General Comments that apply to all CIP-002 through CIP-009 re Compliance:

1. Inconsistency remains between levels of non-compliance across standards…. For example, level one non-compliance for maintenance of log data is different between CIP-005 and CIP-006.

2. The standards drafting team should consider better aligning the measures sections with the requirements sections. In some cases the alignment is strong, where in others it is difficult to determine which requirement a specific measure is intended for. For example, CIP-003 has 8 requirements but 18 measures. Additionally, the non-compliance levels should be more closely aligned with the measures, which needs work in all standards.

3. If an organization makes a conscious decision, due to technical feasibility or practicality, not to implement a requirement as defined by this standard, can the organization document an exception or deviation (as defined above) to the standard without having to report non-compliance? If you have a documented deviation to a standard, can you report being in compliance?

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.

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.

The numbering in this section is inconsistent with the other standards.. R1.1, R1.2, etc. versus R1, R2, etc.

R1.6 No where is "Generating Resources" defined. Is a generating resource a "single generating unit" or a "a combination of units at the same geographical location, i.e. a plant"? This needs to be clarified in the standard.

During the conference call conducted for the first draft, we posed a question as to whether a facility that houses critical assets, but has no external connectivity, either dial-up or network, still fell under this standard. The response from the host of the session, Larry Bugh, was that these assets were not covered by this standard. During the Feb 2 conference call there was discussion around standard CIP-002, which implied that this may not be the case. Can the drafting team clearly address facilities that have no external connectivity, but house critical assets that run a routable protocol?

R1.11 Calls for a risk based assessment to be conducted by the responsible entity to identify critical cyber assets. Can the organization develop its own risk assessment program? Can the drafting team provide examples of acceptable, industry accepted risk based assessment methodologies? Does the assessment process need to be re-performed annually, or just updated as assets are added/removed?

M1 references R1 but it should be R1.2
M3 references requirements R2 and R3 which do not appear to exist.

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.

M3, M4, D.1.3.3 - “Exemptions” is a term used in the Measures M3, M4 (used twice) and Compliance D.1.3.3. This term is used no where else and is not defined. It should say exceptions or deviations.

Also Refer to FRCC Comments

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.

R4 states that Personnel be subjected to a personnel risk assessment process. M4.6 uses the term "screenings" rather than risk assessment. The measure and requirements terminology should be consistent.

In addition, we believe the "every five years" criteria will be extremely costly and is unnecessary. However, if it remains it should be phased in over a longer time period for implementation than in the current plan.

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.

R1 states that non-critical assets within the electronic security perimeter must comply with the requirements of the standard. This is already stated in CIP-002 R1.16 and appears to be redundant here. Would recommend that either this be restated in every standard or deferred to CIP-002.

R2 disable unused network services and port is redundant to CIP-007 R9. It should be stated in one standard to ensure that future modifications do not necessitate changes in two places. We would recommend CIP-007 as that appears to be the all inclusive section on server/device configuration. If a requirement is still needed in CIP-005 it should refer to CIP-007.

R3 Just because it may be technically feasible to remotely activate a dialup connection via SCADA, does not mean that is the most prudent control to implement. If Dialup is necessary because of a SCADA communications problem, then the responsible entity would have no way to access the device except physically, which could lead to a more serious incident. This is something that should not be dictated in the standard, but left to the individual organization to decide, so long as procedural and technical controls are in place over the dialin. We recommend removing this requirement, or providing it as an alternative to other procedural or technical controls which may be more effective.

R4.2 Where a firewall has been implemented to allow access only to and from certain specific IP addresses within the electronic perimeter, does the firewall have to implement one of the strong technical controls listed, or can the critical cyber asset be relied upon to provide the authentication requirement? For example, a server on the corporate network, or within another secure perimeter, has to communicate with a server within the perimeter. Can the authentication take place between the servers, or does the firewall have to provide authentication over and above IP address filtering?

Compliance, Levels of Non-compliance 2.2.2 How does an organization demonstrate compliance (i.e. prove it) with a level that states non-compliance if gap exists in system logs of between 1 and 7 days? How does an organization measure this across the multiple logs that are retained? Or does an organization report it only if it knows about it? In addition, D1.4 indicates we would "supply for inspection" access logs. There will only be 90 days of access logs available, therefore logs cannot be audited for a year.

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.

M4 Human observation (i.e. a security guard checkpoint that is manned 24x7) should be an acceptable method for monitoring physical access control, and added to the table in M4.

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.

R1 The use of a separate non-production environment for testing and acceptance of security changes results in the need to re-licensing EMS, DCS and other software to establish such an environment. Test environments may not be feasible for many older EMS or DCS systems running proprietary hardware and software. The drafting team needs to consider a phased in approach for this requirement due to the cost to the industry, and time required to implement such environments. The industry should be asked for feedback on this requirement, as a large percentage of the

participants do not have such test environments readily available. Those that do, probably also use those environments for testing upgrades and application changes as well, meaning those environments do not always mirror their production counterparts.

R1, R6 During the conference call on 2/2 there seemed to be considerable confusion surrounding the testing of security patches and scanning for vulnerabilities. There was even discussion of trying exploits against production systems after patching. It should be emphasized that great caution should be taken when scanning or testing patches in an EMS or DCS environment. In fact, scanning for open ports and exploits in these environments could result in unintended system outages, and could be considered negligent. Only non-intrusive means to determine open ports, and to verify the installation of patches, should be used in this type of environment, and it the drafting team should modify sections R1 and R6 to ensure that they are not suggesting the use of obtrusive tools for testing patches or identifying open ports in a production environment.

R3.3 This requirement is confusing. What does physical access to an unattended facility have to do with generic account management? For unattended facilities (i.e. substations, backup facilities, unattended control buildings or rooms within a generating station) it is not practical to have approvals of physical access on an instance-by-instance basis. If a trusted employee who has been background screened, has a cardkey, token or other pre-approved access method for physical access to an unattended facility, and the other requirements as dictated by CIP-006 are in place, there is no need to have a separate function approve access each time that employee needs to enter such a facility. Regardless, any requirement of this type belongs in CIP-006.

R3.5 This requirement belongs in standard CIP-006.

R6.3 The intent of this requirement escapes us. Why is this requirement specific to unattended facilities?

R7.2 Again the intent of this requirement for unattended facilities escapes us. A facility that is unattended (substation) should have the same logging requirements as those that are attended (control centers) if the assets housed there are critical.

R8 Does the change control process described in this environment relate to all changes or just those of a security software or patch nature? Please clarify the wording.

R11 For clarity purposes, this requirement is more appropriate to be contained in CIP-009 Recovery Plans. The level of detail discussed in this section is not currently covered in CIP-009, and having recovery requirements in two separate standards only leads to confusion and creates the possibility of conflicting requirements in future standards versions. Any recovery plan should specify the data, retention period, etc to be backed up for recovery purposes. Including in this section only increases administration on the part of the individual entities for developing procedures, and monitoring compliance.

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.

R11 in standard CIP-007 For clarity purposes, this requirement is more appropriate to be contained in CIP-009 Recovery Plans. The level of detail discussed in this section is not currently covered in CIP-009, and having recovery requirements in two separate standards only leads to confusion and creates the possibility of conflicting requirements in future standards versions. Any recovery plan should specify the data, retention period, etc to be backed up for recovery purposes. Including in this section only increases administration on the part of the individual entities for developing procedures, and monitoring compliance.

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.

See FRCC comments

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.

The new standards are a significant increase in scope and requirements over the existing 1200 standard. Implementation and ongoing maintenance of the technical controls required by this standard across the industry will entail time and cost many millions of dollars. Implementation to a point of auditable compliance will likely take several years for many larger organizations, with significant generation or transmission systems. The timetable for passage of this standard has missed 2005 budget cycles, and the standard may not be finalized and passed before most entities can identify costs and budget for 2006. As such we believe that NERC has an obligation to perform a thorough impact analysis, with full participation from the industry, as a part of implementation plan development, and allow for a phased in implementation across multiple years. We support the need for these critical standards. But we don't support standards that neglect costs, complexity and reasonable timeframes for implementation.

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:	Larry Conrad, Doug Hils, Walt Yeager, and Sharon Edwards	
Organization:	Cinergy	
Telephone:	317-838-2022	
Email:	Larry.Conrad@Cinergy.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.

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 following comments do not apply to the definitions, but are general comments that are applicable to all of the proposed standards CIP-002 through CIP-009.

Cinergy supports all of the comments developed by the ECAR CIPP Group, which are being submitted to the Drafting Team under separate cover. Cinergy has these comments in addition to those submitted by the ECAR CIPP Group.

Timing for the reviews of the documentation need to be standardized both in the presentation in the document and also in the time frames prescribed for the reviews. Sometimes the timing requirements appear in the requirements section, sometimes in the measures section, and sometimes they are only referenced in the non-compliance section. (See example in section CIP-004-1 & CIP-005-1 below.) Due to these inconsistencies, there are instances where the timing requirements contradict one another within the individual CIP standard. A table needs to be developed showing all of various timing/review requirements so that periodicity for reviews and updates are clear. For many of the requirements, annual reviews should be sufficient.

Measures should point back to the appropriate requirement. At present it is sometimes difficult to understand which measures point back to which requirements.

Implementation Plan for Other Facilities (not Control Centers): Some weeks ago, participants had been asked to provide an estimate of how long it would take them to implement the proposed permanent standards. Cinergy estimated that approximately four (4) years would be required. The implementation plan states that all entities must be audibly compliant with all sections by 1st quarter of 2007. We once again state that it will take one year for the planning and three (3) additional years to implement all requirements of the permanent standards. We ask that the implementation plan be adjusted to reflect the input of the participants. If the implementation plan is not adjusted for all CIP sections, then at least the sections dealing with Physical Security, Security Management Controls, Systems Security Management, and Electronic Security need to be moved back to reflect the input from the utilities that will have to implement compliance.

Implementation Plan for Control Areas: In most cases the Control Areas are expected to be "auditably compliant" with almost all requirements by 1st quarter of 2006. The logic, provided by an ECAR representative, for this is that these requirements are 'direct descendents" from Standard 1200. However, the scope of CIPP 002 through CIPP 009 has been extended so much that there are very few 'direct descendents' from Standard 1200. While we realize that Control Areas were covered by Standard 1200, Control Areas should have until 1st quarter of 2007 to comply with the requirements which have changed substantially from Standard 1200 to the current proposed permanent standards. Additional detail is provided at the end of these comments indicating specific examples.

Define "Integrity Software."

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.

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.

CIP-002-1 B.R1.1.3 & R1.1.8.IROL: While a definition exists of an IROL, some additional explanation is required to ensure common understanding of how these requirements should be applied.
CIP-002-1
B.R.2.1.Cyber assets that use a routable protocol: Because cyber assets, which use a routable protocol, must be protected both physically and electronically, in effect, entities which move to a routable protocol are penalized. We believe this type of requirement will impede progress toward routable protocols in substations. The level of administrative and cost burden may cause Cinergy and other companies to delay or avoid moving to routable protocols and, therefore, they will continue to operate with less information and less reliability. We urge NERC to reconsider requiring the physical perimeter if a routable protocol is used.

CIP-002-1
B.R.4."Member of senior management must approve the list of critical assets…" This is an un-necessary level of approval. The senior management's name(s) are included in the policy. It is not necessary for the senior management to approve individual lists, etc. These types of requirements add administrative burden with no offsetting enhancement in security.

CIP-002-1
C.M.4. "…update documentation…within 30 calendar days…" See general comment above regarding standardizing the review/updating of requirements.

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.

CIP-003-1General Comment about this section. Many of the requirements are not available through existing legacy systems. Cinergy is working with a vendor on a new EMS system, which should be operational in mid to late 2007. Some clause should be inserted into the documentation to allow time for delivery of a new system on order, which can supply the required controls. For example, other sections state the requirement applies "if it is technically feasible." We suggest adding this type of language to requirements in this section.

CIP-003-001
B.R2.1.We recommend changing "Responsible Entity shall identify all information, regardless of media type…" to "Responsible Entity shall identify information, regardless of media type…" Eliminate the word "all". It is impossible to certify that ALL information is protected. This was also pointed out in Draft I. Requirement as written is impossible to comply with.

CIP-003-001
B.R.4.Documentation requirements here did not change from Draft I to Draft II. This will require approximately 1 FTE to manage all of the required documentation. These ongoing costs will not significantly increase real security. Recommend that the documentation requirements be reduced by eliminating some of the following:
- Formal process for promoting systems into production (covered in testing)
- Keeping separate governance process documentation for cyber security purposes (this is covered in other corporate documents).

CIP-003
B.R.4.1."…approving authority shall…verify…system meets…standards…prior to being promoted to…production environment." This requirement could easily cripple emergency restoration of EMS operation especially in after hour conditions, i.e., getting formal approval and documentation that a system has passed testing criteria in an after hours emergency.

CIP-003-1
Non-Compliance 2.3.4. It is Level 3 violation if the list of designated approving authorities is not maintained and up to date. This seems too harsh. Recommend that this be changed to a Level 3 violation if the list of designated authorities has not been reviewed or updated in the last 12 months.

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.

Section CIP-004-1
B.R.2."…training program that will be reviewed annually." Language is not clear if the training material or the training of the individuals needs to be reviewed annually or if both need annual review. Modify the language so that the intent is clear.

CIP-004-1
B.R.4.Please provide an explanation of how to deal with background checks on service personnel such as HP used for remote computer support.

CIP-004-1
C.M1.Awareness: Since annual training is required, a separate awareness program is un-necessary and requirement should be deleted.

CIP-004-1
C.M.4.2.This measure states: "Review (the list of all personnel and specific access rights) quarterly…" However, CIP-003-1 C. M. 18 states: "...review user access rights…at least annually." See general comment above. Drafting Committee needs to standardize the review/update requirements and provide a consistent table of the frequency for such reviews.

CIP-004-1
C.M4.4The language in this section now pertains to a 'personnel risk assessment' rather than a background screening. Therefore, the language "…A minimum of identify verification (Social Security number verification) and seven year criminal check is required" should be deleted. It is no longer appropriate. Those types of things may not be part of the personnel risk assessment.

CIP-004-1
C.M4.4Recommend that language be inserted stating that bargaining unit employees will be screened prior to granting access to critical cyber assets. If the initial screening proves adequate, subsequent background screening will not be performed on bargaining unit personnel.

CIP-004-1
C. M4.6Change "…shall conduct update screenings…" to "…shall conduct updated personnel risk assessment…" The intent here is the personnel risk assessment of individuals is updated.

FAQ vs. CIP-004-1The FAQ's language refers to 'background screenings.' However the CIP-004 language refers to a personnel risk assessment. The FAQ language is no longer consistent with the

CIP-004 language. For example, the FAQ's say 'no grandfathering'. Recommend changing the FAQ to reflect current language referring to personnel risk assessments rather than background screenings.

CIP-004-1
Additional Questions:

Questions: Reference CIP-004-01 Personnel Training, Section M4.4 and the FAQ.
How aggressive do the methods need to be in order to address Collective Bargaining Agreements (CBA) to meet the Personnel Risk Assessment, if the CBA does not currently allow?
If arrangements still cannot be met through the CBA, will a waiver be granted?

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.

CIP-005-1
B.R.4.3.This requirement states 'where technically feasible'. Some of the requirements in this section and in the Security Management Controls and Systems Security Management sections may NOT be technically feasible with legacy EMS systems. We recommend that organizations, which are in the process of replacing their EMS legacy systems, should be given the time to comply with requirements as they become 'technically feasible' after they implement the new EMS systems. We have made specific recommendations in the implementation section.

CIP-005-1
B.R.4.3.Please explain how companies are to deal with the 24 X 7 monitoring of devices such as RTU's. This 24 X 7 monitoring appears to be mandatory in requirements 4 and 5.

CIP-0005-1
B.R. 5Change this language: "The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring …" to the following: "The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, to log the following and review in a timely manner: monitoring authorized access, detecting unauthorized access…"

CIP-0005-1
B.R. 5This requirement should only be applicable to networks utilizing a routable protocol. The requirement may not be technically feasible otherwise.

CIP-005-1
B.R6. & C.M.6.R6 requirement calls for a review of the documents at least every 90 calendar days with updates made within 30 calendar days. However M6 states that the documents referenced in the standard should be reviewed annually. Is the review requirement every 90 days or annually? See general comments about standardizing the times for review and providing participants with a consistent schedule for updates and reviews. Recommend making the review an annual review rather than every 90 days. Annual should be sufficient time for this requirement.

CIP-005-1
M4.2.2Language states "…periodic review process…defined in CIP-003-1…" The review timing should be spelled out in the relevant CIPP document rather than referencing another section. Timing review requirements are poorly presented throughout the documents and need improvement.

CIP-005-1 D.1.3Strike reference to personnel risk assessment documents as they do not pertain to this section at all.

CIP-005-1
Additional Questions:

Question: If a firewall is established between the operator consoles and the Secure LAN, will the operator consoles be considered outside of the Electronic Perimeter and the Physical Perimeter?

Question: If the operator consoles of a critical cyber asset communicate by non routable serial communications between the keyboard and mouse and the processor and remaining peripherals are secured within the physical and electronic perimeter, is it permissible for the keyboards, mouse and display device to be outside of the electronic perimeter?

Question: What if the keyboard and mouse are USB connected?

Question: To maintain the electronic perimeter, are the consoles required to meet the access requirements of CIP-005-1 Electronic Security, Section B.R4?

Please clarify how the requirements would apply to “read-only” consoles that cannot impact the bulk electric system.

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.

CIP-006-1Physical Security: Because the requirements are very specific, we still believe that NERC should have some idea of the financial impact of its directives across the industry. This comment was made in response to Draft I, and the drafting team response was that this was up to the individual company to assess financial impacts. It is not up to the individual company to assess the financial impact across the entire industry. The drafting team's response to the comment asking that NERC have some idea of the financial impacts across the industry was un-satisfactory and we again recommend that NERC has responsibility to have some idea of the financial impacts across the industry prior to finalizing these requirements.

CIP-006-1
C.M.3Security Officers: Can a control room operator also fulfill the 'security officer' function of monitoring physical access 24 hours a day, 7 days a week? Can the access point be manned by someone other than a security guard if the access point is in a room that is manned by plant personnel 24x7? Would this be sufficient along with the other access controls?

CIP-006-1
C.M.5.Manual Logging: Section now states: "A log book or sign-in sheet or other record of physical access accompanied by human observation or remote verifications." We recommend deleting the phrase "…accompanied by human observation or remote verifications." We believe that the logging book and sign in sheet are sufficient documentation for the manual logs.

CIP-006-1
Additional Question FAQ:
Question: Reference Frequently Asked Questions – Standard CIP-006-01, Cyber Security-Physical Security Section.

The question of "What is the Physical Security Perimeter?" has an answer that says, "is a four wall boundary." Shouldn't the answer be a six wall boundary?

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.

CIP-007-1General Comment about this section. Many of the requirements are not available through existing legacy EMS systems. Cinergy is working with a vendor on a new EMS system, which should be operational in mid 2007 to late 2007. Some clause should be inserted into the documentation to allow time for delivery of a new system, if it is on order, which can supply the required controls. For example, other sections state the requirement applies "if it is technically feasible." We suggest adding this type of language to requirements in this section.

CIP-007-1General Comment about this section: Need additional clarification regarding the definition of attended vs. un-attended facilities. Is a facility, which is manned 8 hours a day and un-manned 16 hours a day, attended or un-attended?

CIP-007-1
B.R1.

Documentation requirements in this section are excessive. Draft I documentation requirements were excessive, and, except for formatting, little changed from Draft I to Draft II of this section. For example, "...The Responsible Entity shall document full detail of the test environment..." is not necessary and should be eliminated.

CIP-007-1
B. R. 2Requirement states: "…shall not store …security procedures…at an unattended facility…" Recommend that this sentence be deleted. Security procedures and other documentation need to be available at backup sites, which may be generally un-attended.

CIP-007-1
B. R.3.1Strong Passwords: The last sentence "Passwords shall be changed periodically per a risk based frequency to reduce the risk of password cracking…" is not practical regarding relays, particularly when networked communication is not used. Recommend that the drafting team modify the language so that relays are excluded from the requirement.

CIP-007-1
B.R.3.3The requirement that physical access is authorized by a control or security center operator on an instance by instance basis is harsher than CIP-006-1 and the language here contradicts language in CIP-006-1. In section CIP-006-1 physical access controls, monitoring, and logging are all described in detail and there is no indication in that section that physical access must be authorized by a control or security center operator on an instance by instance basis. Please delete "instance by instance" and "control or security center operator" references in CIP-007-1.

CIP-007-1
B.R.3.4Access Reviews: Need standardization on the review periodicity throughout the document. This is one of the only sections that has a semi-annual requirement. Can't reviews be standardized generally on an annual basis?

CIP-007-1
B. R.4.2. & R.5.2.Review of Patches and Integrity Software: These sections specify a monthly review requirement. A monthly review is over-kill. Recommend that the period for review should be quarterly in these cases. Need standardization and consistency on the review periodicity throughout the document.

CIP-007-1 R.10.Operating Status Monitoring tools: This is another example of documentation that is not necessary. No specific operating status targets are listed. Therefore, this section simply generates documentation without relevance.

CIP-007-1 R11 Testing the stored information at least annually will result in a lot of work with very little benefit. Recommend that this requirement be eliminated.

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.

CIP-008-1
C.M.1. The wording in the draft standard does not make sense and seem to be missing verbiage. It seems the intent is to require the documentation be reviewed annually and updated within 90 days of a known change. Wording needs to be fixed to clarify the meaning.

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.

CIP-009-1 R4."…updates or changes shall be communicated to personnel…with seven (7) calendar days…" Time period is un-necessarily short. Recommend that updates be communicated quarterly. Timing for updates and reviews needs to be standardized and more consistent throughout the documents generally using quarterly or annual reviews/updates.

CIP-009-1 M4Requiring a drill "at least every 3 years" is too long a time period and the only place in the document where such a time period is recommended. Need standardization on the periodicity referenced throughout the documents, generally specifying annual requirements. Recommend change the drill requirement here to annual drill from at least 3 years.

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.

Self Certification, Page #1: Delete the references to self-certification in the Implementation Plan language. It is no longer relevant.

Implementation Plan for "Other Facilities" (not Control Centers): Some weeks ago, participants had been asked to provide an estimate of how long it would take them to implement the proposed permanent standards. Cinergy indicated that approximately four (4) years would be required. However, the NERC implementation plan states that all entities must be audibly compliant with all sections by 1st quarter of 2007. We once again state that it will take four (4) years to implement all requirements of the proposed permanent standards. One year will be spent planning and the remaining time will be spent in implementation. If the implementation plan is not adjusted for all CIP sections, then at least the following need to be moved back for "other facilities," which are not Control Centers:

- CIP006-1 Physical Security: It is not possible to implement the standards across the number of generation and substation sites involved by the 1st quarter of 2007. Deadline needs to be moved back as indicated by the participants.
- CIP-003-1 Security Management Controls: It is not possible to implement the requirements, such as change management, password management, operating system monitoring tools, and testing, using the existing legacy EMS system. A new EMS system is on order and should provide the needed controls by early 2008.
- CIP-007 Systems Security Management: It is not possible to implement the requirements such as change management, password management, operating system monitoring tools, and testing, using the existing legacy EMS system. A new EMS system is on order and should provide the needed controls by early 2008.
- CIP-005-1 Electronic Security: Being able to sufficiently monitor the sites is tied to new capability to be delivered with the new EMS system. Due to the new requirements and number of sites which are involved, this requirement will be difficult to implement by 1st quarter of 2007.

Implementation Plan for Control Center Requirements to be Audibly Compliant by 1st Quarter of 2006, Page #2: We were told by an ECAR representative that Control Centers would be required to be 'audibly compliant' by 1st quarter of 2006 with those requirements, which were "direct descendent" of Standard 1200. In many cases the Control Centers are expected to be audibly compliant by 1st quarter, but the increase in scope has significantly altered the requirements in CIP-002-1 through CIP-009-1 vs. Standard 1200. Because the scope of the permanent standard has expanded so much over the requirements of Standard 1200, there are very few 'direct descendents' from Standard 1200 to the proposed permanent CIP-002-1 through CIP-009-1. For all of the items listed below, because the scope has increased, we do not agree that these are 'direct descendents'

and we recommend that Control Areas should be given until 1st quarter of 2007 to be "audibly compliant."

For all of the following requirements, the Control Centers must now be Auditably Compliant by 1st Quarter of 2006.

For Control Centers, deadline to be Auditably Compliant should be changed to 1st Quarter of 2007, not 2006.

Comment

CIP-002-1

R1 Parameters for List of Assets This requirement is NOT a "direct descendent" of Standard 1200 requirements because the parameters for the requirement are significantly different from Standard 1200. (IROL's, etc.)

R2 Routable protocol/dial up accessibility This requirement is NOT a "direct descendent" of Standard 1200 requirements because the parameters for the requirement are significantly different from Standard 1200. Differentiations such as routable protocol and dial up accessibility do not exist in Standard 1200.

R4 Approval of list of assets This requirement is NOT a "direct descendent" of Standard 1200. Approval of the list by senior management is a new requirement.

CIP-003-1

R2 Categorize ALL information This requirement is NOT a "direct descendent" of Standard 1200 and goes MUCH farther than Standard 1200. Categorizing ALL of the information regardless of media type, senior management involvement etc. is a new requirement.

R3 Roles & Responsibilities This requirement is NOT a "direct descendent" of Standard 1200. Defining the roles and responsibilities of all parties involved is a new requirement.

R4 Governance Documentation This requirement is NOT a "direct descendent" of Standard 1200. Documenting a formalized governance process was not required in Standard 1200.

CIP-004-1

R1 Awareness Program This requirement is NOT a "direct descendent" of Standard 1200. A separate "Awareness Program" was not required in Standard 1200.

CIP-005-1

R1 Electronic Perimeter This requirement is NOT a "direct descendent" of Standard 1200. Because the scope of CIP-005 has been expanded to include access from sub stations and generation facilities, the electronic access requirements to the perimeter have been expanded.

R4 Electronic Access Controls This requirement is NOT a "direct descendent" of Standard 1200. Electronic Access controls to the EMS system will have to be created for substations and for generation facilities.

R5 Monitoring Electronic Access. This requirement is NOT a "direct descendent" of Standard 1200. Means to monitor access controls to the EMS system will have to be created for substations and for generation facilities.

R6 Documentation This requirement is NOT a "direct descendent" of Standard 1200. Because the scope of the new permanent standard has been significantly increased, much new documentation is now required over and above Standard 1200 requirements.

CIP-006-1

R2 Access Controls following risk assessment This requirement is NOT a "direct descendent" of Standard 1200. The generally accepted industry or government risk assessment procedure was not required in Standard 1200.

R5 Maintenance & Testing Program This requirement is NOT a "direct descendent" of Standard 1200. Maintenance and Testing program was not required in Standard 1200.

R6 Documents This requirement is NOT a "direct descendent" of Standard 1200. Because the scope of the permanent standard has been significantly increased over Standard 1200, additional documentation is required.

CIP-007-1

R1 Testing & Environment This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as documenting full detail of the test environment were not part of Standard 1200. Separating requirements for attended vs. un-attended facilities were not part of Standard 1200.

R3 Account & Password Mgt. This requirement is NOT a "direct descendent" of Standard 1200. The requirements for password management such as strong passwords and the distinction between controls for unattended vs. attended facilities are new to the current version and did not appear in Standard 1200.

R4 Security Patches This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as the monthly review and the risk based assessment are new requirements in this standard and were not part of Standard 1200.

R5 Integrity Software This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as the monthly review and the formal change control process for integrity software were not part of Standard 1200.

R7 System Logs This requirement is NOT a "direct descendent" of Standard 1200. Requirements such as the distinctions for managing logs at unattended facilities were not part of Standard 1200.

R8 Change Control This requirement is NOT a "direct descendent" of Standard 1200. The scope of the requirements for change control has been expanded over the requirements of Standard 1200. Specifics regarding the assets at unattended facilities were not part of Standard 1200.

R10 Op. Status Monitoring This requirement is NOT a “direct descendent” of Standard 1200. Operating Status monitoring and performance monitoring tools requirements have been significantly expanded over Standard 11200 requirements.

R11 Backups & Recovery This requirement is NOT a “direct descendent” of Standard 1200. Items such as the requirement that the backup must be stored in a remote locations and the requirement for annual tests to ensure recoverability are new to this standard.

CIP-009-1

R4 Notification of changes This is not a “direct descendent” of Standard 1200. There was no requirement to notify personnel of changes within 7 calendar days of the modification.

R5 Recovery Plan Training This is not a “direct descendent” of Standard 1200. Standard 1200 did not contain a requirement that all the testing mirror testing defined in current CIP-004 Personnel and Training.

Requirement	Ongoing	Within 30 Calendar Days	Monthly	3-6 months	90 calendar days	Quarterly	Semi Annual	Within Last Calendar Yr.	Annual	Other	Comments
CIP-002-1 List of Assets											
M4. Update documentation within 30 calendar days of adds, removes, modifications to critical asset lists		X									
D.1.2 Verify annually that updates were made in 30 calendar days									X		
CIP-003-1 Security Management Controls											
M2. Cyber security policy review period not to exceed 3 years										Not to exceed 3 years	
M4. Review deviations at least annually									X		
M5. Review information security protection at least annually									X		
M6. Assess information security protection program at least annually									X		
M8 Assess information identification at least annually									X		
M.11 Changes to sr. management official documented within 30 calendar days of effective date.		X									
M12. Review Roles & Responsibilities at least annually									X		
M13. Review internal corporate relationships and processes at least annually									X		
M13.1. Maintain current of designated personnel for authorizing systems suitable for the production environment.	Current										

Requirement	Ongoing	Within 30 Calendar Days	Monthly	3-6 months	90 calendar days	Quarterly	Semi Annual	Within Last Calendar Yr.	Annual	Other	Comments
M14. Maintain current list of personnel responsible to authorize access to CCA's	Current										
M15. Review list of authorizers annually.									X		
M16. Review process for access at least annually.									X		
M17. Review access documentation at least annually.									X		
M 18. Review user access rights at least annually.									X		
2.1.2 Non compliance if not reviewed in the last calendar year. Conflicts with M2 above.								X			
2.1.3 Deviations are not documented with 30 calendar days of the deviation		X									
2.1.4 Review information security program in last calendar yr.								X			
2.1.5. Review process to protect information in last calendar yr.								X			
2.2.2. Assess access to critical cyber information in last calendar yr								X			
2.3.4. List of designated approving authorities is not up to date	Level 3 violation if not current										
2.4.7 Access authorization not reviewed in last calendar yr								X			

Requirement	Ongoing	Within 30 Calendar Days	Monthly	3-6 months	90 calendar days	Quarterly	Semi Annual	Within Last Calendar Yr.	Annual	Other	Comments
CIP-004-1 Personnel & Training											
R2. Training program will be reviewed annually.									X		
M.1. Awareness reinforcement to be used at least quarterly						X					
M3.2. Maintain documentation of review and update of training program annually.									X		
M4.2 Review list of authorized personnel quarterly and update the listing within 7 calendars of a "substantive change"						X				Within 7 calendar days of 'substantive chg'	
M4.3. Access revocation within 24 hrs. for cause and 7 calendar days for normal chg in status.										24 hrs. for cause; 7 calendar days for others	
M4.6 Update personnel screenings every 5 years										Every 5 years	
D. 2.1.1. Access control rights not been reviewed for more than 3 months. See Section CIP 003-1 review requirements appear to be annual.				X							See CIP-003-1 Access review non-compliance - requirements appear to be in the last calendar yr.
CIP-005-1 Electronic Security											
R6. All documents reviewed at least every 90 calendar days and update all documents within 30 days following implementation.		X Update			X Review						

Requirement	Ongoing	Within 30 Calendar Days	Monthly	3-6 months	90 calendar days	Quarterly	Semi Annual	Within Last Calendar Yr.	Annual	Other	Comments
M4.2.3. Periodic review of authorization rights in accordance with CIP-003										Refers to a different standard	All requirements should be contained within that standard rather than cross referencing other documents.
F6. Review documents reference in this standard at least annually and update within 30 calendar days of modification.		X Update							X Review		
CIP 006-1 Physical Security											
M1. Review and update security plan at least annually or with in 90 days of modification					X Update				X Review		
M5. Retain physical access logs for 90 days.					Retain for 90 days						
M6. Document maintenance and testing annually									X		
2.1.1. Documents have not been updated or reviewed in the last 90 days					X						Note: Other language in this section implies documents need only annual review unless modified.
CIP 007-1 Systems Security Management											
R4.2. Perform a monthly review of the security patches			X								
R. 5.2. Perform a monthly review of the integrity software.			X								

Requirement	Ongoing	Within 30 Calendar Days	Monthly	3-6 months	90 calendar days	Quarterly	Semi Annual	Within Last Calendar Yr.	Annual	Other	Comments
R. 6.1. Vulnerability assessment to be conducted annually.									X		
R. 7.1. Retain log data for 90 calendar days					X						
R 11. Information stored shall be tested at least annually.									X		
M2. Access changes with 24 hrs. for cause and 7 days for normal change.										24 hrs. for cause. 7 days for other.	
2.2.1.1. Non Compliance unless a semi-annually review of attended facilities takes place (periodically for un-attended)							X				Where is this required? Only found periodicity ref. In non-compliance
CIPP 008-1 Incident Response Planning											
M.1.Maintain documentation at least annually or within 90 calendar days of known changes.					X for Changes				X		
CIPP 009-1 Recovery Plan											
R1. Exercise recover plan at least annually									X		
R.3. Update recovery plan within 90 calendar days of any major change.					X for Changes						
R. 4 Communicate updates or changes in recovery plan to personnel responsible within 7 calendar days of modification.										Within 7 calendar days.	

M.2 Responsible Entity shall review and update its response to events of varying duration and severity annually or as necessary.									X.		Seems to conflict with R.3 within 90 calendar days for change.
M. 3. Responsible Entity shall review and update recovery plans annually.									X		

REFERENCE										
C.M2. Responsible Entity shall review cyber security policy with a minimum review period not to exceed 3 years. Section 2.1.2 Then makes it a non-compliance violation if the policy "has not been reviewed in the last calendar year." There are too many different timing references in the document. All requirements, measures, and non-compliance items need to be reviewed to ensure timing requirements are consistently represented throughout the document. Standardize the reviews to generally annually to simplify this process.										
Another example of the same type of problem noted above. CIP 004-1 2.1.1 Level 1 non-compliance for Access control rights not been reviewed for more than 3 months. The requirement for a quarterly review is not spelled out in the requirements of CIP 004. There are Measures and requirements in Section CIP-003-1 that deal with review of roles & responsibilities of Critical Assets users and timing for review specified in annually.										
Sometimes the timing requirements for the review can be found in the requirements section, sometimes in the measures section and sometimes the only requirement shows up in the non-compliance violations. These references need standardization as to where they are presented and also the frequency needs standardization!										

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:	Jim Hiebert	
Organization:	California ISO	
Telephone:	916-608-1254	
Email:	jhiebert@caiso.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: WECC EMS Working Group

Lead Contact: **Jim Hiebert**

Contact Organization: **California ISO**

Contact Segment: **2**

Contact Telephone: **916-609-1254**

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

Additional Member Name	Additional Member Organization	Region*	Segment*
Erika Ferguson	**IPCO**	**WECC**	
Michael Roberts	**PG&E**	**WECC**	
Robert Matthews	**PG&E**	**WECC**	
Hein Gerber	**BCTC**	**WECC**	
Chuck Nichols	**BCTC**	**WECC**	
Robin Rice	**IPCO**	**WECC**	
Sherwin Tanner	**IPCO**	**WECC**	
Terry Ryan	**IPCO**	**WECC**	
Paul Emmerich	**SRP**	**WECC**	
Jagjit Singh	**SRP**	**WECC**	
Tom Glock	**APS**	**WECC**	
Jim Hansen	**SCL**	**WECC**	
Gary Bruckner	**PG&E**	**WECC**	
Jon Stanford	**BPA**	**WECC**	
Terry Doern	**BPA**	**WECC**	
Bill Gibbons	**TEP**	**WECC**	
Gray Wright	**SPPC**	**WECC**	
James Sample	**CAISO**	**WECC**	
Randy Schimka	**SDG&E**	**WECC**	
David Ambrose	**WAPA**	**WECC**	

* 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.

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.

1. The definition of Cyber Assets should be clarified to specifically exclude communication links connecting electronic perimeters. You could add the sentence: For the purpose of this standard, communications links connecting discrete electronic permiters are excluded. 2. The term 'Authorized Access' is used in CIP-004,005, and 006 but not defined here. Please add a definition for this term, and specifically describe whether it is intended to mean authorized electronic access, physical access, or both. This would help us understand the intent of these sections. It may be appropriate to spell out physical or electronic (or both) where appropriate in the standard. Training requirements for staff granted authorized physical access but not electronic access would be different than staff granted both for example. If this term means physical access, it would be helpful if exemptions (such as escorted visitors) or any special circumstances were identified. Suggested definition would be: Access that is granted according to an established scheme of governance.

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.

Even though the above answer is Yes it is still unclear on how to identify critical assets. We would like to see the process and a flow chart on how to identify critical assets.

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.

1. CIP-002 to 009: Please tie measures to the pertinent requirements. This will assist us in insuring our compliance with these standards. 2. CIP-002 to 009: Please match compliance levels to specific measures. This will assist us in insuring we are aware of our current level of compliance. 3. CIP-002 to 009: There are overlaps and inconsistencies in some cases since different groups within the drafting team wrote these standards. For example in CIP-005 M5.1 Organizational controls are part of the measurement in this section but are already specified and measured in CIP-003. We recommend that a professional technical writer who can correct these problems in order to avoid causing confusion and unnecessary expense review these standards in total. 4. R1.1.1: The word 'performing' in the first sentence might be interpreted to mean 'actively performing'. This generally does not apply to backup control centers. If applied litterally, then backup control centers would not fall under this requirement unless they were actively performing one of the critical functions listed here. We believe the intent is to monitor these facilities 7x24 whether they are active or not. We suggest that the wording be changed to 'Control centers and backup control centers that, when operational, perform the functions of -' 5. R1.1.2: The use of the phrase 'such as', in this section, when taken together with the last sentence of R1.1 causes us some confusion. Do the authors intend to allow Responsible Entities to apply their risk-based assessment to identify which of these functions are critical to the operation of the control centers or is this a perscriptive list? If the latter, then the phrase 'such as' should be changed to 'shall include'. If not, then the phrase should be changed to 'for example' and it should be made clear that systems performing certain of these functions may not be critical to the operation of the control center. For example, control centers that are not transmission service providers may not need to include cyber assets running real-time power system modelling. Also, depending on the type of data being exchanged, inclusion of inter-utility data exchange may not be appropriate. 6. R1 and R2: It would helpful if a flow chart were provided that would provide the industry with a consistent approach to applying R1 and R2. 7. R1.1.3: The phrase associated with in the first sentence extends beyond equipment within the IROL transfer path. This requirement should state that anything not in the direct transfer path is excluded. Responsible Entities applying their risk-based assessment would identify anything outside the path that might impact the transfer path. 8. R1.1.7 Please tie the requirement to a specific criteria rather than 300 MW. 9. R2: A clarification was made during the conference call, and later confirmed during our WECC EMSWG meeting, that Cyber Assets using a routable protocol would not be considered Critical Cyber Assets if these assets were electronically isolated. In other words, there were no routable or dial-up electronic access points to the system. The requirements in this section do not state this however. The requirements need to be clarified to include this point. We suggest modifying R2.1 to state: The Cyber Asset uses a routable protocol for access from outside the electronic security perimeter. This will exclude power plants and substations that use a network of Cyber Assets to provide governor control, data acquisition, etc. but are connected outside their electronic perimeter by RTU protocol communications only. It would also exclude Cyber Assets in control centers and backup control centers that have no external electronic perimeter access points using a routable protocol or dial-up modem. 10. R4 Please clarify that senior management are not required to sign a detailed list of Critical Assets and Critical Cyber Assets. For example, we should be able to identify our control center and EMS system as critical assets and cyber assets respectively without providing

management with a detailed list of all of the critical equipment in each. 11. M5-6 should require annual review by senior staff. Signature and review on change would usually require daily or weekly review. 12. Compliance should be numbered in the same fashion as Requirementss (Rn) and Measures (Mn). example: R1.1, M1, C1.1.2. This would make it easier to refer to particular sections of the standard from documents and programs we develop for compliance. 13. Please remove the use of 'shall' in measures. 'Shall' should appear in the Requirements section only. For example in CIP-005 M1 – 'The Responsible Entity shall maintain' should be changed to 'The Responsible Entity maintains'.

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.

1. CIP-002 to 009: Please tie measures to the pertinent requirements. This will assist us in insuring our compliance with these standards. 2. CIP-002 to 009: Please match compliance levels to specific measures. This will assist us in insuring we are aware of our current level of compliance. 3. CIP-002 to 009: There are overlaps and inconsistencies in some cases since different groups within the drafting team wrote these standards. For example in CIP-005 M5.1 Organizational controls are part of the measurement in this section but are already specified and measured in CIP-003. We recommend that a professional technical writer who can correct these problems in order to avoid causing confusion and unnecessary expense review these standards in total. 4. M5-10: Is there a difference between the Cyber Security Program in M10 and the information security protection program in M5? We're getting confused between the Cyber Security Policy, the Cyber Security Program, information protection security program, Cyber Security Standard (mentioned in R2.3), etc. Ideally, we'd like the standard to contain easy to identify documents that we can uniquevicollay relate to between requirements, measures, and compliance. In general this standard is well written but we believe could be cleaned up in order to minimze confusion. 5. D 2.1.1: There is no way to avoid at least level 1 non compliance the way this is written. For instance, a Responsibility Entity with a senior management official designated 100% of the time meets the criteria of a senior management official was not designated for less than 30 calendar days. It should be recognized that staff may decide to leave and it may take several days to appoint someone as acting senior management, or appoint alternative senior management. We suggest that this be changed to 20 or more but less than 30.

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.

1. CIP-002 to 009: Please tie measures to the pertinent requirements. This will assist us in insuring our compliance with these standards. 2. CIP-002 to 009: Please match compliance levels to specific measures. This will assist us in insuring we are aware of our current level of compliance. 3. CIP-002 to 009: There are overlaps and inconsistencies in some cases since different groups within the drafting team wrote these standards. For example in CIP-005 M5.1 Organizational controls are part of the measurement in this section but are already specified and measured in CIP-003. We recommend that a professional technical writer who can correct these problems in order to avoid causing confusion and unnecessary expense review these standards in total. 4. Throughout this section the term ‘authorized access’ is used. It is particularly critical to us that this term be clarified (physical or electronic access or both) throughout this section as stated in CIP-002 comments. Please ensure that the use of this term matches the definition if it is added to definitions. 5. R4 and M4.4: Both contain the phrase 'prior to'. Please clarify how existing staff should be handled. We specifically do not want to prohibit existing staff from having access while we are performing the required assessments. 6. R1, M1 and D2.1.5 use the term 'reinforcement' however there is no suggestion within the standard of what would meet NERC's minimum standard of awareness reinforcement. In the measure, e-mails are listed for example without indicating what the content should be. It may have been the drafting team's intent to leave this up to the companies to apply, however, in the interest of ensuring that we comply with the intent, it would be ideal to either specifically state in the compliance section that the content of awareness communications is totally up to the company and any content guarantees compliance, or state specific minimum content. Comment on the Measures: M4.6 – Instead of reading, 'The

Responsible Entity shall conduct update screenings at least every five years or for cause', should read, 'The Responsible Entity shall conduct personnel updates as per their documented company personnel risk assessment process at least every fives years or for cause'.

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.

1. CIP-002 to 009: Please tie measures to the pertinent requirements. This will assist us in insuring our compliance with these standards. 2. CIP-002 to 009: Please match compliance levels to specific measures. This will assist us in insuring we are aware of our current level of compliance. 3. CIP-002 to 009: There are overlaps and inconsistencies in some cases since different groups within the drafting team wrote these standards. For example in CIP-005 M5.1 Organizational controls are part of the measurement in this section but are already specified and measured in CIP-003. We recommend that a professional technical writer who can correct these problems in order to avoid causing confusion and unnecessary expense review these standards in total. 4. Throughout this section the term 'authorized access' is used. It is particularly critical to us that this term be clarified (physical or electronic access or both) throughout this section as stated in CIP-002 comments. Please ensure that the use of this term matches the definition if it is added to definitions. 5. R1 - There is a variety of equipment and software typically used in electronic security perimeter access control. We believe that this is what was intended by the word 'logical' in this section. Can you state this more clearly and also ensure that associated measures and compliance levels incorporate the concept that the electronic access point can be this group of hardware and software used to secure the perimeter? In some cases, a single system may be used in more than one logical perimeter. For example, a router may be used to implement level 1 and 2 security and a variety of target machines may implement other levels. 6. Please remove the use of 'shall' in measures. 'Shall' should appear in the Requirements section only. For example, M1 – 'The Responsible Entity shall maintain' should be changed to 'The Responsible Entity maintains'. 7. R3 – 'unattended' usually has no bearing on securing and being aware of dial-in access. Should this second sentence read '…dial-up equipment shall be…' instead? 8. R4.2 - Should the word 'logical' in the first sentence be removed? 9. R4.2 The measures would be more clear if specific examples were included. 10. R5 Please include 'where technically feasible' as this is not always possible with existing systems. 11. R5 'Monitoring' implies active notification 7x24 when the events specified occur. In the case of Authorized Access, 'Logging' for audit purposes is important, however active notification is not. For unauthorized access attempts, (internally or at electronic perimeter(s)) active monitoring should be used. Please modify R5 to remove the requirement for monitoring authorized access. 12. R4 appears to be written with human access rather than software access to systems. Either can be 'interactive'. We have numerous interactions with specific computers using specific ports and protocols in various DMZ's outside of the electronic security perimeter of our EMS. A variety of methods are used to ensure that logins are never presented to anyone who could gain access to these systems outside the security perimeter and attempt unauthorized access. For example, a custom program receiving XML data delivered by another program across a normally unused port will reject any message that does not match the schema. While it is possible that someone could send a bogus XML data set complying with the schema. The damage would be limited to overwriting data that we could easily recover without threatening the reliability of the grid. The bullets in R4.2 do not cover any of these methods

however we believe they effectively limit access through our electronic security perimeter. Would you please split R4 into two requirements? One governing login access or access on defined ports, and the other programmatic access using specialized application software and interfaces on non-standard ports? 13. M4 and 5 also appear to have been written with login access in mind. If you split R4 into two requirements as requested above, can you also create separate measures? It is not necessary to log authorized programmatic access for example when thousands of transactions using different sessions are conducted each hour. 14. M1 Since this standard focuses on Cyber Security, the document described in M1 should be limited to contain only the Electronic Security Perimeter(s). The remainder of the sentence should be struck as it is outside the scope of this SAR, increases the cost of compliance, and does nothing to increase Cyber Security.

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.

The WECC EMSWG is deferring this section to the WECC Physical Security Working Group chaired by Tom Glock.

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.

Comment on the Introduction/Purpose: The sentence that reads, 'A System Security Management Program is necessary to minimize or prevent the risk of failure or compromise from misuse or malicious cyber activity' should read 'A System Security Management Program is necessary to ensure system availability and integrity by minimizing or preventing malicious and non-malicious activity and misuse, whether authorized or unauthorized. This includes measures necessary to detect, document, and counter such threats.' 1. R1. In the second paragraph, please clarify that a non-production environment can be a production system that has been removed from production mode. This covers the case where non-production testing is not possible, on obsolete equipment for example, while achieving the goal of this section that is to ensure that testing is done safely. 2. R1 requires that we add another layer of tests to our existing test procedures, testing that a vendor's security patches for known security vulnerabilities work correctly. This causes us several problems. For example, we have Solaris Unix systems from Sun. Sun tests their patches prior to releasing them (just as Microsoft is starting to do). We install necessary patches and then verify that the patches were installed correctly. We believe that the vendor should be held accountable for ensuring their security patches actually remove the vulnerability. If damages resulted from the patch not correcting the vulnerability, then the vendor would be held liable. Second, the cost of testing, in both human and financial resources is high. The new CIP standards are already creating a significant increase in resource utilization. We believe it would increase security for us to concentrate our resources on more critical security issues. Third, we do not believe that requiring the industry to test the security patches from vendors is effective in increasing security. Pressure is already placed on the vendors when the computer user industry finds that a security patch does not correct the problem. The operating system vendors have significantly increased their quality assurance testing as a result. If this requirement is not removed from the standard, we will be forced to vote 'no' on CIP-007. 3. R2 should be reworded. We suggest 'The Responsible Entity shall store test documentation, security procedures, and acceptance procedures for Critical Cyber Assets located at unattended facilities at a facility that is staffed 7x24. These documents must not be stored in a facility that is unattended at any time.' The second sentence should be removed since it would be possible to conduct security test procedures at the unattended facility simply by going there and conducing tests on a non-production environment located at that facility. The location of the non-production test environment is not something that should be specified. 4. R3. Entities should be required to 'perform account management to provide for access authentication…' or 'follow an account management program' rather than 'establish an account password management program'. Our program already exists and generic programs that meet these requirements are specified in standard security documents. 5. R3.1 change 'shall use accounts that have a strong password' to 'shall require and utilize strong passwords'. 6. R4.2 requires a monthly review of available security patches. Our vendor provides us with critical security alerts tat we respond to immediately. Our normal cycle for non-critical security patches is to review and download them every 6 months because it takes at least a month to adequately test our EMS applications. Given the other measures employed on our electronic security perimeter in conjunction with the security alert program, we believe that a monthly review requirement is much too frequent. We request that this sentence be struck. 7. In R5, we take 'Integrity Software' to

mean that set of software commonly called ‘anti-virus software’. Is that the intent or is something else meant? In either case, can you clarify with specific examples or more common terminology? 8. R5.1 We believe the drafting team intended for this integrity software to be run on all Critical Cyber Assets within the Electronic Security Perimeter. However R5.1 does not clearly state this requirement. 9. R6.3 Doesn’t this apply to all facilities? 10. R11. As stated in comment 3 above, the location of the non-production test environment is not something that should be specified in any of the CIP standards. Please remove the last sentence so that we can test at an unattended facility if we happen to have a test environment there. 11. M2 typo ‘n’. 12. M10 in general should consider the use of other backup media. Specifically, ‘backup data and tapes’, and ‘backup data’, should be replaced with ‘backup media’.

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.

This Section refers to the NERC Security Guidelines for the Electricity Sector Threat and Incident Reporting that uses the term 'any suspicious event' as a requirement for incident reporting. The concern is that 'any suspicious event' could include most firewall interceptions (and there may be hundreds/day) and that we have 60 minutes to report them [day or night] or be assessed a level-3 non-compliance penalty. We need better definition here.

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.

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.

We like the implementation timeline matrix however it is tied to a specific date rather than the date of adoption of the standard. If the standard isn't adopted until the fourth quarter of 2005, then we are left with very little time to implement. Implementation of the plan in anticipation of a successful ballot without a ratified standard to refer to would be probelmatic if not impossible. We would like the implementation plan to tie its first due date to 6 months after the standard is adopted with all other dates changing, as in a gant chart

General Comments: 1. Should clearly correlate 'Requirements' to 'Measures' and 'Measures' to 'Compliance'. This way there is a clear relationship all the way from requirements to compliance. Currently it is hard to correlate this and it appears that in several cases they don’t correspond with each other. 2. The term 'shall' is used in both the 'Requirements' and 'Measures' sections. The term 'shall' should only be used in the 'Requirements' section and the 'Measures' section shouldn’t use 'shall' but rather performance language. 3. This standard should be broken up into two distingue standards. One with specific requirements for Control Systems and one with specific requirements for plants and sub-stations. This standard seems to be more focused on Control Systems where the requirements seem to fit very well, however, due to the technology, etc. at plants and sub-stations, these requirements don’t fit as well. Also, there is a different risk model for Control Systems versus plants and sub-stations. Due to the risk difference there are should be distingue requirements for each. 4. Technical feasibility – along the lines of the comments above in 3, if this standard isn’t separated between Control Centers, plants, and sub-stations it should take into consideration the technical feasibility of the requirements and annotate it so that the 'exception to standard' overhead doesn’t get out of hand. We don’t want to make this counter productive by creating a massive about of paperwork administration not allowing us to focus on the spirit of the standard.

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:	Robert L. Sypult	
Organization:	Southern California Edison	
Telephone:	626-302-7910	
Email:	Robert.Sypult@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.

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.

N/A

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.

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.

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.

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.

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.

Section CIP 005-R3 instructs HOW to implement this standard, as opposed to defining the specifics needs. It is too prescriptive. This section only needs general guidelines and the responsible entity can determine HOW to meet the compliance requirments. This section should simply state "Responsible entity shall secure dial-up modem connections", and let the responsible entity determine HOW to accomplish that

Section CIP 005-R4.2 This section is also too prescriptive, and it is questionable if some of the bullet items included would be feasible (e.g., "In dial-up access, call back to augment static user id and password authentication"). We do not feel we should be instructed on how to specifically address the problem in terms like "…..include at least one of the following measures:", but this section should be modified to reflect "….these strong procedural or technical measures shall include measures like……" and let the responsible entity determine the appropriate measures to address the concern..

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.

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.

CIP-007-1.R6.1.2 - Scanning for open ports/services and modems. It should be clearly stated that ANY penetration testing/scanning for vulnerabilities is NOT to be performed on the production system, it will ONLY be performed on either the backup control center or the test system configured and running like the production system. In the case where it is not possible to perform penetration testing on an off-line system (due to lack of back of control center or test system), an extensive review of hardware and software configurations shall be performed and documented.

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.

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.

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.

1st Quarter of 2006 is too tight of a timeline for "Auditably Compliant" requirements for Control Centers, as the Standards are not likely to be approved and issued until after 2006 budgets and training plans are developed in 2005. Control Centers should be classified as "Substantially Compliant" in 2006 and "Auditably Compliant" in 2007 and beyond.

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:	Greg Mason	
Organization:	Dynegy Generation	
Telephone:	217 872-2301	
Email:	gregory.mason@dynegy.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.

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.

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.

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.

Section R.1.1.6 defines all Blackstart generators(regardless of size) as Critical Assets.Analogous to Sections R.1.1.4 and R.1.1.5,we recommend that a size limitation be established whereby all Blackstart generators below the specified size limitation are not defined as Critical Assets.One option would be to base the size limitation on a net MW output level.If this approach is adopted,we suggest 25 MW be established as this size limitation.A second option would be to base the size limitation on a % of the total blackstart capability within a Reliability Region or ISO.If this approach is used,the Reliability Region or ISO would need to be involved in setting this percentage.

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.

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.

Requirements R1-R4 and Measures M1-M4 ignore the current industry trend to outsource certain functions such as IT support to third parties at remote locations. These Requirements and Measures are not practical to implement in this type of business environment.Also,as stated in the recent NERC Cyber webcast,if you are not applying these types of Requirements and Measures to third party telcom providers(who have the ability to impact Critical Asset operation),it would be inconsistent to apply these Requirements and Measures to providers of outsourced IT support.We request that either this Standard be modified or a FAQ be developed to exempt providers of outsoured IT support from these Requirements and Measures.

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.

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.

Measure M3 needs to be clarified for Critical Assets in office buidings.This Measure should state that 4 wall security plus additional security monitoring of the surrounding access areas(i.e hallways,etc.) is sufficient to meet the intent of this section for this type of environment.Development of a FAQ on this issue would also be helpful.

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.

Section R3.2 currently only allows the use of group accounts if individual accounts are not technically supported.This section needs to be modified to unconditionally allow the use of group accounts as long as the associated audit trail and account security steps referenced in this section are maintained.These changes will still meet the intent of this section without the imposition of unnecessary costs.The FAQ on this issue also needs to be revised accordingly.

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.

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.

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.

The Implementation Plan needs to clarify the provisions that some entities need to be only "Substantially Compliant"(begun process to become compliant) by 1Q 2006,but it appears they will receive Self Certification forms to certify their compliance shortly after 1Q 2006.Is it the intent to only send these Self Certification forms to those entities required to be "Auditably Compliant" by 1Q 2006?

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:	Carol L. Krysevig	
Organization:	Allegheny Energy Supply Company	
Telephone:	(412) 858-3657	
Email:	ckrysev@alleghenyenergy.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.

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.

Critical Asset – Recommend changing the definition to read as follows: 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, 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. Our recommended change added the word OR at the start of the phrase dealing with detrimental impact. Also, the definition of Critical Asset should refer to the Standard that defines which assets are to be included in the list (CIP-002-1, Requirements).
Cyber Assets – Since most newer electronic devices in a power station can be programmed (configured), this definition should include verbiage that specifically denotes connection to an externally accessible network. This should eliminate additional unintended devices from being deemed cyber assets.
Cyber Security Incident – Recommend changing the first bullet in the definition to read as follows: Compromises or was an attempt to compromise the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,. As originally written, the definition leads one to believe the word PERIMETER only applies to Physical Security.
Physical Security Perimeter - Note that in a power station there is network wiring that does not and cannot be reasonably segregated with a physical perimeter. In some cases, this wiring runs through open cable trays throughout the plant. Is the intent of the Standard to require protection for items such as this?

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.

R1. and R1.1 - Need to resolve the conflict between using a risk-based assessment to identify Critical Assets and the Critical Assets that NERC has identified for us. What takes precedence? Are the assets identified by NERC minimum requirements? Can our risk assessment override the Critical Assets listed by NERC? If that is the intention, then the last sentence of R1.1. should be reworded as follows: Those Critical Assets may include the following: .
R1.1 through R1.8 – If a risk based assessment is required for these listed critical assets, a provision should be provided for Responsible Entity Senior Management to deem that an asset that meets one of the these criteria is NOT a critical cyber asset based on the risk based assessment results.

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.

R1.6 and R1.7 – Provide clarification regarding the difference between these two listed items (common control system vs. control center).
R1. and R1.1. – These items do not address the potential conflict if there are overlapping responsibilities between Responsible Entities. For example, can a Reliability Coordinator choose which assets belonging to or operated by a Generation Owner or Generation Operator are deemed Critical Assets?
R2.1. - For the technically minded, this definition is pretty vague. For example, a PC running Windows NT that is not connected to anything else, may internally use TCP/IP for communications between separate programs running on that PC. By the current definition, this PC would be considered a Critical Cyber Asset. The definition should be more specific. For example, the following revision would clarify the Standard's intent: The Cyber Asset uses a routable protocol and is connected to a data network that is routing that protocol to a network connected outside the Electronic or Physical Security Perimeter. Another example is that DNP is a protocol that can be routed through the public telephone lines and tunneled through TCP/IP based networks. Allegheny Energy believes that an RTU having only a DNP via serial connection is not intended to be included on this Standard’s critical cyber asset list.

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.

General Comment – Confusion throughout this section in terms of understanding the difference between critical information about the Critical Cyber Asset (floor plans, etc.) vs. critical information emanating from the asset that is vulnerable to attack or acquisition by a hacker. Is the Standard asking us to categorize only the first type, or both? Allegheny Energy believes the Standard's intent is to protect the information ABOUT the Critical Cyber Asset. Can you please clarify?
R2.1 - Most Power Plant documentation contains significant amounts of information, cyber and non-cyber that could be used to hinder plant operation. The responsibly entity should be allowed to apply the same security measures to cyber documentation that it applies to other types of plant equipment and operating documentation.
R3. (Second paragraph) – Not sure how to define a Critical Cyber Asset custodian. Can clarification be made on the term custodian?
R4.1 – This item actually addresses two different items: a) Replacement systems and b) patches/changes to existing systems. Allegheny Energy recommends that the responsible entity establish security guidelines for new or replacement systems in lieu of the exact requirements defined here.
R4. 1 Testing and assessment of patches/changes should be allowed to be done by third parties on non-production systems.

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.

M4.4 - Reference to COMPANY PERSONNEL is confusing and should be clarified. Appears to imply that only employees need to have a personnel risk assessment while the implication of the standard is that all personnel (employee, contractor, vendor) who have unescorted access to critical cyber assets must have a personnel risk assessment completed.

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.

R1. Allegheny recommends that any devices controlling entry to the Electronic Security Perimeter should be considered Critical Assets. In other words, firewalls that protect an Electronic Security Perimeter should be considered as devices inside that perimeter.
R4.2 – Can you more specifically define INTERACTIVE, LOGICAL ACCESS? Almost any access could be deemed interactive since most data communication is bi-directional.
R5. - Some devices, such as PLCs, are not capable of being monitored for access. Responsible entities should be allowed to determine the assets inside the Electronic perimeter that need to be monitored directly. The only mandatory monitoring should be via the perimeter access device (firewall). Exact requirements such as this should not be specified. The responsible entity should create its own monitoring guidelines if desired.
D. Compliance, 1.3. Data Retention - The text in this section appears to be a carry over from the previous Standard's Data Retention section (personnel and training) and should be modified accordingly.

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.

General Comment – As mentioned in Allegheny Energy Supply's general comments, there are still a significant number of items in this draft that do not take into account the environment, physical and electronic, of a power station. Therefore, consideration should be given to a plant's overall physical security program and the complexity in trying to physically secure the cyber assets typically spread throughout the facility

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.

R1. - Will third party testing be allowed? Power stations have a fairly wide variety of specialized equipment and having non-production systems for each type of equipment is not feasible.
R3. – How are devices that do not support any type of passwords to be handled? The responsible entity should be able to devise its own guidelines and requirements.
R3.2 - In power station control rooms, generic accounts are used. In some cases because they are required by the application software, and in other cases because these systems cannot be unavailable for use at any time. If there is no other alternative, this type of account should be allowed, but computers using this type of account should be configured to disallow any kind of administrative access using these accounts, if possible. The responsible entity should be allowed to devise its own guidelines and requirements.
R7. - Some systems will be very difficult if not impossible to configure for this type of logging. The responsible entity should be allowed to implement logging on those systems they deem need it.
R9. - This is a duplicate. It has also been covered in Standard CIP-005-1.

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.

R4. Does the Standard infer that the Regional Reliability Organization (or someone else) might be used as an INTERMEDIARY to report incidents?

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.

Purpose - In this draft, NERC said that paragraph three was moved to the FAQ for the following reasons: it primarily explained the degree of recovery required in consideration of the expected impact and risk involved. However, it looks as though NERC actually moved the second and third paragraphs to the FAQs, and may have inadvertently removed the statement that describes the intent of this section. All that remains in the Purpose section of this draft is the boilerplate first paragraph (that's contained in all standards) that describes the overall purpose of Cyber Security. Following is the language provided in Draft 1:
1308 Recovery Plans (Draft 1 language) -

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 above Draft 1 language indicates that the intent of the standard is as follows: to establish recovery plans and put in place the physcial 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. If the intent is NOT as stated above, then please provide alternative guidance.
R1. - Allegheny Energy recommends that the EXERCISE of recovery plans for Power Stations should only be done for each representative type of equipment based on a plan derived by the responsible entity. Exact requirements should not be specified by this standard.
R4. – This Requirement appears to be more of a measure that a requirement.
R3 and M3 – This Requirement and Measure appear to conflict. R3 says you have to update a plan within 90 calendar days of a major change, while M4 says plans need to be updated annually. The verbiage should be modified to state: to be updated at least annually, or within 90 days of a major change.

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.

The requirements section of the compliance schedule do not match the actual standards. As such, a complete determination cannot be made. However, the electronic and physical security, as well as the systems security, sections CIP-005, CIP-006, CIP-007 should only be required to be auditably complete by 1st Qtr 2008. For Power Stations, there are potentially a significant number of systems that could be affected, requiring significant changes, upgrades, and new equipment to comply with these sections. Without actually performing the risk based analysis and cyber asset review, additional details are not available.
CIP-001 does not have sections R2-R4 which are documented in the implementation plan.
CIP-002 has section R-5 which is not documented in the implementation plan.

February 17, 2005

NERC CYBER SECURITY STANDARDS CIP-002-1 THROUGH CIP-009-1
ALLEGHENY ENERGY SUPPLY COMPANY

General Comments and Questions:

1. Why was the reference to penalties/sanctions removed from the Standards without being mentioned as a change from the Urgent Action Standard 1200?

2. There are still a significant number of items in this draft that don't take into account the environment, physical and electronic, of a power station. If someone accesses the "physical perimeter" of a power station, they would be able to cause an outage, through “non-cyber” means, if sufficiently motivated regardless of the kinds of cyber precautions undertaken. This standard should concentrate on preventing “cyber” attacks from locations outside the “physical perimeter” and “electronic perimeter”. Therefore, in order to not create non-uniform requirements between cyber and non-cyber security requirements, the exact means of accomplishing this should be determined by the responsible entity. Prescriptive requirements as defined in the sections of this standard should not be mandated, but rather moved to separate document of “potential safeguards” or “frequently asked questions”.

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:	Linda Campbell	
Organization:	F.R.C.C	
Telephone:	813-289-5644	
Email:	LCampbell@frcc.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: Florida Reliability Coordinating Council, Inc.

Lead Contact: **Linda Campbell**

Contact Organization: **FRCC**

Contact Segment: **2**

Contact Telephone: **813-289-5644**

Contact Email: **LCampbell@frcc.com**

Additional Member Name	Additional Member Organization	Region*	Segment*
Joel De Granda	Florida Power and Light	FRCC	2
Sergio Guzman	Florida Power and Light	FRCC	2
Ray Falcon	Florida Power and Light	FRCC	2
Linda Campbell	F.R.C.C.	FRCC	2
Alan Gale	City of Tallahassee	FRCC	5
William Baldwin	Ft. Pierce Utilities Authority	FRCC	1
Paul Elwing	Lakeland Electric	FRCC	1
Tim Beyrle	Utilities Commission of NSB	FRCC	1
Mark Bennett	Gainesville Regional Utilities	FRCC	5
Paul Elwing	Tampa Electric Company	FRCC	5
Ginny Jones	Tampa Electric Company	FRCC	5
Greg Ramon	Tampa Electric Company	FRCC	5
Wayne Lewis	Progress Energy Florida	FRCC	5
TC Thomas	Progress Energy Florida	FRCC	5
Renny Ramai	City of Homestead	FRCC	1
Ted Hobson	JEA	FRCC	1
Steve Wallace	Seminole Electric Cooperative	FRCC	4

* 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.

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.

There are several issues that need to be addressed before these definitions can be accepted and added to the NERC Glossary.

1. Critical Asset in Draft 2 was previously identified as "Bulk Electric System Asset" in Draft 1. Areas of concern are:

A. The definition should help responsible entities identify critical assets that comprise the "Bulk Electric System" and not make any ambiguous references such as "large quantities", "extended period of time", "detrimental impact", or "significant impact." The NERC Glossary (Version 0 - Draft 4, January 7, 2005) has already defined the Bulk Electric System as being "defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment generally operated at voltages of 100kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition." None of the definitions in the NERC Glossary use the words, "large quantities", "extended", "detrimental impact", or "significant impact."

B. The definition as written in this standard would allow for "scope creep." Scope creep results from a failure to establish clear definitions. It should not be the intent of this standard to impact responsible entities more than necessary. NERC reliability standards should only apply to the facilities of the bulk electric system. The definition now implies facilities all the way down to the distribution level. In fact, including public health and safety is extremely broad.

C. This definition will be added to the NERC Glossary upon approval, when that happens the definition can be utilized by and have impact on other NERC standards, therefore this standard should be very specific, instead of ambiguous.

D. The standards drafting team received 16 comments regarding the ambiguities of words such as "large quantities", "extended period of time", "detrimental impact", and "significant impact" on the previous posting. In response, the drafting team stated on page 226 of 808 of the "Cyber Security Comments and Drafting Team Responses" that "Such phrases as "large quantities of customers" and "extended period of time" have been removed." In fact only the name has been changed, the definition remain exactly same as in Draft 1.

E. CIP-002-1 Purpose section states that the standards intent is to ensure measures are in place to protect assets that are needed "for managing and maintaining a reliable bulk electric system." No where in the definition of "Critical Asset" is the bulk electric system mentioned. This definition needs to be changed in order to ensure that the scope of this standard is limited to only the critical assets that support the bulk electric system.

Proposed language would be:

Critical Asset: Those facilities, systems, and equipment, which if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the bulk electric system.

2. The Cyber Asset definition must be restated, since it refers to the "bulk electric system assets" which have been renamed as only "Critical Asset" in Draft 2.

Proposed language would be:

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data associated with critical assets.

The definition of Critical Cyber Assets should be changed to incorporate the characteristics as described in CIP-002-1, Section R2.1., R2.2., and R2.3.

The proposed definition is as follows: (this definition change has also been added to our comments on CIP-002-1.)

Critical Cyber Assets: Those Cyber Assets essential to the reliable operation of Critical Assets having the following characteristics:

1. The Cyber Asset uses a routable protocol, or
2. The Cyber Asset is dial-up accessible.
3. Dial-up accessible Critical Cyber Assets which do not use a routable protocol require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter.

3. “Exemptions” is still a term used in CIP-002-1 Measures (C.M3, C.M4 (used twice) and Compliance (D.1.3.3). This term is used no where else and is not defined.

Exceptions and deviations are used throughout the standards, and while described as different in the answer to our previous comments (deviations are where you meet part but not all of standard; exception is where you meet no parts of the standard), neither the standard nor the FAQ differentiates the terms. Question 4 in the FAQ describes documenting both in the same manner.

GENERAL COMMENT FOR CIP-002-1 THROUGH CIP-009-1

Nowhere in any of the standards does NERC detail the policies and procedures involved with removing confidential information or configuration information when equipment or other type of media are decommissioned.

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.

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.

During the conference call conducted for the first draft, we posed a question as to whether a facility that houses critical assets, but has no external connectivity, either dial-up or network, still fell under this standard. The response from the host of the session, Larry Bugh, was that these assets were not covered by this standard. During the Feb 2 conference call there was discussion around standard CIP-002, which implied that this may not be the case. Can the drafting team clearly address facilities that have no external connectivity, but house critical assets that run a routable protocol?

The standard does not clearly indicate wheather support systems such as cooling, UPS, generators, etc. that are outside the physical security perimeter should be considered critical assets. If these systems are considered critical assets, then they should be included in the physical security perimeter. The standard must define the outermost boundery of the physical perimeter.

R1.1 must be reworded so as not to regurgitate the definition of a Critical Asset. Critical Asset will be added to the NERC Glossary and will not need to be defined within the standard.

R1.1 should be reworded as follows:
Critical Assets: The Responsible Entity shall identify its Critical Assets, which consists of, but not limited to: monitoring and control, load and frequency control, emergency actions, contingency analysis, special protection systems, power plant control, substation control, and real-time information exchange. Those Critical Assets including the following:

R1.1.1. Should be stricken from the document. There is no need to duplicate the list of applicable functions as already listed the introduction's section 4. Applicability. Removing redundant information will ensure swift compliance and clearly delineate compliance measurements.

R1.1.9. Should be stricken from the document. R1.1.1 through R1.1.8. are just examples used to clarify the types of areas the Responsible Entity has to assess in order to fully comply with requirement R1. There is no further need to reiterate requirement R1.

The words “for the purpose of this standard” have no value when in a sentence with a proposed NERC term. Upon approval of this standard the definition of a Critical Cyber Asset will be added to the NERC Glossary, once approved, all NERC standards that use the term “Critical Cyber Asset” will need to follow the NERC definition. If this sentence is left in the standard, then NERC will be setting precedence that NERC terms can be superseded within any individual standard. The appropriate way to handle this issue is to change the definition of a “Critical Cyber Asset” to incorporate the requirements of R2.

R2. should be re-worded as follows:

R2. The Responsible Entity shall identify the Critical Cyber Assets associated with each Critical Asset listed in section R1.

The definition of “Critical Cyber Asset” should be changed to:

Critical Cyber Assets: Those Cyber Assets essential to the reliable operation of Critical Assets having the following characteristics:
1. The Cyber Asset uses a routable protocol, or
2. The Cyber Asset is dial-up accessible.
3. Dial-up accessible Critical Cyber Assets which do not use a routable protocol require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter.

R3. needs to be re-worded, the words "as identified" were already used in R1. and therefore can allow for a conflicting interpretation of how to determine the applicability of this requirement.

R3. should be re-worded as follows:
Any other Cyber Asset within the same Electronic Security Perimeter of Critical Cyber Assets must be protected as if a Critical Cyber Asset itself.

Section C. M3. has a typo, the first instance of Requirement R3 should be R2. The corrected sentence would be:

M3. The Responsible Entity shall maintain its approved list of Critical Cyber Assets as identified under Requirement R2 and all other Cyber Assets as identified under Requirement R3.

Section D1.1.2. should be reworded to conform to the Compliance sections. Proposed language would be:
D1.1.2. Compliance Monitoring Period and Reset Timeframe.
Self-certification will be requested annually and audits performed at least once every three (3) calendar years. The performance-reset period shall be one (1) calendar year.

D1.1.3. should be as follows:

D1.1.3.The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.

Inconsistency remains between levels of non-compliance across standards…. For example, level one non-compliance for maintenance of log data is different between CIP-005 and CIP-006.

The standards drafting team should consider better aligning the measures sections with the requirements sections. In some cases the alignment is strong, where in others it is difficult to determine which requirement a specific measure is intended for. For example, CIP-003 has 8 requirements but 18 measures. Additionally, the non-compliance levels should be more closely aligned with the measures, which needs work in all standards.

If an organization makes a conscious decision, due to technical feasibility or practicality, not to implement a requirement as defined by this standard, can the organization document an exception or deviation (as defined above) to the standard without having to report non-compliance?

GENERAL COMMENT FOR CIP-002-1 THROUGH CIP-009-1

Nowhere in any of the standards does NERC detail the policies and procedures involved with removing confidential information or configuration information when equipment or other type of media are decommissioned.

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.

R4.1. It is not reasonable to authorize and document test results for routine maintenance changes. For example, Windows updates follow a fixed and repeatable procedure. Standard update procedures should not require formal authorization and documentation steps. Alternate wording could be

Responsible Entities shall identify the controls for testing and assessment of new or replacement systems. 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 prior to the system being promoted to operate in a production environment. Routine software patches/changes are controlled and document via procedures. Formal approval is done only for initial implementation of the procedure.

The words under D1.1.2. really belong under D1.1.3. Data Retention.

D1.1.2. should be as follows:
Self-certification will be requested annually, and audits performed at least once every three (3) calendar years. The performance-reset period shall be one (1) calendar year.

D1.1.3. should be as follows:

D1.1.3. Data Retention
The compliance monitor shall keep audit records for three (3) calendar years. The Responsible Entity shall keep data for three (3) calendar years and make the following available for inspection by the compliance monitor by request:

Inconsistency remains between levels of non-compliance across standards…. For example, level one non-compliance for maintenance of log data is different between CIP-005 and CIP-006.

The standards drafting team should consider better aligning the measures sections with the requirements sections. In some cases the alignment is strong, where in others it is difficult to determine which requirement a specific measure is intended for. For example, CIP-003 has 8 requirements but 18 measures. Additionally, the non-compliance levels should be more closely aligned with the measures, which needs work in all standards.

If an organization makes a conscious decision, due to technical feasibility or practicality, not to implement a requirement as defined by this standard, can the organization document an exception or deviation (as defined above) to the standard without having to report non-compliance?

GENERAL COMMENT FOR CIP-002-1 THROUGH CIP-009-1

Nowhere in any of the standards does NERC detail the policies and procedures involved with removing confidential information or configuration information when equipment or other type of media are decommissioned.

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.

The Purpose section needs to have the words “as defined by this standard” removed. These words are in reference to the term Critical Cyber Assets; this term will be added to the NERC Glossary upon approval of this standard. Therefore, there is no need to have these words in this standard. In addition the word “screening” should be changed to “risk assessment” for continuity. The second paragraph of the Purpose section should be worded as follows:

Personnel having authorized access to Critical Cyber Assets are given a higher level of trust, by definition, and are required to have a higher level of risk assessment, training, security awareness, and record retention of such activity, than personnel not provided access.

R3 Uses the term "background screening" this should be change to "personnel risk assessments."

R4 states that Personnel be subjected to a personnel risk assessment process. M4.6 uses the term “screenings” rather than risk assessment. The measure and requirements terminology should be consistent.

In addition, we believe the “every five years” criteria will be extremely costly and is unnecessary. However, if it remains it should be phased in over a longer time period for implementation than in the current plan.

Proposed wording for M4.6. would be:

M4.6 The Responsible Entity shall conduct an update of the employee's personnel risk assessment at the following intervals:

1. Seventh year of employment.
2. Fifteenth year of employment
3. Every eighth year after the fifteenth year of employment
4. For cause.

The words under Compliance section 1.2. really belong under 1.3. Data Retention.

Compliance section 1.2. should be as follows:
Self-certification will be requested annually and audits performed at least once every three (3) calendar years. The performance-reset period shall be one (1) calendar year.

Compliance section 1.3. should be as follows:

1.3. Data Retention
1.3.1. The compliance monitor shall keep audit records for three (3) calendar years.
1.3.2. The Responsible Entity shall keep data for three (3) calendar years.
1.3.3. The Responsible Entity shall keep risk assessment documents for the duration of employee employment.
1.3.4. The Responsible Entity shall keep service vendors records for the duration of their engagement.

Inconsistency remains between levels of non-compliance across standards…. For example, level one non-compliance for maintenance of log data is different between CIP-005 and CIP-006.

The standards drafting team should consider better aligning the measures sections with the requirements sections. In some cases the alignment is strong, where in others it is difficult to determine which requirement a specific measure is intended for. For example, CIP-003 has 8 requirements but 18 measures. Additionally, the non-compliance levels should be more closely aligned with the measures, which needs work in all standards.

If an organization makes a conscious decision, due to technical feasibility or practicality, not to implement a requirement as defined by this standard, can the organization document an exception or deviation (as defined above) to the standard without having to report non-compliance?

GENERAL COMMENT FOR CIP-002-1 THROUGH CIP-009-1

Nowhere in any of the standards does NERC detail the policies and procedures involved with removing confidential information or configuration information when equipment or other type of media are decommissioned.

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.

R1. Restates the definition of an Electronic Security Perimeter and the first sentence can be deleted. Upon the approval of this standard this term will be added to the NERC Glossary. The last sentence of the paragraph needs to be re-worded so as to mirror CIP-002-1 R3. Proposed language would be: The Electronic Security Perimeter would include any other Cyber Asset as defined in CIP-002-1 Requirement R3.

R2. Disabling unused Network Ports/Service is covered under CIP-007-1 and should be deleted from CIP-005-1. Both CIP-005-1 and CIP-007-1 have this requirement and its associated measurement and level of non-compliance.

R3. Just because it may be technically feasible to remotely activate a dialup connection via SCADA, does not mean that is the most prudent control to implement. If Dialup is necessary because of a SCADA communications problem, then the responsible entity would have no way to access the device except physically, which could lead to a more serious incident. This is something that should not be dictated in the standard, but left to the individual organization to decide, so long as procedural and technical controls are in place over the dialin. We recommend removing this requirement, or providing it as an alternative to other procedural or technical controls that may be more effective.

R4.2. Where a firewall has been implemented to allow access only to and from certain specific IP addresses within the electronic perimeter, does the firewall have to implement one of the strong technical controls listed, or can the critical cyber asset be relied upon to provide the authentication requirement? For example, a server on the corporate network, or within another secure perimeter, has to communicate with a server within the perimeter. Can the authentication take place between the servers, or does the firewall have to provide authentication over and above IP address filtering?

The words under Compliance section 1.2. really belong under 1.3. Data Retention.

Compliance section 1.2. should be as follows:

Self-certification will be requested annually and audits performed at least once every three (3) calendar years. The performance-reset period shall be one (1) calendar year.

Compliance section 1.3. should be as follows:

1.3 Data Retention

1.3.1 The compliance monitor shall keep audit records for three (3) calendar years.

1.3.2 The Responsible Entity shall:

1.3.2.1. Keep documents specified in this standard for three (3) calendar years.

1.3.2.2. Keep personnel risk assessment documents for the duration of employee employment.

1.3.2.3. Keep contractor and service vendor records for the duration of their engagement.

1.3.2.4. Keep document revisions and security incident related data (such as unauthorized access reports) for three (3) calendar years.

1.3.2.5. Keep other audit records such as access records (e.g. access logs, firewall logs and intrusion detection logs) for a minimum of 90 calendar days.

Compliance, Levels of Non-compliance 2.2.2 How does an organization demonstrate compliance (i.e. prove it) with a level that states non-compliance if gap exists in system logs of between 1 and 7 days? How does an organization measure this across the multiple logs that are retained? Or does an organization report it only if it knows about it?

Inconsistency remains between levels of non-compliance across standards…. For example, level one non-compliance for maintenance of log data is different between CIP-005 and CIP-006.

The standards drafting team should consider better aligning the measures sections with the requirements sections. In some cases the alignment is strong, where in others it is difficult to determine which requirement a specific measure is intended for. For example, CIP-003 has 8 requirements but 18 measures. Additionally, the non-compliance levels should be more closely aligned with the measures, which needs work in all standards.

If an organization makes a conscious decision, due to technical feasibility or practicality, not to implement a requirement as defined by this standard, can the organization document an exception or deviation (as defined above) to the standard without having to report non-compliance?

GENERAL COMMENT FOR CIP-002-1 THROUGH CIP-009-1

Nowhere in any of the standards does NERC detail the policies and procedures involved with removing confidential information or configuration information when equipment or other type of media are decommissioned.

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.

M4 Would human observation (i.e. a security guard checkpoint that is manned 24x7) be an acceptable method for monitoring physical access control, and if so can this be added to the table in M4?

M5. How does this measure address piggybacking?

The words under Compliance section 1.2. really belong under 1.3. Data Retention.

Compliance section 1.2. should be as follows:
Self-certification will be requested annually and audits performed at least once every three (3) calendar years. The performance-reset period shall be one (1) calendar year.

Compliance section 1.3. should be as follows:

1.3. Data Retention
1.3.1. The compliance monitor shall keep audit records for three (3) calendar years.
1.3.2. The Responsible Entity shall keep data for three (3) calendar years.

Inconsistency remains between levels of non-compliance across standards…. For example, level one non-compliance for maintenance of log data is different between CIP-005 and CIP-006.

The standards drafting team should consider better aligning the measures sections with the requirements sections. In some cases the alignment is strong, where in others it is difficult to determine which requirement a specific measure is intended for. For example, CIP-003 has 8 requirements but 18 measures. Additionally, the non-compliance levels should be more closely aligned with the measures, which needs work in all standards.

If an organization makes a conscious decision, due to technical feasibility or practicality, not to implement a requirement as defined by this standard, can the organization document an exception or deviation (as defined above) to the standard without having to report non-compliance?

GENERAL COMMENT FOR CIP-002-1 THROUGH CIP-009-1

Nowhere in any of the standards does NERC detail the policies and procedures involved with removing confidential information or configuration information when equipment or other type of media are decommissioned.

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.

R1 The use of a separate non-production environment for testing and acceptance of security changes results in the need to re-licensing EMS, DCS and other software to establish such an environment. Test environments may not be feasible for many older EMS or DCS systems running proprietary hardware and software. The drafting team needs to consider a phased in approach for this requirement due to the cost to the industry, and time required to implement such environments. The industry should be asked for feedback on this requirement, as a large percentage of the participants do not have such test environments readily available. Those that do, probably also use those environments for testing upgrades and application changes as well, meaning those environments do not always mirror their production counterparts.

R1, R6 During the conference call on 2/2 there seemed to be considerable confusion surrounding the testing of security patches and scanning for vulnerabilities. There was even discussion of trying exploits against production systems after patching. It should be emphasized that great caution should be taken when scanning or testing patches in an EMS or DCS environment. In fact, scanning for open ports and exploits in these environments could result in unintended system outages, and could be considered negligent. Only non-intrusive means to determine open ports, and to verify the installation of patches, should be used in this type of environment, and the drafting team should modify sections R1 and R6 to ensure that they are not suggesting the use of obtrusive tools for testing patches or identifying open ports in a production environment.

R3.3 This requirement is confusing. What does physical access to an unattended facility have to do with generic account management? For unattended facilities (i.e. substations, backup facilities, unattended control buildings or rooms within a generating station) it is not practical to have approvals of physical access on an instance-by-instance basis. If a trusted employee who has been background screened, has a cardkey, token or other pre-approved access method for physical access to an unattended facility, and the other requirements as dictated by CIP-006 are in place, there is no need to have a separate function approve access each time that employee needs to enter such a facility. Regardless, any requirement of this type belongs in CIP-006.

R3.5 This requirement belongs in standard CIP-006.

R6.3 The intent of this requirement escapes us. Why is this requirement specific to unattended facilities?

R7.2 Again the intent of this requirement for unattended facilities escapes us. A facility that is unattended (substation) should have the same logging requirements as those that are attended (control centers) if the assets housed there are critical.

R8 Does the change control process described in this environment relate to all changes or just those of a security software or patch nature?

R11 For clarity purposes, this requirement is more appropriate to be contained in CIP-009 Recovery Plans. The level of detail discussed in this section is not currently covered in CIP-009, and having recovery requirements in two separate standards only leads to confusion and creates the possibility of conflicting requirements in future standards versions. Any recovery plan should specify the data, retention period, etc to be backed up for recovery purposes. Including in this section only increases administration on the part of the individual entities for developing procedures, and monitoring compliance.

R2. The intent of this statement is not clear. Please provide clarification beginning at:

The Responsible Entity shall conduct security test procedures for Critical Cyber Assets at the unattended facility on a controlled non-production environment located at another secure attended facility.

The words under Compliance section 1.2. really belong under 1.3. Data Retention.

Compliance section 1.2. should be as follows:
Self-certification will be requested annually and audits performed at least once every three (3) calendar years. The performance-reset period shall be one (1) calendar year.

Compliance section 1.3. should be as follows:

1.3. Data Retention
- 1.3.1. The compliance monitor shall keep audit records for three (3) calendar years.
- 1.3.2. The Responsible Entity shall keep data for three (3) calendar years.

Inconsistency remains between levels of non-compliance across standards…. For example, level one non-compliance for maintenance of log data is different between CIP-005 and CIP-006.

The standards drafting team should consider better aligning the measures sections with the requirements sections. In some cases the alignment is strong, where in others it is difficult to determine which requirement a specific measure is intended for. For example, CIP-003 has 8 requirements but 18 measures. Additionally, the non-compliance levels should be more closely aligned with the measures, which needs work in all standards.

If an organization makes a conscious decision, due to technical feasibility or practicality, not to implement a requirement as defined by this standard, can the organization document an exception or deviation (as defined above) to the standard without having to report non-compliance?

GENERAL COMMENT FOR CIP-002-1 THROUGH CIP-009-1

Nowhere in any of the standards does NERC detail the policies and procedures involved with removing confidential information or configuration information when equipment or other type of media are decommissioned.

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.

The words under Compliance section 1.2. really belong under 1.3. Data Retention.

Compliance section 1.2. should be as follows:
Self-certification will be requested annually and audits performed at least once every three (3) calendar years. The performance-reset period shall be one (1) calendar year.

Compliance section 1.3. should be as follows:

1.3. Data Retention
1.3.1. The compliance monitor shall keep audit records for three (3) calendar years.
1.3.2. The Responsible Entity shall keep data for three (3) calendar years.

Inconsistency remains between levels of non-compliance across standards…. For example, level one non-compliance for maintenance of log data is different between CIP-005 and CIP-006.

The standards drafting team should consider better aligning the measures sections with the requirements sections. In some cases the alignment is strong, where in others it is difficult to determine which requirement a specific measure is intended for. For example, CIP-003 has 8 requirements but 18 measures. Additionally, the non-compliance levels should be more closely aligned with the measures, which needs work in all standards.

If an organization makes a conscious decision, due to technical feasibility or practicality, not to implement a requirement as defined by this standard, can the organization document an exception or deviation (as defined above) to the standard without having to report non-compliance?

GENERAL COMMENT FOR CIP-002-1 THROUGH CIP-009-1

Nowhere in any of the standards does NERC detail the policies and procedures involved with removing confidential information or configuration information when equipment or other type of media are decommissioned.

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.

The word – major, should be clearly defined as it is subject to interpretation.

R3. The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.

Does M4 speak to the attendance to the training or the drill?

M4. The Responsible Entity shall conduct drills at least every three (3) years and keep attendance records to its Recovery Plan(s) training

The words under Compliance section 1.2. really belong under 1.3. Data Retention.

Compliance section 1.2. should be as follows:
Self-certification will be requested annually and audits performed at least once every three (3) calendar years. The performance-reset period shall be one (1) calendar year.

Compliance section 1.3. should be as follows:

1.3. Data Retention
1.3.1. The compliance monitor shall keep audit records for three (3) calendar years.
1.3.2. The Responsible Entity shall keep data for three (3) calendar years.

Inconsistency remains between levels of non-compliance across standards…. For example, level one non-compliance for maintenance of log data is different between CIP-005 and CIP-006.

The standards drafting team should consider better aligning the measures sections with the requirements sections. In some cases the alignment is strong, where in others it is difficult to determine which requirement a specific measure is intended for. For example, CIP-003 has 8 requirements but 18 measures. Additionally, the non-compliance levels should be more closely aligned with the measures, which needs work in all standards.

If an organization makes a conscious decision, due to technical feasibility or practicality, not to implement a requirement as defined by this standard, can the organization document an exception or deviation (as defined above) to the standard without having to report non-compliance?

GENERAL COMMENT FOR CIP-002-1 THROUGH CIP-009-1

Nowhere in any of the standards does NERC detail the policies and procedures involved with removing confidential information or configuration information when equipment or other type of media are decommissioned.

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.

The new standards are a significant increase in scope and requirements over the existing 1200 standard. Implementation and ongoing maintenance of the technical controls required by this standard across the industry will entail time and cost many millions of dollars. Implementation to a point of auditable compliance will likely take several years for many larger organizations, with significant generation or transmission systems. The timetable for passage of this standard has missed 2005 budget cycles, and the standard may not be finalized and passed before most entities can identify costs and budget for 2006. As such we believe that NERC has an obligation to perform a thorough impact analysis, with full participation from the industry, as a part of implementation plan development, and allow for a phased in implementation across multiple years. We support the need for these critical standards. But we don't support standards that neglect costs, complexity and reasonable timeframes for implementation.

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: Ken Fell			
Organization: New York Independent System Operator			
Telephone: (518) 356-6000			
Email: kfell@nyiso.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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

There is no formal means to communicate general comments, and the review process should be revised to accommodate such comments.

The timeframe for review and comments was particularly brief. In the future, a 45 day minimum review period should be implemented.

A second document (with the same version number) was published on NERC's website for consideration without notice, which had significant changes in format and numbering, which made an organized effort to review and comment that much more difficult.

The amount of both redundancy as well as contradictions across CIP's show a need for some consolidation and review of all CIP's prior to submission to the public. A technical writer may be needed to assure consistency.

Performance Reset Period, referred to often in various CIP's, needs to be defined.

Levels of non-compliance should be better defined, to eliminate the need for "dangling or's." Clearly state that any finding of non-compliance constitutes's a non-compliance rating consistent with the ranking system. Assure consistency and separation of non-compliance definitions to eliminate overlap.

Standardize on timelines across CIP's.

Modify requirement for approval or signature from "senior management" to allow for senior management designee.

Change Measure M4 to require documentation for "significant or material change" of cyber assets, in place of the existing "addition of, removal of, or modification to." Allow for 90 day time frame to reflect said change.

Migrate Requirements R1.2-R1.10 to faq section, allowing appropriate Risk Based Assessment to identify critical assets.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

There is no formal means to communicate general comments, and the review process should be revised to accommodate such comments.

The timeframe for review and comments was particularly brief. In the future, a 45 day minimum review period should be implemented.

A second document (with the same version number) was published on NERC's website for consideration without notice, which had significant changes in format and numbering, which made an organized effort to review and comment that much more difficult.

The amount of both redundancy as well as contradictions across CIP's show a need for some consolidation and review of all CIP's prior to submission to the public. A technical writer may be needed to assure consistency.

Performance Reset Period, referred to often in various CIP's, needs to be defined.

Levels of non-compliance should be better defined, to eliminate the need for "dangling or's." Clearly state that any finding of non-compliance constitutes's a non-compliance rating consistent with the ranking system. Assure consistency and separation of non-compliance definitions to eliminate overlap.

Standardize on timelines across CIP's.

This initiative is contingent on CIP-002 being ready for ballot. CIP-002 is not ready for ballot.

Delete last sentence in R1.

In R3, the words "from the requirements of this standard" should be replaced by "from the requirements of the NERC CIP series of standards. Delete the sentence beginning with "Roles and responsibilities shall also…"

Delete R5 as it is redundant with R2.

Modify C.M1 to state: "The responsible entity shall maintain a written cyber security policy."

Modify M7 to change "procedures" to "controls." Eliminate M5 and M6 as it overlaps with M7.

NYISO feels that M10 is too prescriptive, and should be modified to require less information, i.e. name/title/date.

Remove M13.1 as it is covered in M12 (for 13.1) or overly prescriptive. Migrate M13.2 to requirements section.

Remove statement from M13 "and that executive management is continually engaged in the process" as it cannot be measured.

Measures 15 and 10 are redundant, one of them must go.
Eliminate Measures 17 and 18 as those acts are already addressed in Measures 4.1 and 4.2 of CIP-004.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

Reflect corresponding requirement to complement Compliance 1.3.4

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

There is no formal means to communicate general comments, and the review process should be revised to accommodate such comments.

The timeframe for review and comments was particularly brief. In the future, a 45 day minimum review period should be implemented.

A second document (with the same version number) was published on NERC's website for consideration without notice, which had significant changes in format and numbering, which made an organized effort to review and comment that much more difficult.

The amount of both redundancy as well as contradictions across CIP's show a need for some consolidation and review of all CIP's prior to submission to the public. A technical writer may be needed to assure consistency.

Performance Reset Period, referred to often in various CIP's, needs to be defined.

Levels of non-compliance should be better defined, to eliminate the need for "dangling or's." Clearly state that any finding of non-compliance constitutes's a non-compliance rating consistent with the ranking system. Assure consistency and separation of non-compliance definitions to eliminate overlap.

Standardize on timelines across CIP's.

This initiative is contingent on CIP-002 being ready for ballot. CIP-002 is not ready for ballot.

M2.4 has no corresponding requirement, one should be added.

Measures 4.1-3 should be removed as they are redundant with CIP 003.

Measure 4.6 should be based on risk assessment process.

Non-compliance Level 3 2.3.1 has no corroborating requirement.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

There is no formal means to communicate general comments, and the review process should be revised to accommodate such comments.

The timeframe for review and comments was particularly brief. In the future, a 45 day minimum review period should be implemented.

A second document (with the same version number) was published on NERC's website for consideration without notice, which had significant changes in format and numbering, which made an organized effort to review and comment that much more difficult.

The amount of both redundancy as well as contradictions across CIP's show a need for some consolidation and review of all CIP's prior to submission to the public. A technical writer may be needed to assure consistency.

Performance Reset Period, referred to often in various CIP's, needs to be defined.

Levels of non-compliance should be better defined, to eliminate the need for "dangling or's." Clearly state that any finding of non-compliance constitutes's a non-compliance rating consistent with the ranking system. Assure consistency and separation of non-compliance definitions to eliminate overlap.

Standardize on timelines across CIP's.

This initiative is contingent on CIP-002 being ready for ballot. CIP-002 is not ready for ballot.

Migrate the definition of "Electronic Security Perimeter" from R1 to the definition section/faq section.

The use of the word "port" needs to be better defined within Requirement 2.

There's no need to limit securing modems to unattended facilities, delete "unattended" in R3.

Migrate R4.2 "examples" to faq, Citing "strong procedural or technical measures" should suffice.

Change the word "monitoring" with "logging" in R5.

R6 has no corroborating requirements for documentation.

Measures M1-M3.2 need to have complementary requirements defined.

M5.2 appears in CIP 007, R7/M6.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

There is no formal means to communicate general comments, and the review process should be revised to accommodate such comments.

The timeframe for review and comments was particularly brief. In the future, a 45 day minimum review period should be implemented.

A second document (with the same version number) was published on NERC's website for consideration without notice, which had significant changes in format and numbering, which made an organized effort to review and comment that much more difficult.

The amount of both redundancy as well as contradictions across CIP's show a need for some consolidation and review of all CIP's prior to submission to the public. A technical writer may be needed to assure consistency.

Performance Reset Period, referred to often in various CIP's, needs to be defined.

Levels of non-compliance should be better defined, to eliminate the need for "dangling or's." Clearly state that any finding of non-compliance constitutes's a non-compliance rating consistent with the ranking system. Assure consistency and separation of non-compliance definitions to eliminate overlap.

Standardize on timelines across CIP's.

This initiative is contingent on CIP-002 being ready for ballot. CIP-002 is not ready for ballot.

Requirement R6 should be deleted as it is redundant with R1.

The 90 day requirement in M1 is not reflected in the requirements section.

Measures M3-5 should have the first sentence and table eliminated for each. They are too prescriptive.

M4 is redundant with M1.

Non-Compliance 2.1.1 is not consistent with M1.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

There is no formal means to communicate general comments, and the review process should be revised to accommodate such comments.

The timeframe for review and comments was particularly brief. In the future, a 45 day minimum review period should be implemented.

A second document (with the same version number) was published on NERC's website for consideration without notice, which had significant changes in format and numbering, which made an organized effort to review and comment that much more difficult.

The amount of both redundancy as well as contradictions across CIP's show a need for some consolidation and review of all CIP's prior to submission to the public. A technical writer may be needed to assure consistency.

Performance Reset Period, referred to often in various CIP's, needs to be defined.

Levels of non-compliance should be better defined, to eliminate the need for "dangling or's." Clearly state that any finding of non-compliance constitutes's a non-compliance rating consistent with the ranking system. Assure consistency and separation of non-compliance definitions to eliminate overlap.

Standardize on timelines across CIP's.

This initiative is contingent on CIP-002 being ready for ballot. CIP-002 is not ready for ballot.

Delete R1,R2,R3.3-5 as they are addressed in other CIP's.

Modify references from "critical cyber security assets" to "critical cyber assets."

R4.1 should be modified to reflect "relevant" patches.

Employ phrase "given the technical capability of the critical cyber asset" as in R6.3 in place of more prescriptive requirements.

Integrity software as used in R5 should be explained in definitions/faq section.

Tie R5.3 into R5.1.

Change R5.4 to be "Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall ensure the integrity of the software being installed prior to each software deployment in order to prevent manual dissemination of malware."

R7.1 and R7.2 are in conflict with last sentence in R7 opening.

Remove R8 as it is addressed in CIP 003.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

R9 is redundant with CIP 005.

R11 is dependent on a “central test facility” which too prescriptive. Remove last sentence.

M3 contradicts change control processes in CIP 003, delete.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

There is no formal means to communicate general comments, and the review process should be revised to accommodate such comments.

The timeframe for review and comments was particularly brief. In the future, a 45 day minimum review period should be implemented.

A second document (with the same version number) was published on NERC's website for consideration without notice, which had significant changes in format and numbering, which made an organized effort to review and comment that much more difficult.

The amount of both redundancy as well as contradictions across CIP's show a need for some consolidation and review of all CIP's prior to submission to the public. A technical writer may be needed to assure consistency.

Performance Reset Period, referred to often in various CIP's, needs to be defined.

Levels of non-compliance should be better defined, to eliminate the need for "dangling or's." Clearly state that any finding of non-compliance constitutes's a non-compliance rating consistent with the ranking system. Assure consistency and separation of non-compliance definitions to eliminate overlap.

Standardize on timelines across CIP's.

This initiative is contingent on CIP-002 being ready for ballot. CIP-002 is not ready for ballot.

Retain use of "cyber security incidents" when referring to incidents within CIP.

Requirement R4 is too broad, and creeps into R3 territory. Modify to "The Responsible entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through a documented intermediary. Documentation to be submitted is outlined in R2.

Break R1.4-1.4.5 into a new R2, with corresponding measures.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

There is no formal means to communicate general comments, and the review process should be revised to accommodate such comments.

The timeframe for review and comments was particularly brief. In the future, a 45 day minimum review period should be implemented.

A second document (with the same version number) was published on NERC's website for consideration without notice, which had significant changes in format and numbering, which made an organized effort to review and comment that much more difficult.

The amount of both redundancy as well as contradictions across CIP's show a need for some consolidation and review of all CIP's prior to submission to the public. A technical writer may be needed to assure consistency.

Performance Reset Period, referred to often in various CIP's, needs to be defined.

Levels of non-compliance should be better defined, to eliminate the need for "dangling or's." Clearly state that any finding of non-compliance constitutes's a non-compliance rating consistent with the ranking system. Assure consistency and separation of non-compliance definitions to eliminate overlap.

Standardize on timelines across CIP's.

This initiative is contingent on CIP-002 being ready for ballot. CIP-002 is not ready for ballot.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

Modify R1 from "The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise it's plan's per Risk Based Assessment process.

Measure M1 and M2 are redundant.

Merge M3 and M4.

M5 is in conflict with R1.

Rework Levels of Non-Compliance section to clearly categorize violations, rather than repeating violations across Levels.

Level 3 Non-Compliance cites a new requirement "types of events that are necessary."

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.

Given this standard is not expected to become official before October 1, 2005, it is not realistic to expect an acceptable level of auditable compliance by Q1 2006.

The CIP's are much deeper and broader in scope than NERC 1200, and will require a significant compliance effort.

Standards need to be confirmed and solidified prior to accommodate budgeting process. Budgets typically are confirmed 4-5 month's prior to fiscal target year.

Change 2006 to 2007 (and successive columns) and change from auditably to substantially compliant. A good requirement would be to require a corporate implementation plan for compliance 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.

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**
☐ **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
John Miller	Conectiv Energy	MAAC	5
Glenn Hein	Potomac Electric Power Company	MAAC	1
Charles Peresta	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
Jeff Sabatini	PHI Corporate Services	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.

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.

Improvements have been made in definitions. Access to the glossary being developed would assist in our review and understanding. Additional definitions are required for terminology utilized in the standards which are not presently defined under the definitions (e.g. Under Control of a Common System, Routable Protocol, differentiation between Special Protection Scheme and a standard Protection System,).

Cyber Assets definition includes telecommunication networks. As part of the NERC conference call communication systems was deemed out of scope for these Standards. If telecommunications is in scope, a clear defintion is needed to understand what portion is in scope. If out of scope, similar to the comment on Nuclear Facilties being out of scope is needed.

The definition of Cyber Security Incident is far too vague. In particular the terms “suspicious event,” “attempt to compromise,” and “attempt to disrupt” are all overbroad and subject to numerous interpretations and differing applications. The concern is that an entity may be found out of compliance with the standards simply because an auditor has an interpretation of one of these terms different from a rartional interpretation used by an entity subject to the standards. It would be useful if this definition, and perhaps each entire definition section as an a whole, were to be clarified by addition of language to the effect that interpretations of terms (especially those unable to be further clarified) will be acceptable for compliance purposes, even if they may differ from those of other entities or of auditors, as long as they are reasonable or justifiable under normal standards of business decision-making.

Despite being stated here regarding each Definition section – and especially if that suggestion is not adopted – the preceding comment suggesting the inclusion of general language endorsing interpretation made as a result of reasonable business decisions bears repeating at several locations throughout the Standards in regard to terms that are not given a specific definition.

What are the differences, if any, between a “member of senior management” and a “senior management officer” (CIP-002-1 M5 and CIP-003-1 R3) or a “senior management official” (CIP-003-1 Compliance 1.3.2)? If no differnece is meant, then one term should be used consistently throughout the permanent cyber security standards. If there are differences, then each term should be further defined.

CIP-003-1: When compared to the other definition sections in the other standards there appears to be a minor formatting problem. The definition of Critical Cyber Assets should not be in bold.

CIP-003-1 The phrases “clearly and distinctly” and “engaged” in Compliance 2.3.3 and 2.4.8 are too vague. How will an auditor judge whether any choice or level of “engagement” was appropriate? Further clarification/definition is needed.

CIP-004-1 The term “properly” in Compliance 2.1.3. is too vague. How will an auditor determined what was “proper”?

CIP-004-1 The word “consistently” in Compliance 2.1.5. should be deleted, as it creates confusion for the auditing process (e.g. How would posters used in a program at one time be compared to brochures or some other method used to raise awareness at another time?)

CIP-005-1 The word “some” is too vague in Compliance 2.3.3.2. How will an auditor judge "some" is met? Either a firm lower limit needs to be established or additional clarification is needed.

General comments:

Why was the comment period for this version of the standards shortened from 45 to 30 days? The shorten period, the small differences in posted final versions, and the significant format changes from the previous draft, have made meeting the deadline to provide comments challenging at best. As a result our comments may not be complete. As a result comments that may have been raised during this draft may not be raised until the next draft.

Compliance measurement factors must be much more directly, specifically, and obviously linked to each specific Requirement of the standards, in order to facilitate both compliance and auditing. At the very least, this means that each measurement factor should have the same number as its related Requirement, as well as wording similar enough to prevent confusion. It would help to have each factor listed on the same page as, and in conjunction with, its respective Requirement.

The document previously referred to as an “FAQ” (frequently asked questions) should be adopted along with the standard, in order to facilitate proper understanding and compliance, and to ensure that such material always remains consistent with the standards. If the FAQ is not adopted, then some of the material previously appearing therein – especially the illustrative diagrams – must be placed into the standards in order to make the standards more intelligible to those who have not been intimately involved in the extensive explanatory discussions taking place during the drafting process.

CIP-007-1 Includes much material that also appears elsewhere. Such duplication should be eliminated. The approach taken in these comments is to suggest that material in other sections be removed if it is duplicative of CIP-007.

As a result of adopting new cybersecurity standards, NERC must also update and revise its Indications, Analysis and Warning program to bring it into conformity with those standards.

Why were sanctions removed from the standards? Is there no sanction now for various levels of compliance?

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.
CIP-002-1, R1. requirements state that Responsible Entities shall identify their Critical Assets using their preferred risk-based assessment. However, the Requirement then proceeds to include a very specific list of Critical Assets (R1.1.1 - R1.1.8). The impression is given that this list overrides an entity's own risk-based assessment (i.e. if you have these assets then they are Critical Assets no matter what the risk). Is the intent to define these as Critical Assets independent of a risk-based assessment? If yes, R1.1 and R.1.1.9 appear to be the only items that the risk-based assessment applies and this should be clearly stated. If no and R.1.1.1 through R1.1.8 are intended as a list of assets to consider as part of your assessment in identifying Critical Assets then the lead in sentence "Those Critical Assets include the following:" perhaps should be modified to state "Critical Assets may include the following depending on the outcome of a risk-based assessment".

The risk-based assessment appears to only apply to the process of identifying Critical Assets (CIP-002-1, R1) and not Critical Cyber Assets (CIP-002-1, R2) and therefore it is not clearly communicated in the standard that one must use an appropriate assessment methodology to identify critical cyber assets.

Further guidance is needed on "using their preferred risk-based assessment". Are there infinite risk-based assessment procedures that a Responsible Entity can choose from or create? If yes would this mean that it is possible that there would be no consistency in identifying Critical Assets and ultimately Critical Cyber Assets across the electric industry?

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.

R1: The requirements state that Responsible Entities shall identify their Critical Assets using their preferred risk-based assessment. However, the Requirement then proceeds to include a very specific list of Critical Assets (R1.1.1 - R1.1.8). The impression is given that this list overrides an entity's own risk-based assessment (i.e. if you have these assets then they are Critical Assets no matter what the risk). Is the intent to define these as Critical Assets independent of a risk-based assessment? If yes, R1.1 and R.1.1.9 appear to be the only items that the risk-based assessment applies and this should be clearly stated. If no and R.1.1.1 through R1.1.8 are intended as a list of assets to consider as part of your assessment in identifying Critical Assets then the lead in sentence "Those Critical Assets include the following:" perhaps should be modified to state "Critical Assets may include the following depending on the outcome of a risk-based assessment".

R1: The risk-based assessment appears to only apply to the process of identifying Critical Assets (CIP-002-1, R1) and not Critical Cyber Assets (CIP-002-1, R2) and therefore it is not clearly communicated in the standard that one must use an appropriate assessment methodology to identify critical cyber assets.

R1: Further guidance is needed on "using their preferred risk-based assessment". Are there infinite risk-based assessment procedures that a Responsible Entity can choose from or create? If yes would this mean that it is possible that there would be no consistency in identifying Critical Assets and ultimately Critical Cyber Assets across the electric industry?

R1: If Critical Assets are defined at one of the ten NERC Area Regional Reliability Councils (e.g. MAAC) for members of that Council (i.e. other Responsible Entities such as Transmission Owners or Generator Owners) does the burden of measures and compliance for R1 fall on the NERC Area Regional Reliability Council rather than the other Responsible Entities?

R1.1.6: What T&D assets are included in scope from a blackstart perspective (e.g. generator substation, transmission substations, substations with load)? If a unit has blackstart capability but is not part of the blackstart plan are these assets Critical Assets?

R4; M5; M6: This requirement states that a member of senior management must approve the list of Critical Assets and the list of Critical Cyber Assets. The term "senior management" is unclear. Does this mean the "senior management officer" mentioned in CIP-002-1 Measure M5 & M6, or the "officer or senior management official" responsible for the cyber security policy under CIP-003?

M3. This measure makes reference to R3 as the identification of Critical Cyber Assets. Should this be R2?

M5; M6: Are these meant to be annual approvals by the senior management officer or must the senior management officer approve each list for every individual change through out the year? If for every change, could this be reconsidered? Perhaps the senior management officer would

approve annually but a delegate would approve through out the year. Even this may be burdensome for M6.

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.

R4. This entire Requirement is redundant here, as substantially identical material also appears in CIP-007.

R5. This Requirement may be redundant here, as similar material appears at CIP-007-1 Requirement R3.4. However, in this case, it may be appropriate to address the issue here only.

M5, M6, M8. Is there a need for these three separate Measures or can they be combined? The same issue appears to be addressed using only slightly different wording: "review," "perform an assessment," and "assess … to ensure compliance." If there are differences, they need to be more clearly expressed.

M13.1, M13.2. These two sub-requirements are redundant here, as substantially identical material also appears in CIP-007.

Compliance 1.3.2. Please reference the comment under definitions regarding the diverse terminology utilized to describe a responsible person (e.g. current designated senior management official) within the Responsible Entity. Does one individual have to be designated or can this be a shared designation/responsibility? Most large utilities have major operating subdivisions or lines of business (e.g. regulated T&D, unregulated Generation, and Corporate IT); some of that division may even be required by FERC regulation. Where appropriate or convenient, Responsible Entities should be permitted to appoint multiple responsible persons.

Compliance 2.1. (Level 1): Action cannot be taken instantaneously, therefore there must be a reasonable lower bound to define noncompliance. Would suggest 21 days as a lower bound to allow adequate time for personnel changes to be implemented and reflected.

Compliance 2.1.4, 2.1.5. These appear to state the same point. They should be merged, or the intended difference clarified.

Compliance 2.2.2, 2.2.3, 2.3.4, 2.4.7, 2.4.8. These five sub-levels are redundant here, as substantially identical material also appears in CIP-007. However, 2.2.2 here uses the more appropriate calendar year, whereas CIP-007-1 Compliance 2.2.1.1 uses an unduly stringent semi-annual review period.

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.

M4.3. To improve the clarity of the language, we suggest changing the third line to read as follows: "…change in status when they are no longer allowed access…"

M4.4, 4.6. These two Measures should be clarified to express that they do apply to contractors and vendors.

Compliance 2.1.2. Since updates need to made to actual access as well as to the access lists, we suggest modifying the second line to read as follows: "…in which access and the access control list were not updated…"

Nonetheless, even with such a clarifying change, it is unclear how such a factor will be measured. Against what is such a list to be compared in order to determine whether it was appropriately updated?

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.

R1. In the last line of this Requirement, reference is made to "this standard." Since the original Standard 1300 has been divided into eight separate standards, it is no longer clear which standard is intended. For instance, does this refer to CIP-005-1, to the entire set from CIP-002-1 through CIP-009-1, or to some subset of the entire set?

R2. This Requirement is redundant here, as substantially identical material also appears in CIP-007.

R3 and R4.2. Is SCADA-activated relays required for all dialed up modems accessing Crtical Assets? Is R3 and R4.2 intended to be the only permitted solution for dial-up modems? Alternative methods should be allowed such as hardware keys. Note the call back can be defeated. 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.

M2. This Measure is redundant here, as substantially identical material also appears in CIP-007.

M5. Is this intended to apply to dial-up modems as well? If so, there are serious technical difficulties with attempting to do so.

M5.3. The original language is unclear and confusing. We suggest that it be clarified by changing it to read as follows: "…implemented to review all access and attempts in order to permit reports and alerts regarding unauthorized access and attempts…"

Compliance 2.1.1, 2.2.2. The time periods in these items are more stringent than for physical security of cyber assets. Suggest that the time periods here be made the same as those listed for Physical security of cyber assets. More, there needs to be a reasonable lower bound, as otherwise an Entity could be held noncompliant for even a one-second lapse. Twelve hours has been suggested as a reasonable lower limit.

Compliance 2.3.2. This item is redundant here, as substantially identical material also appears in CIP-007.

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.

I

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.

In general, much of this standard appears to have been duplicated in other standards. We suggest that the other material be removed.

R3.3, 3.5. It would be more appropriate to move these two Requirements into CIP-006, as they appear to relate more to physical access.

R.3.4. In this case, it may be more appropriate to address the issue in CIP-003-1 Requirement R5.5 where there is similar material.

R6.1.3, 6.1.4. There appear to be no Measures that correspond to these two Requirements. As noted above, Measures and Requirements should correlate one-for-one.

M2. The second half of this measure, reviewing access permissions, appears already to be covered, and more appropriately located in, the personnel standard CIP-004. It should be removed from this Measure.

Compliance 2.2.1.1. In CIP-003-1 Compliance 2.2.2, the applicable review period is one calendar year. Although the review issue should be addressed here rather than there, that longer period is the more appropriate term for review.

Compliance 2.3. The intent of the list of items is unclear. The list may be appropriate, although overly complex, if Level 3 noncompliance results from noncompliance with all of the items on the list. On the other hand, it would be completely inappropriate for Level 3 noncompliance to result from noncompliance with any one or two items on the list. If the original intent was to do just that, then this entire structure should be moved to Level 2, as otherwise it is far too easy to fall into the most severe Level 3 noncompliance.

Why is there so many items listed under a Level 3 non-compliance? Should some of the items in Level 3 be in Level 2?

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.

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.

Suggest that material found in the FAQ supporting this standard be relocated into the standard. Simmilar comment for other standards.

As part of the NERC conference call, it was communicated that Urgent Action 1200 expires in mid August and that under the by-laws that it can not be extended futher. It was hoped that passage of the permanent standards (or a least some) could be achieved so that there would only be a 2 week gap (i.e. become effective the beginning of September). Each draft permananet standard lists a Proposed Effective Date of October 1, 2005 which would mean there would be a 6 week gap not a 2 week gap. Should the Proposed Effective Date be September 1 in each Standard? As a contingency can a second urgent action identical to 1200 be implemented to cover any gap in cyber security standards (i.e. effective from the expiration of 1200 until the passage of the permanent standards)? Note that if a portion of the permanent standards are passed you may not have an effective cyber security policy (e.g. CIP-002-1 does not immediately pass but others do - How would you know what Critical Cyber Secuirty Assets to apply the other standards that may have passed?).

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.

Thank you for providing an implementation plan. Our comments on the draft plan are dependent on the responses to our comments to the standards. It is therefore difficult at this time to offer comments on the timing.

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:	Trevor Tidwell	
Organization:	Texas-New Mexico Power Company	
Telephone:	(281) 337-6589 x108	
Email:	ttidwell@tnpe.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.

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.

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.

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.

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.

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.

The Training requirement, R2, states that all personnel having authorized access to Critical Cyber Assets shall be trained etc. Does authorized access include access to a web server using an Internet browser? Or does it only include access that allows to users to make changes to the system? The wording of authorized access to Critical Cyber Assets is broad and vague. Either it needs to be specified personnel having authorized access regardless of type (i.e. read-only, or view-only) to Critical Cyber Assets shall be trained etc. Or a caveat needs to be included for read-only access.

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.

Requirement R2 is regarding Disabling unused Network Ports/Services, however it is also stated in CIP-007 R9. This should be either in only one CIP or each should be more specific to what the CIP is covering. R2 could just cover disabling unused Network Ports/Services on all electronics access points. The similar wording could be used in CIP-007, where the Network Ports/Services applied only to Critical Cyber Assets. See my CIP-007 comments for the more detailed suggestion. If no distinction is to be made in the Network Ports/Services wording between the two CIPs then it should only be in CIP-007.

Logical access is mentioned several times in the document, but remains vague as to what it is. There are several types of electronic or logical access, but have varying degrees of risk. A VPN or a dial-up access to a network where the computer getting access is a high risk because the setup allows for greater access and visibility to the secure network. However a user getting access through a firewall only to view a web page from a web server on the secure network is less of a risk, because the user can only access port 80 of that machine provided a properly setup firewall. Right now we use a web server to allow personnel access to SCADA information. No one logging into the web site regardless of privileges can control any devices. Is this considered have authorized access to a Critical Cyber Asset, since the server is in the control center and uses a routable protocol? Do all the web users than have to go through the training required for personnel with electronic access to a Critical Cyber Asset.

Also logical access does not seem to cover what to do for ICCP links. Not all ICCP links goto other companies that the NERC CIPs would apply to. Some ICCP links are used to connect to other computer systems on non-secure networks that use the data.

Also R2 should have a caveat for Critical Cyber Assets that do not access a wide-area network, the Internet, or to another device that is connected to non-secure network (e.g., printer). This caveat is already in CIP-007 R5.1 regarding Integrity Software. Disabling unused Network Ports/Services can be difficult since it is not always clear what Ports or Services are being used. Unused ports or services are only a threat it the machine is accessible by a malicious threat. Such threat would have to be on the electronic network, which already has physical security, electronic access control, and integrity software on the machines that access unsecured networks protecting it. Requiring disabling unused Network Ports/Services is overkill for devices that cannot reach unsecured networks.

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.

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.

With regards to R3.1 Strong Passwords, the use of strong password for user login to PC attached to the secured network only encourages written passwords, thus defeating any gain in using strong passwords. Once someone discovers where a user writes down his or her password then it is compromised. It is stated "Passwords shall be changed periodically per a risk-based frequency to

reduce the risk of password cracking". Isn't that why strong passwords are required? It was knowing where the password was written down that allowed a character in the movie War Games to get into the school computer system, even after a periodic change in passwords. It may only be a movie, but it a long known hacker tactic. Strong Passwords should be required of electronic access points. All the other security measures are for not if a password is discovered written down. A good article regarding this is located at the following link
http://www.smat.us/sanity/pwdilemma.html

Also when we began to implement requirements for 1200, our auditors said that we should also have all accounts lock out via screensaver or some other mechanism after 10 minutes of inactivity. Our operator complained about have to recall the password if the system were to alarm and the screensaver had lock them out. Imagine what it would be like if a system event was occurring and the operator could not act in time because he could not remember the strong password required. Cyber security should be to protect the grid, not prevent the operator from controlling it. Inactivity of logged in user accounts is not addressed in CIP-002 through CIP-009.

R4 Security Patch Management refers to the testing of security patches. This is unrealistic. Many security patches deal with buffer overflows, and malformed TCP/IP packets. It would take sometime to train up staff to do this and not to mention hiring extra staff to cover this. We are hard pressed to keep staffing at a level to maintain SCADA, much less take on this responsibility. If testing is to make sure that the system suffers no ill effect in terms of up time or does not interfere with normal or emergency operation, then it is acceptable.

With regards to R5 Integrity Software, R5.1 states "use integrity software on all Critical Cyber Assets that are connected to a wide-area network, the Internet, or to another device that is connected to a network (e.g., printer)". The statement could be better worded. A suggested statement is "use integrity software on all Critical Cyber Assets that are connected to unsecured network, or can connect to unsecured networks back through an electronic access point, or connected to a device that is connected to an unsecured network and the device could transmit malicious software to the Critical Cyber Asset". The phrase "another device that is connected to a network" could include a master system talking via a serial link to an RTU that is connected to a substation network. This type of connection poses no threat since the serial communication is master poll driven, and no virus or intrusion to the master system is possible.

R6.1.2 Scanning for open ports/services and modems should be scanning for open ports/services and modems on access points to the Electronic Security Perimeter and for modems on Critical Cyber Assets. It is our position that open ports/services on access points is a valid concern, but not for all Critical Cyber Assets.

R9 refers to disabling unused host ports/services. However CIP-005 also addresses this issue. The wording should be changed to allow for better distinction of what each is to cover. If no wording change is to be made then it should only be in this CIP. See my comments under CIP-005 regarding suggested rewording for CIP-005. While the wording could be changed to clarify that R9 refers only to Critical Cyber Assets and not any electronic access point, it is our position that this is unnecessary. The secure network has not only strong controls to the electronic access points, but also to the physical security. It is hard to disable all ports and services on all Critical Cyber Assets because it may not be known what is and is not being used. Our system does not run email, touch the Internet, and has firewall seperating it from the corporate network. Considering this and the other security implementations, the disabling of all unused ports seems beyond excessive. Either make a caveat for systems that have a very low or no profile to the outside world, or remove this requirement.

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.

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.

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.

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:	Don Miller / Ray Morella	
Organization:	FirstEnergy Corp	
Telephone:	330.384.4649/330.384.5686	
Email:	donjmiller@firstenergycorp.com/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.

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.

Definitions are clear.

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.

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.

An additional document or section is needed showing "appropriate risk-based assessment methodology" for the entity's circumstances. This assessment methodology would further give the guidance and clearity to the environments included in the permanent standard. Also provide some consistenancy across the industry on what the critical items are and how NERC views their impact on the entity's environment and the country. This would not be an exact science since all the environments differ, only a guideline.

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.

Some of the Measures do not match up with the requirements, the timing for reviews, data retention periods, and senior management designation, etc are spelled out in the measures and omitted in the requirements. The measures should match the requirements!

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.

R3 - Under Records retention the "background screening" should be changed to "personnel risk assessment".

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.

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.

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.

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.

Why does the retention period need to be 3 years, 2 years should be acceptable.

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.

The responsible entity should exercies their Recovery Plans when there are significant changes to the infrastructure or facilities.

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.

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 the 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:	**Roger Champagne**	
Organization:	**Hydro-Québec TransÉnergie**	
Telephone:	**514-289-2211 ext. 2766**	
Email:	**champagne.roger.2@hydro.qc.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*
Martin Ferland	Hydro-Québec TransÉnergie	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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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 devided 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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

~~NPCC~~HQTÉ feels that there are many incidents have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>.

~~NPCC~~HQTÉ is concerned that "suspicious event" is too broad. We recommend changing the Cyber Security Incident definition to <<Any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.>>

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

~~The NPCC answer to question 2 is "yes."~~Yes ~~Yes~~Yes

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.

~~NPCC strongly~~HQTÉ believes ~~s~~ that CIP-002 is not ready for ballot. This is a Cyber Security Standard. A definition of the Bulk Electric System (BES) does not belong in this standard. Recently the industry approved a BES definition, in the Version 0 Glossary. That Glossary was approved so there would be one industry wide definition. ~~NPCC~~HQTÉ feels that CIP-002 conflicts with that approved definition. We suggest the following Purpose, Requirements, Measures and Compliance.

<<

PURPOSE:

This standard is intended to ensure that appropriate cyber 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.

With the increased use of standard technologies to connect Control Center computer systems to the bulk electrical systems, corporate business systems, and the internet, the separation of the critical assets of the bulk electrical system from the an insecure infrastructure has been dramatically reduced. This connectivity requires that the Control Center systems put in place a high level of Cyber Security measures to protect the Control Center and bulk electrical system assets.

Business and operational demands for managing and maintaining 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 Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system.

The Critical Cyber Assets are identified by the application of a risk-based assessment procedure on the operation cyber assets supporting the monitoring and control of the interconnected bulk electric system.

REQUIREMENTS

R1. The Responsible Entity shall identify their cCritical Cyber Assets associated with support of the bulk electrical system Critical Assets using their preferred risk-based assessment. For the purpose of this standard, Critical Cyber Assets will be limited to those Cyber Assets having the following characteristics:

R1.1 The Cyber Asset uses a routable protocol, or

R1.2 The Cyber Asset is dial-up accessible.

R1.3 Dial-up accessible Critical Cyber Assets which do not use a routable protocol require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter

R2.Any other Cyber Asset within the same Electronic Security Perimeter as identified Critical Cyber Assets must be protected to ensure the security of the Critical Cyber Assets.

R3. A member of senior management or designee must approve the list of Critical Cyber Assets.

MEASURES

M1.The Responsible Entity shall maintain its approved list of Critical Cyber Assets as identified under Requirement R1 and all other Cyber Assets as identified under Requirement R2.

M2.The Responsible Entity shall maintain documentation depicting the risk-based assessment used to identify its Critical Cyber Assets in R1. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure.

M3.The Responsible Entity shall review, and as necessary, update the documentation referenced in M1, and M2 at least annually, or within 30 calendar days of the addition of, removal of, or modification to any Critical Asset or Critical Cyber Asset.

M4. A signed and dated record of the senior management officer's approval of the list of Critical Cyber Assets must be maintained.

COMPLIANCE

1. Compliance Monitoring Process

1.1 Compliance Monitoring Responsibility
Regional Reliability Organization

1.2 Compliance Monitoring Period and Reset Timeframe

Verify annually that necessary updates were made within 30 calendar days of asset additions, deletions or modifications. The performance-reset period shall be one (l) calendar year. The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.

1.3 Data Retention
The Responsible Entity shall make the following available for inspection by the compliance monitor upon request:

1.3.1 Documentation of the approved list of Critical Cyber Assets, and

1.3.2 Documentation of the senior management official's approval of both the Critical Asset list and the Critical Cyber Asset list.

1.4 Additional Compliance Information

Not specified

2. Levels of Non-Compliance

2.1 Level l:The required documents exist, but have not been updated with known changes within thirty (30) calendar days.

2.2 Level 2:The required documents exist, but have not been approved, updated or reviewed in the last calendar year.

2.3 Level 3: One or more document(s) missing.

2.4 Level 4: No document(s) exist.
>>

********** Please clarify the performance reset period in D.1.2. What is being reset? Why is it being reset?

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

~~NPCC~~HQTÉ feels CIP-003 needs a little more work before it is ready for ballot. This answer assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot, for more information see the response to the previous question.

~~***** Possible alternate words to A.R3. Who has these alternate words?~~

~~NPCC~~HQTÉ does not agree with C.M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets. We recommend that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>

Please explain what <<information security protection programs>> C.M5 refers to.

~~NPCC~~HQTÉ feels that C.M10 is too prescriptive. The Compliance Submittal is signed by an authorized representative of the Responsible Entity. That commits the Entity to that information. If it is later discovered that person did not have authorization, then the Entity did not submit compliance on time, which makes the Responsible Entity non-compliant. This incents Entities to insure the appropriately documented information is submitted on-time.

***** ~~(Ian) NPCC~~HQTÉ is concerned that C.M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the structure of internal corporate relationships>> too frequently.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

~~NPCC~~HQTÉ feels CIP-004 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

~~NPCC~~HQTÉ feels this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.

Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.

Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003.

Measure 4.6 should be modified. The requirement for a regular 5 year update to the security screening is not consistent with Requirement R4, which states that a risk based approach be used. The need for rescreening should be cause only.

Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

~~NPCC~~HQTÉ feels CIP-005 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

~~NPCC~~HQTÉ requests clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.

Requirement 4.2's third bullet is not clear. We recommend changing from
<<
Out of band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication.
>>
to
<<
Out of band authentication procedures to augment static user id and password access. (e.g. Access will not be enabled via static user id and password authentication unless a telephone call is received from the entity requesting access. On receipt of the telephone call an administrator will enable access allowing the entitiy to utilize their static user id and password.)
>>

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

~~NPCC~~HQTÉ feels CIP-006 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

The term "six-wall boundary" should be in the definitions. We recommend moving this information from question 16 under CIP-006 in the FAQ

Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2.

Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.

Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement.

Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.

Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Measure M4 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

~~***** rework numbers!~~

Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.~~———~~

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

~~NPCC~~HQTÉ feels CIP-007 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

~~***** what are IESO's comments on R1, R2 and the early parts of R3?~~

~~***** what are the IESO's comments on R3 to R3.2, inclusive?~~

Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006.

Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.

Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.

Requirement R3.6 should be modified. The second sentence repeats the first, as such it is necessary and may confuse some.

Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>.

***** Requirement R4.1 is too prescriptive

Add <<where technically feasible>> to the end of Requirement R4.3.

Requirement R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means.

Requirement R5.3 allows exception to R5.1. As such, these Requirements should be combined, otherwise one could be non-compliant with R5.1 and fully compliant with R5.3 while the intent appears to be full compliance with R5.1 and R5.3.

***** The combined requirement should allow technically feasible alternative solutions.

Change Requirement R5.2 from
<<

The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.
>>
to
<<
Where integrity software is deemed to be technically implementable and has been implemented, the Responsible Entity shall perform a monthly review of the integrity software to ensure that the release level of the integrity software is functionally effective and maintainable for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.
>>

~~***** Requirement 5.4 is acceptable?~~

Change Requirement R6.1 from
<<
The Responsible Entity shall perform a vulnerability assessment at least annually that includes:
>>
to
<<
The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes:
>>

Change Requirement 6.1.3 from
<<
Factory default accounts
>>
to
<<
Scanning for factory default accounts
>>

Change Requirement 6.1.4 from
<<
Security patches and anti-virus version levels
>>
to
<<
Assessing security patches and/or anti-virus version levels, as appropriate
>>

The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assesssment schedule than an attended facility?

Requirement R9 should clarify that it pertains to ports inside the perimeter. Requirement R2 of CIP-005 covers ports at the perimeter.

The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.

Requirement R11 belongs in CIP-009. This requirement should be moved to that standard. This requirement references Critical Assets. That is not correct. It should a requirement for the backup and recovery of Critical Cyber Assets. The requirement starts with <<on a regular basis>>, and the third sentence says <<at least annually>>. The requirement should stipulate one or the other. We recommend removing <<annually>>. The last sentence is unclear and should be deleted.

Change Measure M2. The semi-annual audit is too prescriptive. This requirements recognizes that the frequency of password changes should be determined by risk assessment.

~~***** decide on <<The measure should be that remedial measures are taken within 7 days for passwords found to be non-compliant>>~~

<<where applicable>> should added to the end of Measure 4.3.

Change the Measures M5.1 - M5.3 from
<<
M5.1 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.
M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found.
M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities.
>>
to
<<
M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments.
M5.2 The documentation shall include a record of the results of the annual vulnerability assessment.
M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions.
>>

Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the perimeter.

Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.

Which Requirement and Measurement is Compliance 2.1 associated with?

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

CIP-008 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from
<<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>>
to
<<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>>

Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3.

The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows
<<
The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

CIP-009 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

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.

The Implementation Plan does not allow enough time for compliance. These standards have substantial changes from 1200. A Responsible Entity could be compliant with 1200 and require much work before they are compliant with these standards.

We recommend that the 2006 dates change to 2007 dates, the 2007 dates change to 2008 dates, etc.

There is concern with compliance for substations. Substations are part of the <<Other Facilities>>. Therefore it is recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant. ———

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:	**Joe Weiss**		
Organization:	**KEMA**		
Telephone:	**(408) 253-7934**		
Email:	**joe.weiss@kema.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	X	8 - Small Electricity End Users
☐	SPP	☐	9 - Federal, State, Provincial Regulatory or other Government Entities
☐	WECC		
X	NA - Not Applicable		

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Cyber Assets – Those programmable and interconnected electronic devices and communication networks including hardware, software, and data associated with electric system assets.

Cyber Security Incident – Any malicious act, suspicious event, or unintentional 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 electronic operation or monitoring of a Critical Cyber Asset

NERC identifies this as the Permanent Cyber Security Standard. However, the Drafting Team and other NERC CIPC members agree that this is simply a minimum starting point. Many utilities and others that are not part of the NERC process will read the NERC Website and assume this is the final document since it is named the Permanent Standard. Consequently, NERC needs to either change the title to something such as Interim Cyber Security Standard or this Standard needs to address significantly more items in much more detail.

From an equipment perspective, there has been a blurring of the distinction between transmission and distribution, particularly above 15- 69KV. There are distribution applications above the classic definition of bulk being 35KV or above. Consequently, the term bulk could result in precluding the review of critical equipment that could have a potential impact on the bulk electric grid. Additionally, communications is a critical path for cyber vulnerabilities of Critical Cyber Assets. There have been actual cases where cyber impacts on communications have resulted in cyber impacts on bulk critical assets. Therefore, I would make the following suggestion under Applicability in each section:

Applicability
Include a risk-based approach to determine the applicability of all electronic assets that are interconnected to the bulk electric grid including those explicitly excluded if the risk warrants.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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?

X No

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

CIP 006 FAQ 9. The response provides three generally accepted risk assessment methodologies. It should be noted that ISA TR99.00.02-2004, Technical Report 2 – Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment provides a risk methodology specific to process control systems and should be referenced. Care should be taken when applying any risk assessment methodology to address control system cyber-specific frequencies and consequences.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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

X 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.

Business and operational demands for managing and maintaining a reliable electric system increasingly require Cyber Assets supporting critical reliability control and diagnostic 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 electric system assets. This standard requires that Responsible Entities identify and protect critical Cyber Assets that support the reliable operation of the electric system.

The Critical Assets are identified by the application of Critical Asset cyber risk-based assessment procedure on the operation of the electric system.

R1.2. Critical Assets: The Responsible Entity shall… critical operating functions and tasks affecting the interconnected electric system …power plant control and diagnostics, substation control and diagnostics and real time information exchange…

R1.6. All electronically interconnected generating assets that can be electronically dispatched, monitored, or controlled from a central control center.

This criteria was not based on cyber considerations. Even small units that are cyber vulnerable and electronically connected to a control center can impact the control center and associated bulk electric grid. Additionally, packages of small combustion turbine units that individually would be considered too small to individually address can constitute a large station. Each small unit could be cyber vulnerable. Having the standard ignore these units can contribute to the electronic vulnerability of the bulk electric grid.

R.13. A risk-based graded approach should be used to determine the applicability of all Critical Cyber Assets whether using a routable or non-routable communication protocol.

Communication protocols such as DNP3, Modbus, and Profibus currently can be (and in many instances have been) accessed to make the Critical Asset vulnerable. The cyber vulnerability of control system non-routable protocols have been demonstrated in laboratory demonstrations such as the DOE Pacific Northwest National Laboratory (PNNL) demonstrations and in field cases resulting in actual (though not publicly reported) control system cyber impacts. Non-routable control system communication protocols have actually actual caused cyber impacts. Consequently, there is a need for a graded risk-based approach to determine the impact of the Asset independent of the protocol. If they cannot impact the bulk electric grid, they do not need to be addressed. If they can impact the bulk electric grid, the risk-based approach should provide a basis for the level of protection.

R.15. Delete.

FAQ 2. Critical Cyber Assets using non-routable protocols could have a range of potential cyber impacts and should be assessed using a risk-based approach.

FAQ 3. This addresses common mode failure within the power plants. However, many large and small power plants are now electronically interconnected to the bulk electric system for real time dispatch and other real-time functions. That means that the power plants, however small, can be an insecure electronic path into the bulk electric grid and control center. Consequently, a risk-based approach should be used to determine if they should be included in this standard.

FAQ 8. A continuously connected dial-up, if interrupted, becomes non-permanent communication connection as it will need to be reconnected at which time it could become vulnerable.

FAQ 12. Since cyber impacts on communication systems have already impacted Critical Cyber Assets, a risk-based approach should be used to evaluate communication systems between Electronic Security perimeters and Critical Cyber Assets. The risk-based approach would identify if the communications need to be addressed and to what level.

FAQ 13. The exception would be if there is electronic interconnectivity between the environmental or support system and the Critical Cyber Asset. If there is electronic connectivity, then the environmental or support system should meet the same criteria as the Critical Cyber Asset.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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

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

☐Yes
X 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.

R1. The Responsible Entity shall create and maintain a Critical Asset cyber security policy…
Having a security policy is insufficient to protect Critical Assets; it must be a security policy designed specifically for Critical Assets (control systems).

M1. The Responsible Entity shall maintain its written Critical Asset cyber security policy stating its commitment to protect Critical Assets. Having a security policy is insufficient to protect Critical Assets; it must be a security policy designed specifically for Critical Assets (control systems). It is also inconsistent to not have a specific Critical Asset cyber security policy and yet maintain it has a commitment to protect those assets.

M2. The Responsible Entity shall review the Critical Asset cyber security policy ….

2.1.2 A written Critical Assets cyber security policy has not been developed or reviewed in the last calendar year…

2.1.4 A Critical Assets information security protection program exists but has…

2.4.2 No Critical Assets cyber security policy exists

Additional item: This section should reference ISA TR99.00.02-2004, Technical Report 2 – Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment

FAQ 1. This should explicitly state that the Cyber Security Policy should be specifically designed for Critical Cyber Assets (Control System Security Policy not a traditional IT Security Policy).

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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

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

X 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.

R1. The Responsible Entity shall develop, maintain, and document its Critical Assets security awareness program.
Typical security awareness programs do not address Critical Assets.

R2. The Responsible Entity shall develop and maintain a company Critical Asset specific cyber security training program...
Typical cyber security training programs do not address Critical Assets.

M1. The Responsible Entity shall develop and maintain Critical Asset awareness programs designed to maintain and promote sound Critical Asset security practices….
Typical security awareness programs do not address Critical Assets.

M2. The Responsible Entity shall develop and maintain a company Critical Asset specific cyber security training program...
Typical cyber security training programs do not address Critical Assets.

M2.1 The Critical Assets cyber security policy.
Typical cyber security policies do not address Critical Assets.

M4.4 The Responsible Entity shall conduct a documented company personnel risk assessment process of all company, vendors, and contractors being granted authorized access ... It is not clear that vendors and contractors are addressed and need to be.

Additional item: This section should reference ISA TR99.00.02-2004, Technical Report 2 – Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

CIP–005–1 — Cyber Security — Electronic Security

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

X 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.

R2. To the extent possible, the Responsible Entity shall enable only those ports/services required for normal…
It may not be practical or even possible to disable all unused ports and services for Critical Assets.

R3. …Where remote activation of dial-up connectivity from Critical Assets is technically feasible, dial-up equipment in substations and power plants shall be physically deactivated, if possible, when not in approved use and remotely activated upon approval of activation. In all other cases, the Responsible Entity shall implement procedural or technical measures to ensure authenticity of the accessing device and/or application.
This is not just a SCADA issue and it may not be possible to disable the dial-up connection.

M2. To the extent possible, the Responsible Entity shall disable all unused ports and services, and where possible maintain documentation of status/configuration of all ports and services available on Critical Cyber Assets.
It may not be practical or even possible to disable all unused ports and services or identify their status.

Additional item: This section should reference ISA TR99.00.02-2004, Technical Report 2 – Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment.

FAQ 1. The schematic represents the electronic security perimeter for the Urgent Action Standard that does not address substations or power plants. A risk-based assessment should be performed to determine where the security perimeter should be established based on the cyber vulnerability of the RTU and networked substation control and diagnostic devices and the power plant networked control and diagnostics systems.

FAQ 2. A risk-based assessment should be performed to determine the whether and to what level communications to networked control and diagnostic systems should be addressed.

FAQ 3. A risk-based assessment should be performed to determine where the security perimeter should be established based on the cyber vulnerability of the RTU and dial-up substation control and diagnostic devices that are input to the RTU.

FAQ 9. This should reference ISA TR 99.00.01-2004, Security Technologies for Manufacturing and Control Systems and ISA TR99.00.02-2004, Technical Report 2 – Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

CIP–006–1 —Cyber Security — Physical Security

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

X 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.

A risk-based assessment should be performed to determine what facilities should be addressed by this standard.

It should be noted that the NERC Control System Security Working Group (CSWWG) debated the issue of excluding the term bulk from the Physical Security - Substations Guideline. The CSSWG removed the term bulk in the next to last version of the Guideline because utilities had identified distribution substations as meeting the Critical Assets definition.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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

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

X 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.

R1. The Responsible Entity shall use documented Critical Asset information security test procedures to augment functional test….
Typical information security test procedures do not address Critical Assets.

R3.1 In the absence of more sophisticated authentication methods that are stronger than passwords, and don't require a password, (e.g., multi-factor access controls, certificates, or biometrics), the Responsible Entity shall use accounts that a have a strong password where possible.
It may not be possible to implement strong passwords in certain Critical Assets.

R6.1.1 An engineering review including walkdowns of access points (e.g., modems) to the Electronic Security Perimeter.
R6.1.2 An optional additional approach would be to scan for open ports/services utilizing accepted tools and methodologies for use specifically in scanning control systems. The scanning team shall include personnel expert in scanning techniques and also in the operation of the control system to be scanned.

It is very risky to scan a control system network. There have been numerous cases where scanning a control system network has shut it down or caused actual damage to control system devices. If scanning is to be performed, it should be done using a scanning tool and methodology that has been approved for control system use and in concert with control system personnel. It should be noted that electronic scanning for open ports/services will not identify all control system vulnerability points and can lead to a false sense of security.

R9. To the extent possible, The Responsible Entity shall enable only those ports, services, and applications required for normal and emergency operations of Critical Cyber Assets. All other identified ports, services, and applications, including those used for testing purposes, must be disabled prior to production usage.
It may not be practical or even possible to disable all unused ports and services for Critical Assets.

M8. To the extent possible, the Responsible Entity shall disable unused ports, services, and applications and maintain documentation of status/configuration of all ports, services, and applications available on critical Cyber Assets.
It may not be practical or even possible to disable all unused ports and services for Critical Assets. It may also not be possible to identify all ports and services that are used.

Additional item: This section should reference ISA TR99.00.02-2004, Technical Report 2 – Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment

FAQ 5. Staff experienced in control system operations should be part of the test development and testing team to minimize the potential for impacting Critical Cyber Assets.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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?

X 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.

R1. The Responsible Entity shall develop and document a Critical Assets incident Response Plan.

FAQ 5. This should also reference ISA TR99.00.02-2004, Technical Report 2 – Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

CIP-009-1 – Cyber Security – Recovery Plans

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

X 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.

R1. The Responsible Entity shall create recovery plan(s) from cyber events for Critical Cyber Assets and exercise its recovery plan(s) at least annually. Recovery plans generally exist for Critical Assets for expected events but not necessarily for cyber events.

Additional item: This section should reference ISA TR99.00.02-2004, Technical Report 2 – Programs, Integrating Electronic Security into the Manufacturing and Control Systems Environment

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**
☐ **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: Edison Electric Institute

Lead Contact: **L.W. Brown**

Contact Organization: **Edison Electric Institute**

Contact Segment: **0**

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.

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.

Please see "ATTACHED EEI SECURITY COMMITTEE GENERAL and SPECIFIC COMMENTS"

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.

Please see “ATTACHED EEI SECURITY COMMITTEE GENERAL and SPECIFIC COMMENTS”

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 EEI SECURITY COMMITTEE GENERAL and SPECIFIC COMMENTS"

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 EEI SECURITY COMMITTEE GENERAL and SPECIFIC COMMENTS"

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 EEI SECURITY COMMITTEE GENERAL and SPECIFIC COMMENTS"

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 EEI SECURITY COMMITTEE GENERAL and SPECIFIC COMMENTS"

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 EEI SECURITY COMMITTEE GENERAL and SPECIFIC COMMENTS"

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 EEI SECURITY COMMITTEE GENERAL and SPECIFIC COMMENTS"

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.

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 EEI SECURITY COMMITTEE GENERAL and SPECIFIC COMMENTS"

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 EEI SECURITY COMMITTEE GENERAL and 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 Institute on Draft 2 of the Proposed NERC Cybersecurity Standards, CIP-002-1 through CIP-009-1	**November 1, 2004**

Background

We appreciate the hard work, expertise, integrity, and cooperation reflected in this proposal. Some good progress has been made beyond the first draft Standard 1300 language. As with any document created by committee, however, there nonetheless remain items that require further clarification and development before the Standards are 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 two hours of discussion during a conference call among EEI member-company security and IT staff, including one member of the Standard Drafting Team, to discuss the 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 may, as a result, see many of these comments mirrored in individual company comments, which may also raise other 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.

Overall Comments

We note that because the comment period for this version of the standards was shortened from 45 to 30 days, we cannot assure the drafting group that we have addressed all relevant issues. In part this comment is based on the significant format

changes from the previous draft, and in part because different versions of this draft were posted. Moreover, although the differences between the two versions may have seemed small or insignificant to some, the fact that there were two different versions caused confusion and consternation that was aggravated by the shortened comment period.

The NERC cybersecurity standards should apply to all entities affecting the bulk market, as well as all entities participating in the bulk market. In particular, this includes NERC itself, as NERC is increasing its cyber links both to that market and to market participants, and will have access to, as well as possession of, information sensitive to that market.

Regarding the implementation schedule, NERC must remain sensitive to the normal corporate budgetary cycle. Since many companies will be finished with or already well into finalization of their Fiscal Year 2006 budgets before these Standards could be approved, it would be unreasonable to expect more than "substantial compliance" in 2006.

Compliance measurement factors must be much more directly, specifically, and obviously linked to each specific Requirement of the standards, in order to facilitate both compliance and auditing. At the very least, this means that each measurement factor should have the same number as its related Requirement, as well as wording similar enough to prevent confusion. It would help to have each factor listed on the same page as, and in conjunction with, its respective Requirement.

It must be more clearly specified that these standards do not apply to facilities subject to regulation by the Nuclear Regulatory Commission (NRC), including any non-nuclear facilities that may happen to be within physical perimeters subject to such regulation. Facilities subject to NRC regulation will soon have their own NRC cybersecurity standards to comply with. Since the NRC standards are still in development, while NERC's cannot be postponed, the industry must be assured that facilities subject to the NRC standards will not have to comply with potentially inconsistent NERC standards.

The references to telecommunications equipment remain unclear in that they still give the impression that these standards apply to all of an entity's interconnected telecommunication system. It was the understanding of many that the standards were actually intended only to apply to specific pieces of telecommunication equipment that was located within a secure perimeter or otherwise "directly" connected to critical cyber assets.

The document previously referred to as an "FAQ" (frequently asked questions) should be adopted along with the standard, in order to facilitate proper understanding and compliance, and to ensure that such material always remains consistent with the standards. If the FAQ is not adopted, then some of the material previously appearing therein – such as examples of risk assessment or business continuity methodologies, as well as illustrative diagrams – ought to be placed into the standards in order to make the standards more intelligible to those who have not been intimately involved in the extensive explanatory discussions taking place during the drafting process.

CIP-007-1 Includes much material that also appears elsewhere. Such duplication should be eliminated. The approach taken in these comments is to suggest that material in other sections be removed if it is duplicative of CIP-007.

As a result of adopting new cybersecurity standards, NERC must also update and revise its Indications, Analysis and Warning program to bring it into conformity with those standards.

There should at least be an explanation of why sanctions were removed from the standards. Some commenters would have preferred to have retained them as part of the standards.

Comments on Language Appearing in All or Many Standards

The definition of Cyber Security Incident is far too vague. In particular the terms "suspicious event," "attempt to compromise," and "attempt to disrupt" are all overbroad and subject to numerous interpretations and differing applications. The concern is that an entity may be found out of compliance with the standards simply because a standards-compliance auditor disagrees with a completely reasonable interpretation made by a Responsible Entity. There are no objective, measurable criteria in the Standards or the FAQ by which a Responsible Entity or an auditor can determine what is sufficiently suspicious to trigger action. Moreover, it is simply not knowable whether any specific event is an "attempt," because that involves knowing the intent of the actor

Instead, it would be more useful if this definition, and perhaps each entire definition section as a whole, were to be clarified by adding language to the effect that interpretations of terms (especially those, like the three here, unable to be further clarified) will be acceptable for compliance purposes, even if they may differ from those of other Responsible Entities or of auditors, as long as they are reasonable or justifiable under normal standards of business decision-making.

Despite being stated here regarding each Definition section – and especially if that suggestion is not adopted – the preceding comment suggesting the inclusion of general language endorsing interpretation made as a result of reasonable business decisions bears repeating at several locations throughout the Standards in regard to terms that are not given a specific definition.

What are the differences, if any, between a "member of senior management" and a "senior management officer" (see CIP-002-1 Measure M5, and CIP-003-1 Requirement R3) or a "senior management official" (see CIP-003-1 Compliance 1.3.2)? One term should be used consistently throughout all of the cybersecurity standards.

Comments on Individual Standards

CIP-002-1

R1. The opening sentence indicates that each Responsible Entity may use their preferred risk assessment methodology to identify Critical Assets. However, the Requirement then proceeds to include a very specific list of facilities (R1.1.1 - R1.1.8). The impression is given that such list would override any entity's own risk assessment.

It would be better if the standard only include R1.1 and R1.1.1 (renumbered as "R1.2"). The listed facilities should either be moved to the FAQ, or – if the FAQ is not included – more clearly identified only as facilities that are likely to critical and so must be included within an assessment, but which may – after such an assessment – be found reasonably excludable. Such a revision would require either removing the last sentence of the current R1.1, or (if the current list at R1.1.1 - R1.1.8 is retained) inserting the word "may" or "could" prior to the word "include" in that sentence.

R1.1.1. Use of the term "Generation Operator" in R1.1.1 implies that all generation equipment is covered by the standard. It had been the understanding of most companies that generation facilities were not to be covered in all cases.

R4. The term "senior management" is unclear. Does this mean the "senior management officer" mentioned in CIP-002-1 Measure M5, or the officer or senior management official responsible for the cybersecurity policy under CIP-003?

M3. Reference is made to R3 – that appears to be typo, as the identification of Critical Cyber Assets is in R2.

M5. Must the record of approval of the list be updated for every individual change to that list? If so, we urge reconsideration, as that is far too burdensome.

CIP-003-1

Definitions There appears to be a formatting problem – based on a comparison with the other Definition sections, the definition of Critical Cyber Assets should not be in bold.

R4. This entire Requirement is redundant here, as substantially identical material also appears in CIP-007.

R5. This Requirement may be redundant here, as similar material appears at CIP-007-1 Requirement R3.4. However, in this case, it may be appropriate to address the issue here only.

M5, M6, M8. The need for these three separate Measures is unclear – they all seem to be addressing the same issue using only slightly different wording: "review," "perform an assessment," and "assess … to ensure compliance." If there are differences, they need to be more clearly expressed, or the three Measures should be combined into one.

M13.1, M13.2. These two sub-requirements are redundant here, as substantially identical material also appears in CIP-007.

Compliance 1.3.2. In addition to the already mentioned diverse terminology regarding who is meant by the various terms describing a responsible person within the Responsible Entity, this factor implies that only one such person can be named for compliance purposes, despite the existence of multiple business entities or units under the corporate structure. Some of that division may even be required by FERC regulation. Where appropriate or convenient, Responsible Entities should be permitted to appoint multiple responsible persons.

Compliance 2.1. Action cannot be taken instantaneously. Thus, there must be a reasonable lower bound to define noncompliance. It has been suggested that 21 days allows adequate time for personnel changes to be implemented and reflected.

Compliance 2.1.4, 2.1.5. These appear to state the same point. They should be merged, or the intended difference must be clarified.

Compliance 2.2.2, 2.2.3, 2.3.4, 2.4.7, 2.4.8. These five sub-levels are redundant here, as substantially identical material also appears in CIP-007. However, 2.2.2 here uses the more appropriate calendar year, whereas CIP-007-1 Compliance 2.2.1.1 uses an unduly stringent semi-annual review period.

Compliance 2.3.3, 2.4.5. The phrases "clearly and distinctly" and "engaged" are too subjective in the context used. At 2.3.3, it is not clear how an auditor is to determine whether a Responsible Entity's judgment about clear and distinct definitions of roles and/or responsibilities is correct, or under what criteria. It would seem sufficient compliance if the employees, contractors, venders, etc. of the Responsible Entity actually do understand their roles and/or responsibilities. At 2.4.8, it is not clear how an auditor is to determine whether a Responsible Entity's judgment about the "engagement" of executive management was appropriate, or under what criteria.

If not done generally in each of the Definition sections, it would be more useful if these phrases were to be clarified by addition of language to the effect that interpretations of such qualitative terms will be acceptable for compliance purposes – even if they may differ from those of other Responsible Entities or of compliance auditors – as long as they are reasonable or justifiable under normal standards of business decision-making.

CIP-004-1

M4.3. To improve the clarity of the language, we suggest changing the third line to read as follows: "...change in status when they are no longer allowed access..."

M4.4, 4.6. These two Measures should be clarified to express that they do apply to contractors and vendors.

Compliance 2.1.2. Since updates need to made to actual access as well as to the access lists, we suggest modifying the second line to read as follows: "...in which access and the access control list were not updated..."

Nonetheless, even with such a clarifying change, it is unclear how such a factor will be measured. Against what is such a list to be compared in order to determine whether it was appropriately updated?

Compliance 2.1.3. The term "properly" is far too subjective in the context used. How will an auditor determine what was proper documentation of a personnel risk assessment program, and under what criteria? If not done generally in each of the Definition sections, it would be more useful if this phrase were to be clarified by the addition of language to the effect that interpretations will be acceptable for compliance purposes – even if they may differ from those of other entities or of auditors – as long as they are reasonable or justifiable under normal standards of business decision-making.

Compliance 2.1.5. The phrase "consistently or" should be deleted, as it creates confusion for the auditing process. The intent of the phrase is unclear. Is it consistency of message content or of delivery methodology? The FAQ seems to indicate that variety of methodology is appropriate. In fact, variety of delivery method is one recognized tool for keeping "fresh" a message that needs to be repeated often. Even addressing only message content as opposed to methodology, how would, for instance, posters used in a program at one time be compared to brochures, or emails, or some other method used to raise awareness at another time? It would be far simpler to audit compliance if this item addressed only the frequency of the message delivery.

CIP-005-1

R1. In the last line of this Requirement, reference is made to "this standard." Since the original Standard 13430 has been divided into eight separate standards, it is no longer clear which standard is intended. For instance, does this refer to CIP-005-1, to the entire set from CIP-002-1 through CIP-009-1, or to some subset of the entire set?

R2. This Requirement is redundant here, as substantially identical material also appears in CIP-007.

R3. Is this intended to be the only permitted solution for dial-up modems? Alternative methods should be allowed.

R4.2. Is this intended to apply to dial-up modems as well?

Is this intended to be the only permitted solution? Alternative methods should be allowed, such as by means of hardware devices.

Moreover, it has been pointed out that the final bulleted method ("call back") can be defeated.

M2. This Measure is redundant here, as substantially identical material also appears in CIP-007.

M5. Is this intended to apply to dial-up modems as well? If so, there are serious technical difficulties with attempting to do so.

M5.3. The original language is unclear and confusing. We suggest that it be clarified by changing it to read as follows: "...implemented to review all access and attempts in order to permit reports and alerts regarding unauthorized access and attempts..."

Compliance 2.1.1, 2.2.2. The time periods in these items are more stringent than for physical security of cyber assets. There does not appear to be a justifiable reason for such additional stringency, and these should be modified to conform to those.

More, there needs to be a reasonable lower bound, as otherwise an Entity could be held noncompliant for even a one-second lapse. Twelve hours has been suggested as a reasonable lower limit.

Compliance 2.3.2. This item is redundant here, as substantially identical material also appears in CIP-007.

Compliance 2.3.3.2. The word "some" is too vague. Either a firm lower limit needs to be established, or it should be clarified that interpretations will be acceptable for compliance purposes, even if they may differ from those of other entities or of auditors, as long as they are reasonable or justifiable under normal standards of business decision-making.

CIP-006-1

Applying these Requirements to generation facilities raises unique and difficult issues that should be dealt with separately, as they will take a great deal of time and attention to adequately or reasonably address. As noted above (at CIP-002-1 Requirement R1.1.1), we believe most of these Standards should not be applied to most generation facilities. There are simply too many locations within any one generating facility that cannot reasonably be secured more than is the plant as a whole. For instance, network wiring may be located in cable-trays throughout the facility.

CIP-007-1

In general, much of the substance in this standard is duplicated in other standards, and thus we have suggested that the other material be removed.

R3.3, 3.5. It would be more appropriate to move these two Requirements into CIP-006, as they appear to relate more to physical access.

R.3.4. In this case, it may be more appropriate to address the issue in CIP-003-1 Requirement R5.5 where there is similar material.

R6.1.3, 6.1.4. There appear to be no Measures that correspond to these two Requirements. As noted above, Measures and Requirements should correlate one-for-one.

M2. The second half of this measure, reviewing access permissions, appears already to be covered, and more appropriately located in, the personnel standard CIP-004. It should be removed from this Measure.

Compliance 2.2.1.1. In CIP-003-1 Compliance 2.2.2, the applicable review period is one calendar year. Although the review issue should be addressed here rather than there, that longer period is the more appropriate term for review.

Compliance 2.3. The intent of the list of items is unclear. It appears that noncompliance with any one or two of the items may result in a finding of Level 3 noncompliance. We do not think it is fair or appropriate for that to be the criteria for such a severe finding.

If the original intent was to penalize noncompliance with any one item on the list, then this entire structure should be moved to Level 2.

On the other hand, if Level 3 noncompliance results only from noncompliance with all of the items on the list, then the list may be appropriate, if somewhat complex.

If there is some other numerical combination that was intended to trigger Level 3 noncompliance, then that must be explicitly stated to allow the industry to comment.

CIP-008-1

No comment.

CIP-009-1

Either the Purpose section or Requirement R1 should recognize that recovery plans may appropriately utilize various established business continuity and disaster recovery techniques, methodologies, and practices.

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 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:	Gerald Rheault	
Organization:	Manitoba Hydro	
Telephone:	(204) 487-5423	
Email:	gnrheault@hydro.mb.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.

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.

CIP-007 R5 “Integrity software” is not used in IT circles to identify any specific genre of applications, so it should be defined. Does it mean only file integrity checking software (e.g. Tripwire), or is a broader definition intended? For example, are host intrusion prevention systems and anti-virus programs considered to be integrity software?

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.

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.

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.

Standards CIP-003 & CIP-007 need to be better coordinated in order to avoid existing confusion, overlap and redundance between the two standards. Suggested improvements are:
1. Rename CIP-003 Security Management removing the word "controls" to imply that this standard contains the high-level policy and governance requirements.
2. Rename CIP-007 Systems Security Controls replacing the term "Management" with "Controls" to reduce conflict with CIP-003 and imply that standard CIP-007 has more technical requirements versus the management requirements in standard CIP-003.
3. CIP-003 R4.2, a repeat of CIP-007 R8.1, should be deleted and left in the more technical standard CIP-007.

CIP-003 uses the term "Executive" while other cyber secuirty standards use the terms "senior management" or "senior management official". One term should be used for all the cyber securtiy standards. Adding the word Senior in Senior Management really has little value.

CIP-003 R1 should not refer to "this standard" or governance "controls". Suggested wording change to:"The Responsible Entity shall create and maintain a cyber security policy which includes governance that addresses the requirements of the cyber security standards."

CIP-003 R2.1 from "The Responsible Entity shall identify and protect all information, regardless of media type, related to the entity’s Critical Cyber Assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible. This includes 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." Removing the last sentence " These documents must be protected as well." and changing the first sentence to include "…identify and protect…".

In CIP-003 R2.2 and R.2.3 use both the terms "categorize" and "classification". We sSuggest using only the term "classification".

Change CIP-003 R2.2 to shorten and clarify as follows: "The Responsible Entity shall classify criticial cyber asset information based on sensitivity; to facilitate that only authorized access occurs."

Delete CIP-003 R2.3 "Responsible Entities must identify the information access controls related to Critical Cyber Assets based on classification level as defined by the individual entity." This requirement is redundant with R2.1 and R2.2.

In CIP-003 R3 change "designate delegate" to "designated delegates" (pural).

In CIP-003 R4.2 suggest replacing "minimal security configuration standards" to "responsible entity's security configuration standards". Testing should also ensure a working functional system before going into production not that just security is in place

In CIP-003 R5 Change to "The Responsible Entity shall institute and document a process for the management of access to information associated with Critical Cyber Assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible." Adding "the" management…

CIP-003 R5.1 Change "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." to "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 designated personnel. All access authorizations must be documented."

CIP-003 R8 Change to "Responsible Entities shall define and document procedures to ensure that modification, suspension, or termination of user access to Critical Cyber Assets is accomplished in a time frame that ensures Critical Cyber Assets are not put at significant risk. All access revocations/changes must be authorized and documented." removing the word "user" as this requirement also applies to asset custodians and owners.

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.

In CIP-004 R3 "background screening" should be changed to "personnel risk assessment". A similar change is required in M4.6 and D1.4.1.

CIP-004 M4.4 mandates a seven year criminal check prior to granting access. This is not allowed by some hiring regulations. The requirement should be that each company has a policy for personnel risk assessment, and that they can demonstrate following that policy - no additional prescriptive requirements should be presented in this area. The company's policy should cover how contractors (or vendors) with authorized access are treated, but should not prescribe how a company needs to treat such circumstances. Any additional information could be included in the FAQs or reference material.

Delete CIP-004 M4.5 as this a Responsible Entity issue and not a NERC issue.

In compliance section 2 focus should be on removing the actual access for personnel rather than updating the list within the prescribe time period.

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.

In CIP-005 & CIP-006 a requirement should clearly state that unauthorized personnel must be escorted by authorized personnel.

CIP-005 R2 is redundant with CIP-007 R9. Delete CIP-005 R2 lefting this requirement in CIP-007.

In CIP-005 the FAQ should provide examples of access points. Are routers and firewalls the only types of access points? Specifically, for devices within the electronic security perimeter, are their keyboards/monitors and corresponding login mechanisms also considered to be access points?

CIP-005 R3 and M3 uses the term "dial-up modem connections" which should include VPN access using networks. Remove the technology reference to modems and perhaps use "dial-up accessible" as in CIP-002 R2.

In CIP-005 R3 we disagree with the requirement for dial-up access physical disconnnection via SCADA. There are other ways to ensure secure dial-up access and this one method should not be listed as a must , rather it could listed as an option or alternative in the FAQs.

In CIP-005 R3 while SCADA activated relays are a relatively secure mechanism, there are insecure aspects to it. For example, SCADA operators could be susceptible to social engineering attacks. Furthermore, there are arguably more secure methods (e.g. requiring two-factor authentication), so the method involving SCADA activated relays shouldn't be put forth as the most secure method. Also, this method is not feasible when stations allow dialup connectivity to be initiated both manually by people and automatically by computers.

In CIP-005 R5 it is unclear what the Responsible Entity must respond to on a 7 x 24 basis. CIP-005 FAQ #6 implies that certain events must be responded to immendiately. If that is the case then it should be stated in CIP-005 and that not all events require this level of response.

CIP-005 R6 "90 calendar days" should be changed to match the "annual" requirement in M6.

Compliance sections in CIP-005 & CIP-006 should more closely align.

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.

In CIP-005 & CIP-006 a requirement should clearly state that unauthorized personnel must be escorted by authorized personnel.

Compliance sections in CIP-005 & CIP-006 should more closely align.

In CIP-006 M5 Logging Physical Access under manual logging "…accompanied by human observation or remote verification." This statement does not belong under logging rather under either/both M3 Physical Access Controls or M4 Monitoring Physical Access Controls.

In CIP-006 compliance section 2 "aggregate interruptions" is mentioned with no previous explanation or reference in the requirements or measures sections. What do they mean? How are they measureed? Is this reallly required?

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.

Standards CIP-003 & CIP-007 need to be better coordinated in order to avoid existing confusion, overlap and redundance between the two standards. Suggested improvements are:
1. Rename CIP-003 Security Management removing the word "controls" to imply that this standard contains the high-level policy and governance requirements.
2. Rename CIP-007 Systems Security Controls replacing the term "Management" with "Controls" to reduce conflict with CIP-003 and imply that standard CIP-007 has more technical requirements versus the management requirements in standard CIP-003.
3. CIP-003 R4.2, a repeat of CIP-007 R8.1, should be deleted and left in the more technical standard CIP-007.

In CIP-007 R1 & R2 a number of various tests are mentioned without explanation such as "information security test, functional test and acceptance test". Perhaps just stating that the requirement is to have documented test procedures is sufficient. As stated in our comment in CIP-003 R4.2 - "testing should also ensure a working functional system before going into production not that just security is in place."

In CIP-007 R1 & R2 the statement ”Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment." is not practical in most situations. It would be better to indicate that a non-production environment would be used to the extent practical or a partial test environment would be required. In most situation end devices can differ from one environment to another which can signifcantly affect the test procedure and test results.

CIP-007 R5 “Integrity software” is not used in IT circles to identify any specific genre of applications, so it should be defined. Does it mean only file integrity checking software (e.g. Tripwire), or is a broader definition intended? For example, are host intrusion prevention systems and anti-virus programs considered to be integrity software?

CIP-007 R5.1 It is unclear which critical cyber assets this applies to. It appears to be for those machines which are directly connected to the internet or a WAN. Is it intended to apply only to those machines which do not have an electronic perimeter? If so, doesn’t that water down the requirement to have an electronic perimeter in the first place? Or if all critical cyber assets need integrity software then just state it.

During the last NERC CIP webcast, Larry Bugh mentioned that when patches are applied, not only must each machine be tested to verify that the patch was properly installed, but also testing must be performed to confirm that the underlying vulnerability no longer exists. Doing this kind of testing on critical production systems seems to go beyond best practices, and it can be destructive. If this

is actually the intention, then this should be reflected in the text of the standards; otherwise it will not be enforceable.

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.

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.

CIP-009-1 R1 indicates annual test frequency while M4 indicates drills every three years. The test frequency should be consistent.

Is there a difference between "exercising its recovery plan" in R1 and "conduct drills" in M4? If not, then the terminology should be kept consistent between R1 and M4. Otherwise, the difference should be explained.

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.

The compliance schedule for Balancing Authorities and Reliability Coordinators is acceptable as stated. The compliance schedule for other facilities is too aggressive considering that most responsible entities will have multiple sites requiring compliance. We suggest that the compliance schedule for other facilities be delayed by one year with SC in 2006, SC in 2007 and AC in 2008.

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:	Keith Fowler, Britt Crawford	
Organization:	LG&E Energy Corp.	
Telephone:	502-627-2724, 502-627-3552	
Email:	keith.fowler@lgeenergy.com, britt.crawford@lgeenergy.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.

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.

We are in agreement with the comments submitted by the ECAR CIPP group.

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.

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.

We are in agreement with the comments submitted by the ECAR CIPP group.

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.

We are in agreement with the comments submitted by the ECAR CIPP group.

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.

We are in agreement with the comments submitted by the ECAR CIPP group. Additionally, we would like to recommend the following changes:

Section i.d.	Current Language	Recommendation – Change to
B. R4	Personnel Risk Assessment – The Responsible Entity shall subject all personnel having access to Critical Cyber Assets, including contractors and service vendors, to a documented company personnel risk assessment process prior to be being granted authorized access to Critical Assets.	Recommend: Most contractors and service vendors conduct criminal background checks as required by their contracts. However, due to privacy concerns, contractor companies may not release criminal background information on their employees to utilities. We recommend adding a statement that the "personnel risk assessment" can be based upon the certification of the contractor that their employee's background is "clear". Change To (add): The personnel risk assessment can be based upon the certification of the contractor that their employee's background is clear.
C.M4.4	The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel prior to being granted authorized 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 identify verification (e.g., Social Security Number verification in the U>S>) 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.	Recommend: Latitude should be provided under "personnel risk assessment process" to substitute a "known" history of an employee for the "seven year criminal check." In essence, "grandfathering" those with a clean 10, 20 or 30 year history with a company in lieu of a seven year check. Criminal histories should then be required for all "company" employees with less than seven years. Change to (add): Employees with a clean 10, 20 or 30 year history with a company may be grandfathered in lieu of a seven year check. A criminal history check is required for all company employees with less than seven years.

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.

We are in agreement with the comments submitted by the ECAR CIPP group.

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.

We are in agreement with the comments submitted by the ECAR CIPP group. We do however have one additional question with regard to **C.M.5**:

Does "physical access logs shall be retained for at least 90 days" intend to require retention of digital electronic capture of video images?

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.

We are in agreement with the comments submitted by the ECAR CIPP group.

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.

We are in agreement with the comments submitted by the ECAR CIPP group.

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.

We are in agreement with the comments submitted by the ECAR CIPP group.

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.

As noted under each of the previous sections we are in agreement with the comments submitted by the ECAR CIPP group. Additionally, we would like to emphasize that in general the timelines are not only too aggressive, but simply unrealistic. In particular if typical planning and budgeting cycles are taken into account implementation work required to address the increased scope likely will not yet have begun, let alone be complete, by the deadlines proposed in draft I of the implementation plan.

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:	Tony Kroskey	
Organization:	Brazos Electric Power Cooperative	
Telephone:	254-750-6357	
Email:	tkroskey@brazoselectric.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.

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.

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.

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.

In Measure M5 the requirement for senior management officer's approval should be reworded to be approval of a member of senior management. The same for M6.

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.

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.

Measure M4.4 describes a background check and criminal check as required. If this is a requirement then it should be stated in R4 and M4.4 would say that documentation is on-hand showing that the checks were completed.

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.

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.

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.

The R1 requirement for testing of security patches is unreasonable. As discussed in the phone meeting on Feb 2, the requirement to check for known vulnerabilities was interpreted to mean that each company would have a test environment that they would use to attempt to exploit the system with the known vulnerability after patches are applied in order to prove that the vulnerability was successfully dealt with. This is unreasonable for several reasons. Several known vulnerabilities have no known exploits making the requirement all but impossible. Several vulnerabilities that have exploits still require a high level of programming skill to exploit. Known exploit code that can be taken from the internet comes from suspect sites and should not be used even in a test lab unless you are prepared to do a complete rebuild of the lab. If you do find that the exploit was not fixed you can not write a patch to fix it, so you the only thing you have accomplished is the ability to notify the vendor that the patch does not work. A more appropriate requirement would be for each company to have the ability to test each system for patch requirements, have a test environment to test patches on before they are deployed on their production system, have a way to verify that the patch was actually applied, have a way to roll the patches back if they cause a problem. We should be held accountable for keeping all systems to the vendors specifications for a "secure" system, not the security testing entity for a vendor. If NERC is going to require the use of some type of vulnerability scanning to take place, then they need to supply a list of approved products as the capabilities of the products in this field vary widely.

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.

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.

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.

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:	Patrick Miller	
Organization:	PacifiCorp	
Telephone:	503.813.7014	
Email:	patrick.miller@pacificorp.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.

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.

In section “Cyber Security Incident”, the term “attempt” should be qualified with adjectives such as “obvious”, “clear”, or “definite”.

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.
Throughout the standards, the requirements do not map directly to the measures (1:1 ratio). It would be much easier to adhere to – and enforce – the measures if they directly represented the requirements. Without the 1:1 relationship, there will be requirements that will go unaddressed to a certain degree.

There is no clear language around the framework or minimum requirements for a "risk based assessment." Without some form of directional statements, models or representations, there will be much confusion and [often only] minimal effort put forth which may not meet the spirit of the standard.

There is a significant amount of redundant information at the beginning of each standard. This can introduce an element of complacency for the reader by presenting the same (or only slightly different) information multiple times. It would create efficiency and clarity if there were a single section for definitions, purpose, applicability, etc…

The current naming convention is very hard to reference, in both type and speech. Since the name has changed from "1300" to "CIP-002-01 through CIP-009-01", it is easier (which will ultimately mean a defacto usage) to revert to "1300" or "CIP." Please consider using a single standard name again, and breaking out the individual standards – something similar to what was used for the 1300 nomenclature but still meets NERC intentions.

The information provided in these reports could, by inference, indicate areas where organizations are weak, or may have insufficient controls/security in place. As such, the information should be protected accordingly. NERC should provide an encryption mechanism so that when this information is submitted it will be appropriately protected.

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.

For section B, the requirements are listed as R1.1 through R1.17. This is inconsistent with the outline format. Assuming that all requirements are not subsets of the first, they should be R1 through R17 instead.

In section R1.15, it makes no sense to remove the requirement for a physical security perimeter around a critical cyber asset simply because it does not use a routable protocol to communicate with other assets. What about substations with only dial up access? Do they not need a physical perimeter?

For the section B, R1.17, our organization has critical cyber assets in Generation, Transmission and IT. This entry implies one senior manager will be responsible for approving the list of critical assets. It would be more flexible if it were 'OK' to have multiple senior mangers approve since these assets reside under multiple senior managers.

For section C, M1 – it is mentioned "…as identified as in R1" which does not exist (as stated above in ID2), rather R1.1. This should be modified to reflect the true reference.

For section C, M2 – it is mentioned "…Critical Assets in R1) which does not exist (as stated above in ID2), rather R1.1. This should be modified to reflect the true reference.

For the section C, M3 – it is mentioned "..as identified under Requirement R2 and all other Cyber Assets as identified under Requirement R3." Neither R2 nor R3 exist, rather R1.2 and R1.3. This should be modified to reflect the true reference.

For the section C, M4, within an organization of our size it may be more appropriate to have a 60 or even 90 day window for update.

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.

For the section B, R2, the subsections are inconsistent with the outline numbering format as R1 through R3 where they should be R2.1 through R2.3 instead. This should be modified to adhere to the correct outline format.

For the section B, R4, the subsections are inconsistent with the outline numbering format as R4 and R5 where they should be R4.1 and R4.2 instead. This should be modified to adhere to the correct outline format.

For the section B, R5, the subsections are inconsistent with the outline numbering format. Items R6 through R8 should either be in line with the R5 with respect to the indentation, or represented as subsections R5.1 through R5.3 to correctly adhere to the outline format.

For section C, M6, it is stated that "The Responsible Entity shall perform an assessment…" – there is no mention of the type or scope of assessment required. The standard "risk based assessment" language should be used.

For the section C, M11, within an organization of our size it may be more appropriate to have a 60 or even 90 day window for update.

For section C, M13, there are two subsections R1 and R2 listed. These subsections should either be in line with respect to the indentation and listed as M14 and M15 or they should be represented as subsections of M13. If these are not subsections of M14, then the rest of the measures should be adjusted respectively.

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.

For section B, R2, the mandated recipients of information handling training should be clarified. Does this include all janitorial staff? Linemen? Ditch diggers? Electrical contractors and plumbers?

For section B, R3, it was mentioned in the webcast that the term “background screening” was replaced with “personnel risk assessment.”

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.

For section B, R4.2, there are bulleted items which can not be referenced within the letter/number outline format. These items should be represented as R4.2.1 through R4.2.6 to correctly adhere to the outline format.

For section C, M4.2, the submeasures are incorrectly referenced as M1.4.2 through M3.4.2. This should be corrected to refer to these submeasures as M4.2.1 through M4.2.3 to adhere to the outline format. If there is no 'real-time' requirement, it would be assumed that log review would satisfy this.

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.

For section B, R3, it is unclear if the monitoring requirement is 24/7 or simply by reviewing logs at a later time/date.

For section C, M3, there are tabled items which can not be referenced within the letter/number outline format. These items should be represented as M3.1 through M3.5 to correctly adhere to the outline format. There is also an unreferenced paragraph at the end of the measure which should have some identifier attached for reference.

For section C, M4, there are tabled items which can not be referenced within the letter/number outline format. These items should be represented as M4.1 and M4.2 to correctly adhere to the outline format. There is also an unreferenced paragraph at the end of the measure which should have some identifier attached for reference.

For section C, M5, there are tabled items which can not be referenced within the letter/number outline format. These items should be represented as M5.1 through M5.3 to correctly adhere to the outline format. There is also an unreferenced paragraph at the end of the measure which should have some identifier attached for reference.

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.

For section B, R3.1, there is the requirement for a 6 character password. Most Best Practice recommendations stand at a minimum of 7 characters, and often 8 characters.

For section B, R3.1, there is the requirement that passwords be changed frequently, but there is no recommended/required expiration period. The standard best practice for this is 90 days maximum (quarterly).

For section B, R5, the use of the term "Integrity Software" is confusing, with respect to the standard information security lexicon. This term is usually reserved for applications such as Tripwire or Intact which use forms of hashing algorithms or similar mechanisms to validate the integrity of a system. The term "AntiVirus Software" is widely accepted and is more appropriate. It is reasonably clear from the context that AntiVirus software is being referenced, and not Integrity Software. If Integrity Software is also required, please specify where they (Integrity Software and

AntiVirus Software) are both applicable. Essentially, the use of Integrity Software in this context is a misnomer.

For section B, R6.1.2, "Scanning" is a powerful term, and may imply that just any utility will work for this need. It should be noted that not all critical cyber assets behave the same when scanned by traditional IT vulnerability scanning tools. Programs such as NMAP can cause serious issues for example.

For section B, R9, though this requirement is worded better, it appears to be redundant with CIP-005-01, section C, M2.

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.

For section B, R2, classification guidelines and examples should be offered.

For section B, R4 – it is stated "…reported to the ES ISAC either directly or through an intermediary." Please define what qualifies as an intermediary (give examples).

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.

For section B, R2 – The language seems unclear. The language could imply that scenario-based plans are required. Scenario based planning is not considered a best-practice approach unless there is a high likelihood of a particular type of event. Following is a suggested amendment:
"The Responsible Entity shall have recovery plans that allow for response to events of varying duration and severity"

Section C, M1 & M2 are duplicate entries and also seem repetitive to Section D, 1.2 Data Retention. Suggest that section C, M1.2 state:
"The Responsible Entity shall maintain records of exercises or drills conducted and maintain those records in accordance to Data Retention Requirements. (3-Years).

Section C, M5 combines two requirements and may be better suited to be separated or the attendance requirement clarified. The first requirement is that a drill is conducted at least every three (3) years. The second is that attendance records are to be kept on Recovery Plan training. Instead of training, is the intent to require attendance records of who participated in the drill? Requiring it for "training" may be too broad, implicating requirements to tracking attendees for awareness training, which can be in many forms.

Section D, 1.2 Data Retention – Seems to be duplicative of Section C, M1 & M2. If Section C requirements are clarified, this section would seem adequately stated.

Suggest an additional requirement in section C. Measures, that states: "The Responsible Entity will include recovery design considerations within the scope of projects that involve implementations, upgrades or modifications to Critical Cyber Assets"

PacifiCorp distinguishes between Business Continuity Plans and Disaster Recovery Plans. This is a common approach across industries. These types of plans are not clearly distinguished within the standards in CIP-009-01.
PacifiCorp Definitions:
Business Continuity Plans are response procedures following events that impact a critical asset site and focuses on mobilization and relocation of employees to continue critical functions at an alternate location.
Disaster Recovery Plans are the technical recovery procedures to recover a critical cyber asset at an alternate location.

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.

PacifiCorp has double (or more) the Transmission line mileage than any other WECC member. Additionally, PacifiCorp has many more substations that most other utilities, by far. Please consider allowing an exception or extension to the compliance for "other facilities" where this is the case.

The terms "Auditably Compliant" and "Substantially Compliant" would be more effective (and accepted) if there were more language around exactly what they mean. Consider providing a minimum and maximum specification or framework for each. As they stand, there is a considerable amount of ambiguity which could lead to misinterpretation.

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:	Gordon Pietsch	
Organization:	Great River Energy	
Telephone:	763-241-2235	
Email:	gpietsch@GREnergy.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.

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.

None.

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.

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.

Requirement R1.1.6 states that "Systems, equipment and facilities critical to System Restoration, including Blackstart generators and substations associated with transmission lines used for initial system restoration" must be included in an organization's list of Critical Assets. It is not clear what the scope of "initial system restoration" includes, and therefore is unclear which substation and transmission lines are to be included. Does this apply only to the substations and lines that directly support a Blackstart generator and are within a certain proximity? Or does it include all subs and lines used in cranking paths to baseload generators? Or is the scope limited in terms of time (i.e., does "initial" mean the first 1 or 2 or 3 days of restoration)?

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.

CIP-003 contains language that is redundant/overlapping with CIP-007. These two should be combined into one.

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.

Suggest a wording change in Section 2.1.2 Levels od non-compliance to focus on whether the access was revoked within 24 hours (rather than focus on whether the access list was updated).

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.

R3 should be modified by deleting all the language except the first sentence and the last sentence. In particular the reference to technically feasibility is to vague. It is adequate to require that entities implement procedures they have defined as appropriate based on their risk analysis.

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.

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.

R5 should be deleted. It could be replaced by ageneral requirement to address the appropriate use of such software in a security plan.

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.

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.

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.

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**
☐ **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: 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**	**SPP**	**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.

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 for Critical Assets listed in each Definitions of Terms page is fine, but it is much different from the definition in CIP-002 where it says "Those Critical Assets include the following" The former definition allows entities to determine themselves which assets are critical. CIP-002 gives a long list of items that must be considered Critical Assets. Responsbible entities should be left to determine their own Critical Assets.

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.

This standard says all cyber assets associated with Critical Assests using routable protocols or that are dial-up accessible are critical Cyber Assets. No mention is made of using an appropriate assessment methodology. A risk-assessment methodology is referenced in R1.1.9 with regard to defining Critical Assets, but no methodology is discussed for determining Critical Cyber Assets.

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.

Once again, listing specific items as being included in the list of Critical Assets is not recommended, but if you are going to keep this list, we offer the following comments:

R1.1.3 - the language is OK, but it would help to include or reference where to find the definition of "elements monitored as IROL's."

R1.1.4 and R1.1.5 are unnecessary. Instead this should merely state any generator whose loss would cause instability, uncontrolled separation(s) or cascading outages.

R!.1.7 - Why reference 300MW for load shedding? Wouldn't this be different for different size utilites?

R1.1.9 - We are still waiting to see what is meant by "risk-based assessments." We've been promised some guidelines on this, but they have still not been produced.

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.

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.

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.

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.

Maintenance of videotapes for logging physical access should be cut from 90 days to something more reasonable, like 30 days.

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 define what is meant by "attended facility" and "unattended facility".

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.

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 clarify the distinction between Requirement R1. "exercise its recovery plan(s) at least annually" and Measure M4. "conduct drills at least every three (3) years".

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.

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 the 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:	**Hein Gerber**	
Organization:	**British Columbia Transmission Corporation**	
Telephone:	**604-699-7484**	
Email:	**Hein.Gerber@bctc.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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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 devided 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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

Remove the use of the term "integrity software" as this is not an IT adopted term. Explicitly say what is intended (e.g., virus detection and intrusion detection software.)

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

Confirm if the title should be “Incident Response Planning” or “Incident Reporting and Response Planning”. The former was used in the introduction title (A.1), the latter was used in the header and seems to be more accurate to the intent.

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.

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.

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:	Bryan L Singer	
Organization:	Rockwell Automation, Chairman ISA SP-99	
Telephone:	205.621.8170	
Email:	blsinger@ra.rockwell.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.

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.

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.

Dear Chairman of the committee:

I do not believe the majority of NERC's Cyber Security Standards CIP–002–1 through CIP–009–1 are ready to ballot at this time, because they do not adequately address a key segment of our country's critical power infrastructure - generation control systems.

I have examined the draft standards as part of my role in developing technical reports, recommended practices and standards for manufacturing and control systems security, as a part of the Instrumentation, Systems, and Automation Society's SP99, "Manufacturing and Control System Security" standards committee.

I am the chairman of this effort, and a representative of many other areas within the industry. As part of Rockwell Automation, I am also the leader in security services and am active in developing and implementing consistent approaches to improve the reliability and cyber-security of the process controls environment. As a long time professional in security of electronic and computer based systems, I am very active in this community as we come to a new realm of understanding about the issues that face process control systems. ISA is interested in consistency with other standards, where appropriate, to avoid end user confusion and an impossible challenge for manufacturers of control systems equipment. To that end, we are working with Tom Flowers of your CSSWG to establish a liaison process that would allow such considerations to be addressed earlier in the process. However, you have asked for comments at this time, and we believe these issues need to be addressed now, before issue, for the standard to be effective.

In addition to the direct impact on generation, generation control systems, if not adequately addressed, become additional "back door" electronic avenues that can compromise the bulk grid that the NERC standard/s appear to be focused on protecting. The standard/s should either acknowledge they do not cover the generation aspects of our critical power infrastructure, or add information on how to treat it.

Wholesale application of typical business systems security approaches to control systems is not appropriate. The ISA SP-99 committee was founded and continues to proceed largely upon this basis. We have assembled over 200 companies across many faces of the industry, representing over 250 individual emembers. We have all united with the common purpose of developing a singular standard which will contribute to the industry as a whole by providing a consistent and thorough approach to control systems security. SP99 was created to provide guidance on how to apply security to control systems. Substantial guidance has been published by the SP99 committee, and has been available since April of 2004. It should be referenced in the NERC standard.

Additionally, given that we have many members from across the industry, including members from other areas of the electrical and power generation community, we recommend a closer relationship between ISA SP-99 and the NERC. A closer relationship is essential to ensure that no competing standards or conflicting information is released that will degrade the goals of the industry as a whole.

Joe Weiss, a member of ISA's SP99 , and NERC 's CSSWG, has provided specific comments and recommended revisions which address these concerns. Those comments should be responsibly addressed.

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.

See comments above

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.

See comments above

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.

See comments above

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.

See comments above

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.

See comments above

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.

See comments above

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.

See comments above

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.

See comments above

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.

See comments above

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:	Jerry Heeren	
Organization:	MEAG Power	
Telephone:	770-661-2866	
Email:	jheeren@meagpower.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.

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.

Bulk Electric System needs to be defined clearly. NERC has created confusion by allowing varying definitions to appear in different locations. For example, NERC's Cyber Security Standards FAQ says the Bulk Electric System is above 35kV or as approved in a tariff filed with FERC; NERC's TOP-003-0 Standard shows the Bulk Electric System as greater than 100kV; NERC staff has verbally mentioned that the Bulk Electric System includes those systems above 100kV; and finally, NERC's Version 0 Glossary says the Regional Reliability Organization should define Bulk Electric System, with 100kV as a minimum. MEAG Power believes that the Bulk Electric System should be defined as those systems that operate above 200kV. MEAG's suggested definition of Bulk Electric System follows: "Bulk Electric System – A term commonly applied to the portion of an electric utility system that encompasses the electrical generation resources and high-voltage transmission system (above 200kV)."

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.

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.

A3 and R1.1 - The term “bulk electric system” needs to be capitalized in R1.1, and defined on the Definitions of Terms page. A definition of this term is suggested at the top of this document.

Each of the eight Cyber Security Standards, including this CIP-002-1, begins with a page of definitions. One of the defined terms is Critical Asset. Yet within CIP-002-1, requirement R1.1 presents a significantly different definition of Critical Assets. The definition at R1.1 lists specific items that are not on the Definition of Terms page. But the R1.1 definition also omits concepts that are on the Definition of Terms page (for example, time, heath, and safety). Why are two different definitions needed? This ambiguity makes it difficult for smaller utilities to determine whether CIP-003 through CIP-009 apply.

R1.1's definition of Critical Assets uses two terms: "the electric grid" and "the interconnected bulk electric system." While the Cyber Security FAQ's Venn diagram does depict the "Bulk Electric System," it does not show "the electric grid." We believe that there are portions of the electric grid that lie outside the bulk electric system. We do not believe this standard was intended to apply to all of the electric grid, including for example our 46 kV and 69kV assets. Unless this definition is clarified, we will decide for ourselves which portions of our electirc grid (>200 kV) comprise the bulk transmission system when we perform our risk-based assessment.

We own but do not directly operate any Bulk Electric System generation or transmission facilities. We are joint owners of assets that are operated by another owner. Thus, we recommend that the last sentence in R1.1 be changed to read: "Those Critical Assets may include the following:"

R1.1.4 and R1.1.5 use 80% of the Region's largest single contingency as a threshold for defining critical generation assets. Yet R1.1.7 uses 300 MW as the threshold for defining automatic load shed systems as critical assets. In our Region, the difference between the generation threshold and the load shed system threshold is greater than 500 MW. This means relatively small generators are NOT considered critical to reliability, but the same magnitude of load shed capability IS critical to reliability. Why use such different thresholds? We suggest changing the 300 MW used under R1.1.7 to the same 80% standard of largest single contingency as is used in R1.1.4 and R1.1.5.

R2.1 – The term “routable protocol” needs to be defined and clarified further. Does routable protocol include TCP/IP and DNP 3.0 only – or are there other routable protocols? Also, is the R2.1 requirement removed if a “routable protocol” (as it is defined) is encrypted?

Other Comments – Requirements and Measures numbering scheme does not match.

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.

A3 - The term "bulk electric system" needs to be capitalized and defined in the Definitions Section of CIP-003-1. A definition of this term is suggested at the top of this document.

M14 needs to be clarified. Perhaps its intent would be clearer if two simpler sentences were used in place of one very complicated sentence.

In the Compliance portion of this Standard, the Data Retention subparagraph 1.3.4 discusses documentation of mitigation strategies. However, the need for mitigation strategies is not established in any Requirement or Measure.

Other Comments – Requirements and Measures numbering scheme does not match.

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.

We suggest that the phrase “background screening” in R3 be replaced by the phrase “identity verification” – as in other areas of the document.

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.

We suggest that the beginning of section R1 begin with, "To the extent technology allows, the Responsible Entity shall enable only those ports/services required…" Certain technologies (e.g., network hubs) do not allow for port by port configuration and disabling. Typically only Layer 2 and 3 switching/routing devices allow for the disabling of individual ports.

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.

Other Comments – Requirements and Measures numbering scheme does not match.

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.

We suggest that the words “security patches" and "cumulative patches” be removed – as most utilities do not have the capability of and cannot test every software patch that a software manufacturer releases – such as Microsoft, HP, etc. In addition, to fully test whether or not a software patch works, a utility’s controlled non-production environment would need to be attacked before and after a patch was applied – to prove that the new patch works. This could be an expensive approach since a utility would have to fully duplicate hardware and software for the systems under test. In addition and in certain cases, if a utility were to try to prove that certain software patches were 100% effective, a utility may have to attack its production environment (versus non-production environment) to verify whether or not a patch worked. Testing in a production environment is very dangerous and can be compared to putting a gun to your head. As a general statement, NERC needs to trust that the general software industry will update its registered users (i.e., utilities) as appropriate on software patches/fixes. In turn, NERC needs to ensure that its utility members will 1) get the software patches that they need and 2) that they will apply the software patches as appropriate and within acceptable timeframes.

Other Comments – Requirements and Measures numbering scheme does not match.

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.

Other Comments – Requirements and Measures numbering scheme does not match.

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.

Other Comments – Requirements and Measures numbering scheme does not match.

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.

Until the CIP standards are more clearly defined, MEAG Power cannot make a judgment call as to the appropriate timeframes for compliance.

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**
☐ **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 Power Company

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*
Greg Stone	**Duke Power Company**	**SERC**	**1**
Mark Tully	**Duke Energy Corporation**	**SERC**	**6**
Phyllis Withers	**Duke Power Company**	**SERC**	**1**
Mike Butler	**Duke Power Company**	**SERC**	**5**
Vicky Bannon	**Duke Power Company**	**SERC**	**1**
Glen Frix	**Duke Power Company**	**SERC**	**5**
Jon Decoste	**Duke Power Company**	**SERC**	**5**
Ernie Scronce	**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.

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.

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.

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.

Overall – Effective date of 10/1/05 for this standard is probably reasonable.

Where "nuclear" ends and "transmission" begins is still an open issue.

R1.1.7: is senior management REALLY required? Who is that? A VP, a direct report to a VP?

R1.1.7. A member of senior management must approve the list of Critical Assets and the list of Critical Cyber Assets.

R1.1.5: is the logic backwards here? Wouldn't a dial up asset need physical security MORE than electronic?

R1.1.5. Dial-up accessible Critical Cyber Assets which do not use a routable protocol require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter

R1.2 – Uses a different definition for Critical Assets than used in definitions Section. Need to clarify which is correct. Need to define "detrimental impact".

R1.6 – Does a common control system constitute "common system". If so, then essentially ALL generating resources of a large CA would fall under this requirement. An example of how purported flexibility is superseded by broad scope expectations

B - R4 – What level is considered senior management? Should say senior management or designee.

R4, M5, M6, D1.3.4 – Says senior management officer in M5 & M6, says senior management in R4, senior management official in D.1.3.4.

M3 – Correct the error ...Critical Cyber Assets identified under Requirement R3... should be R2.

D - 1.2 – How do we verify updates were made within 30 calendar days?

M4: 30 calendar days is too strict.

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.

Overall – Effective date of 10/1/05 for this standard is unrealistic due to requirement B R2.1

Creates administrative nightmare spanning multiple organizational departments/functional model entities.

M3 – Senior management official ? Consistency…

M13 – Says executive level management… all standards need to be consistent with management level requirements?

M13.2 – typo? …shall verify that all the Responsible … ?

M1.4 – what is this trying to say?

M4, M5, M6, M13: is annually really necessary? Will things change that often? It would be better to review AFTER significant changes or at a period not to exceed 3 years.

M10. Identity of the individuals should be just sufficient to uniquely identify the person. Titles and business addresses are subject to change and these events should not require an update of the program documents.

M15. Identity of the individuals should be just sufficient to uniquely identify the person. Titles and business addresses are subject to change and these events should not require an update of the program documents.

R2: looks like formatting (step numbering for sub-steps) is messed up. The first item under R2 probably should be R2.1, then R2.2, etc.

R3 – What level is considered senior management? Is this one person for the entire company or can there be several?

R4 – Says executive level management… all standards need to be consistent with management level requirements?

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.

Overall – Effective date of 10/1/05 for this standard is probably reasonable.

A - 4 – typo? Any reference in this Standard to Critical…. Why is this repeated here and in A - 3 ?

R3 – Clarify requirements for Responsible Entity to retain records for contract employees. These employee records are typical created and retained by the contracting agency, not the Responsible Entity.

R4 – Clarify this requirement or a "risk assessment"

M4.4. This requirement is an impediment to the rapid response requiring the intervention of a vendor and should be dropped. Further, it is discriminatory since some employees would be checked more rigorously than others and the minimum requirements would produce no reasonable assurance that a person is not a security risk.

M4.2 – Seven days may be difficult in some cases to achieve.

M4.3 – Seven days may be difficult in some cases to achieve.

M4.4 – Do we have to conduct background screenings on current employees?

M4.3 Physical and electronic access revocation must be completed within 24 hours for any personnel terminated for cause and seven calendar days for any personnel who have a change in status where they are not allowed access to Critical Cyber Assets (e.g., resignation, suspension, transfer, requiring escorted access, etc.).

M4.6 – Uses term "screening". Term "risk assessment" is used elsewhere. Be consistent. Requiring updated screenings every five years is burdensome and will provide no reasonable assurance that a person is not a security risk. What would update screenings entail?

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.

Overall – Effective date of 10/1/05 for this standard is unrealistic due to the volume of systems that must be documented and setup for monitoring.

We are still getting our hands around this one.

A - 4 – typo? Any reference in this Standard to Critical…. Why is this listed here and in A - 3 in the other standards?

R5: this is a HUGE effort. It will take a LONG time to implement.

R6: this is an even LARGER effort than #R5 above. It will take an even LONGER time to implement.

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.

Overall – Effective date of 10/1/05 for this standard is unrealistic due to the volume of systems and locations that must be modified or enhanced to become compliant with the required physical access restrictions.

The entire issue of logging may need to be addressed. Does Duke have any "critical assets" in remote locations? How expensive is it going to be to meet the logging requirements? To implement manual logging as described in M5, the utility would have to automatically send two technicians on every job. And if one wanted to be devious, he'd just go back after hours when no-one is around. Plus, such manual logging is reactive at best. It won't prevent anything.

Is this intended to require physical security (including logging, monitoring, maintenance and testing, etc.) at remote, unstaffed, substations?

A - 4 – typo? Any reference in this Standard to Critical…. Why is this listed here and in A - 3 in the other standards?

R1.1. Need the definition of "defense strategy". Tom: This appears to be more than passive physical security provided by locks, etc. Do others read it this way?

M3 – Security Enclosure is a nice addition to this requirement. It will still be a significant feat to get all the cabinets at these locations where they can be locked.

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.

Overall – Effective date of 10/1/05 for this standard is unrealistic due to the volume of systems and locations that must be modified or enhanced to become compliant with this requirement.

A - 4 – typo? Any reference in this Standard to Critical…. Why is this listed here and in A - 3 in the other standards?

R3.1 – typo? … stronger than passwords and don't but do not require a password ...

R3.1: strong passwords are a great idea, but do our legacy systems support this?

R3.3, R3.5 – Is this talking about physical access or electronic access? This requirement is confusing.

R4.2: a MONTHLY review of security patches available will be a huge effort.

R5: the definition of "INTEGRITY SOFTWARE" should be included in the definitions section.

R6.1: scanning annually - huge burden. Plus, will operational equipment support such scanning? Such scanning must be done VERY carefully if at all.

R11 – Annual test of complete system restores is a MAJOR, very time consuming requirement.

M2 – Is it necessary to repeat the password requirements here and in CIP-004-1, C - M4.3 ?

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.

Overall – Effective date of 10/1/05 for this standard is probably unrealistic due to the volume of systems that must be modified or enhanced to become compliant with this requirement.

R2 - R4 –Should these requirements be sub-bullets of R1?

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.

Overall – Effective date of 10/1/05 for this standard is probably unrealistic due to the volume of systems that will require physically being at the system to be modified or enhanced to become compliant with this requirement.

A - 4 – typo? Any reference in this Standard to Critical…. Why is this listed here and in A - 3 in the other standards?

R1: create recovery plans and exercise the recovery plan at least annually - huge burden depending on the scope. If the scope is every piece of critical equipment, then this is darn near impossible.

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.

See comments for the specific standards for Implementation Plan change recommendations.

There seems no better place than this to include general comments, so below are comments that apply to multiple standards:

- General formatting is still problematic and creates problems following references. The numbering scheme is confusing and not consistent. Why use R's, M's, then switch to numbers?
- Clarification is needed whether the implementation plan is included in proposed ballot process. If not, how can we be assured plan will not be changed requiring more immediate compliance?
- This has much broader impact that 1200. Other than delaying implementation of 2 years, we need to review scope and refine to take a smaller incremental step from 1200.
- The implementation plan dates is too aggressive and not realistic.
- While this purports to provide flexibility in determining which assets are in scope, the words used in defining Critical Assets/Critical Cyber Assets are very broad and include expectations that scope is very broad.
- What excludes a unit or station from being in the plan?
- Clarification on controlling access to transmission control houses is needed.

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:	James W. Sample	
Organization:	California Independent System Operators	
Telephone:	916-608-5891	
Email:	jsample@caiso.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.

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?

☒ Yes
☐ 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?

☐ 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 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

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.

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 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 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.

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 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 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.

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 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 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.

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 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 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.

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 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 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.

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 comments in Question 3 above and Specific comments in attached

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 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 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.

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.

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 ful 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 previouly) 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.

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:	Terry Doern	
Organization:	Bonneville Power Administration, Department of Energy	
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**	☒ ☐ ☒ ☐ ☐ ☒ ☐ ☐ ☐ ☒	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*
Jon Stanford	**BPA Cyber Security**		
Randi Thomas	**BPA Transmission**		
Sharon Brown	**BPA Transmission**		
Cliff Carpenter	**BPA Power**		
Ross Pies	**BPA Power**		
Paul Arnold	**BPA Transmission**		
Joe Andres	**BPA Transmission**		
Jon Daume	**BPA Transmission**		
Bob Windus	**BPA Physical Security**		
Roger McElhaney	**BPA Cyber Security**		

* 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.

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.

Cyber Assets: change 'communication networks' to 'computer networks'. NERC has stated that telecommunications is excluded and will be addressed in a separate standard.

Cyber Security Incident: '. . . . malicious act include accidental, unintentional.'

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.
BPA prefers that risk assessment be based on electrical utility criteria such as safety, reliability & economics. This will help all electrical utilities insure more consistent results during audits.

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.

R.1 Issue: The first sentence in the requirement states that the entity must identify their Critical Assets using their preferred risk-based assessment followed by R1.1, which provides a detailed list of all the Critical Assets that must be on the list. Requirement R1.1.9 then repeats the verbiage in the first sentence in R1.
Recommendation: Delete the first sentence in R1 and move the verbiage from R1.1 to R1. Make the second sentence in R1, the second sentence in the new requirement.

R1.1 -- A numbering issue: There is no need for a R1.1 if there is no R1.2.
Recommendation: Make R1.1 part of R1 and renumber R1.1.1 thru R1.1.9 as R1.1 thru R1.9.

R2.1: This should specify that the critical cyber asset is ONLY exclusively and/or remotely accessible via dial-up, direct physical connection or wireless, and does not use a routable protocol. It is unclear what situation is trying to be addressed. Please be specific.

R2.3 Issue: Requirement is confusing. It's not clear why a critical cyber asset would not need to be physically protected.
Recommendation: Show an example similar to - 'What about an external laptop dial-up from home, connecting to a controlled location?'

R2.3 and R3 Issue: Requirement discusses Electronic and Physical Security Perimeters. The physical and electronic perimeter should not alone be a factor for producing a list of Critical Cyber Assets. While it is best practice to hold all cyber systems within an electronic security perimeter to the highest network security requirements, it does not, by default, make them all Critical Cyber Assets. One system in the network could be turned off without impact to the mission while the other cannot. Incident response while required will be different.
Recommendation: Delete R2.3 and R3. R3 is taken care of by the last sentence of CIP-003-1 R1. CIP-002 should be limited to the requirements for identifying critical cyber assets.

M3 Issue: Measure refers to R3 twice in the same sentence when it should refer to R2 in the first reference. Recommendation: Change the first R3 to 'R2'.

D. 1.3- Compliance: What is the definition of making the following documents available for inspection? Since these documents contain sensitive information - - is this an only on-site physical inspection? These documents shall not be mailed, e-mailed, faxed, or otherwise taken off-site!
Recommendation - Change text to now read 'The Responsible Entity shall make the following available for inpection on-site, by the compliance monitor upon request'

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.

CIP003 R1, R2, R3
Issue: Requirement R1 is not titled.Recommendation: Title it 'Cyber Security Policy:'

Issue: Requirement R2 is not titled.Recommendation: Title it 'Information Protection Program:'

Issue: Requirement R3 is not titled.Recommendation: Title it 'Roles and Responsibilities:'

R4.2 & M13.2 (repeated in CIP-007) Issue: Requirement CIP-007 R8.1 and M7 appear to be duplicates of CIP-003-1 R4.2 and M13.2. CIP-003 should be focused on management level policies, roles, responsibilities and procedures that apply to all systems while CIP-007 should be a system level requirement to ensure the Change Control Process has been and is being followed. Recommendation: Modify CIP-003 R4 such that it is clear the measures and compliance is management level documentation. Modify CIP-007 so it is clear the measures and compliance are system level documentation (i.e., a system unique identifier, system user and maintenance documentation that represents the system, test reports for the production version of the system, etc.)

R4.1 Significant Issue: Requirement defines the role of the designated approving authority to formally authorize and document that the system has passed testing criteria and to for verifying that a system meets minimal security configuration standards. Under the NIST SP 800-37 'Guide for the Security Certification and Accreditation of Federal Information Systems', the designated approving authority (authorizing official) is the official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk.
Recommendation: Change this section to read 'Responsible entities shall designate approving authorities that will formally assume responsibility for operating the Critical Cyber Assets. The approving authority shall ensure a comprehensive assessment of the system's compliance with this standard has been performed to determine the extent to which the cyber security controls are implemented correctly and operating as intended.

R4.1 Clarification Issue: The requirement mentions minimal security configuration standards but these are not clearly mentioned under CIP-005 'Electronic Security' or CIP-007 'Systems Security Management'.
Recommendation: Update CIP-003, 005, and/or 007 to more clearly show the association between the responsibility to verify minimal security configuration standards and CIP-005 and CIP-007.

R5 Issue: Requirement R5 is not titled.Recommendation: Title it 'Access Authorization:'

Compliance 2.4.6 Issue: This is the first mention of the phrase 'corporate governance program'. Requirement R4 uses the phrase governance process. Recommendation: Include this phrase in Requirement R4 and Measure M13 for clarity.

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.

R4: Add 'If background checks cannot be completed prior to access, they shall be escorted at all times.'

M4.4 Issue: This measures requires a 7-year criminal check versus the normal 5-year criminal check. In accordance with BPA Human Resources Personnel Letter No. 731-1 dated July 2, 2004, the current National Agency Check and Inquiries (NACI) performed for all new BPA employees and the equivalent performed for contractors is only 5 years. BPA performs the minimum federal background investigation for suitability for federal employment. This is also true for the background investigations for 'Public Trust' positions. Recommendation:
Change to 'five year criminal check' versus seven, or add a comment - 'may be less than 7 years because US, state or local regulations may take precedence .'

M4.6: DOE cannot perform timely background checks for this quantity of employees, to meet this standard. BPA may need to write an exemption.

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.

R2. : Replace where it states 'The Responsible Entity shall enable only those ports/services required for normal and emergency operations of Critical Cyber Assets' with 'The Responsible Entity shall enable only those ports/services required for normal and emergency operations and monitoring of Critical Cyber Assets'.

R2.3 and R3 Issue: Requirement discusses Electronic and Physical Security Perimeters. The physical and electronic perimeter should not alone be a factor for producing a list of Critical Cyber Assets. While it is best practice to hold all cyber systems within an electronic security perimeter to the highest network security requirements, it does not, by default, make them all Critical Cyber Assets. One system in the network could be turned off without impact to the mission while the other cannot.

e.g. Incident response, while required, will be different for non-critical assets.

Recommendation: Delete R2.3 and R3. R3 is taken care of by the last sentence of CIP-003-1 R1. CIP-002 should be limited to the requirements for identifying critical cyber assets.

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.

R5: Change 'Unauthorized Activity' to 'Unauthorized Access'.

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.

R1 Issue: Many of the requirements in R1 should apply to Critical Cyber Assets in unattended facilities. Recommendation: Change R1 so that it addresses all requirements that apply to both attended and non-attended.

R2 Change R2 to address the requirement of storing procedures at an attended site.

R3: Define Attended and Unattended

R3.2 Issue: Many of the requirements in R3.2 should apply to Critical Cyber Assets in unattended facilities also. Recommendation: Delete 'Attended' or change the wording on R3.2 so that it is understood which requirements apply to cyber assets at both attended and unattended facilities.

R3.3 Issue: Change item to address only that users must request physical access to an unattended facility for each individual event OR delete 3.3 OR move to the physical standard.

R8.1 M7 Issue: Requirement R8.1 and M7 appear to be duplicates of CIP-003-1 R4.2 and M13.2. CIP-003 should be focused on management level policies, roles, responsibilities and procedures that apply to all systems while CIP-007 should be a system level requirement to ensure the Change Control Process has been and is being followed.
Recommendation: Modify CIP-003 R4 such that it is clear the measures and compliance is management level documentation. Modify CIP-007 so it is clear the measures and compliance are

system level documentation (i.e., a system unique identifier, system user and maintenance documentation that represents the system, test reports for the production version of the system, etc.)

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.

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.

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.

Recommend extending general implementation date at least until 1st quarter 2007 for Control Centers' Balancing Authority.

We can't comment on the implementation plan until we understand the scope of the requirements. For example due to size and scope of our system, an assessment could take upwards of a year. Completing the technical feasibility study and addressing budget issues related to implementation could take multiple years.

In some cases like CIP006 Physical Security M4 Alarm System or CCTV, full compliance could take 20 years assuming 4-5 sites a year are improved to the standard at a cost of $100,000 or more per site.

GENERAL COMMENTS:

1- Address the situation where dial-up relays a Single Relay

3) Assessment of Assets is a lot of work and will take 6-12 months to complete before follow-up work can begin. This should delay the implementation schedule.

4) Documentation must be manageable not burdensome. A few control center sites versus hundreds of field sites. For example BPA has an estimated 5,000 intelligent electronic devices that could be considered critical. Just listing them all, let alone changing all the passwords if someone retires - - as only one of many change tasks, is burdensome. We would have to visit each and every site within 7 days. Impossible!

5) It is unclear if our risk assessment should address just a single contingency (N-1), a double contingency (N-2) or multiple contingencies (N-K). From the power system engineering point of view N-1 is achievable, N-2 is difficult, N-K is impossible

6) GENERAL Issue: Requirements are not consistently titled. The requirements in CIP-002 and CIP-003 don't use titles. CIP-004 titles each requirement with a hyphen prior to the actual requirement. Some requirements are titled followed by a colon. Recommendation: Title all requirements and use a hyphen or a colon consistently for CIP-002 thru 009. A Techical writer needs to edit this material - - not an engineer or cyber security professional.

7) GENERAL Issue: It's difficult to correlate requirements to the associated measures, compliance data retention, and the levels of non-compliance in the standard.Recommendation: Use the requirement title, a numbering scheme or a table that shows the correlation to the requirements. (e.g., R1.1 M1.1). CIP-003 is number poorly.

8) GENERAL Issue: The procedure to exempt items in these standards should be clearly defined at the start of each standard.

9) GENERAL Issue: The words 'entity and responsible entity' are used in various ways throughout CIP standards. Clarify if possible.

10) GENERAL Issue: Non-routable protocols may be cyber security risk in some cases and should not be excluded where there is a risk to the power system. Recommend adding text where needed stating - 'if high risk to the power system safety or reliability then non-routable protocols shall be considered, using these standards.'

11) GENERAL DOUBLE-CHECK: FISMA may take precedence over NERC. ???? Did this get resolved? If so where?

12) GENERAL: It may be nearly impossible to be compliant with CIP002-009 due to the large scope, number of sites, thousands of critical cyber assets and detailed documentation requirements. A better approach towards compliance would be for the utility to identify its most critical issues using a risk based assessment and then devote staff and money to resolving the most critical items. Striving to be compliant for low value work when it could impact reliability is not prudent utility practice. Compliance with burdensome documentation or low probability risks shall not take resources away from our key missions – to be safe and to keep the lights on.

13) The exemption process must be a tool for management to reach compliance for these standards.

14) Control centers compliance reporting should be separate from unattended facilities such as substations.

15) The implementation plan should be prioritized to fix the most critical cyber assets first.

----------MATERIAL FROM THIS POINT ON HAS BEEN APPENDED FROM WECC's SUBMITTAL DOCUMENT FOR REFERENCE ----------
---

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.

1. Cyber Assets – In this definition you refer to 'communication network'. The understanding is a separate standard is going to cover the communication networks. In the case of this standard,

you should qualify this right up front and add something like this to the definition: (for the purpose of this standard, communications links connecting discrete electronic perimeters are not considered.)

2. Throughout the standard you refer to the term 'authorized access', so shouldn't it be included in the definitions section? Suggested definition would be: 'is Access that is granted according to an established scheme of governance.'

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.

Even though the above answer is 'Yes' it is still unclear on how to identify critical assets. We would like to see the process and a flow chart on how to identify critical assets.

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.

Introduction/Purpose:

In the second paragraph of the introduction it reads ', where loss or compromise of these assets…' it should read ', where loss of availability or compromise of the integrity of these assets…'.

Requirements:

R1.1 & R1.1.2 – change 'such as' to 'shall include'

R1.1.1 – change 'performing' to 'with' to read: '…backup control centers with the functions of…'.

R1.1.3 – This requirement should state that it excludes anything not in the direct transfer path associated with the IROL.

R1.1.7 – Shouldn't the load shedding requirements refer to the reporting requirements imposed operating standards versus the prescriptive 300 MW. Tie it to reporting criteria.

R2 – We are looking for more clarification regarding this requirement due to mixed messages from the working, the NERC 1300 Web cast, and discussions with drafting team members. If a control center and a plant have routable protocols within each of their electronic perimeters, but have no routable protocols through their electronic perimeter are both or either subject to the electronic requirements of this standard? Understanding that both are subject to the physical security requirements of this standard.

R4. – Due to the update frequency of a detailed list, this requirement should be wording in a manner that will only require senior management to sign off on functions/systems and not the detailed components of these functions/systems. The detailed list is required to be keep up to date by an operational unit.

Measures:

M5 & M6 – These measures refers to 'Officers' and is not consistent with all other references to 'Senior Management'. These measures should also include time frames like all the other measurements (e.g. M4). Suggest a measurement of an annual review.

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.

Measures:

M5 & M10 – M5 uses the term 'information security protection program' and M10 users the term 'cyber security program', was this intended? If so, why? If not, this needs to be fixed.

Compliance:

2.1.1 – 'for less' should be changed to 'for more than'

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.

Measures:

M4.6 – Instead of reading, 'The Responsible Entity shall conduct update screenings at least every five years or for cause', should read, 'The Responsible Entity shall conduct personnel updates as per their documented company personnel risk assessment process at least every fives years or for cause.'

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.

Requirements:

R3 – 'Unattended' doesn’t apply, you should comply with this requirement regardless if the facility is attended or unattended.

R4.2 – The word 'logical' is not needed.

R4, R4.2, & R5 – The reference to 'organizational, technical, and procedural controls' are not consistently used in R4 and R5 sections.

R4.2 – Digital certificates is a form of Two-factor authentication. Should be removed as it's own bullet and be used as an example for Two-factor authentication.

R4.2 – In the sentence 'These strong procedural or technical measures shall include at least one of the following measures', 'measures' should be replaced with 'methods'.

R5 – Best practices is not to necessarily perform real-time monitoring of authorized access, but rather create logs to track authorized access in a manner that creates an audit trail. We agree that you should 'monitor' unauthorized access attempts. So, this requirement should be worked in a way that allows for best practices without creating unnecessary administration overhead that doesn't reduce any risk.

Measures:

M1 – Remove the reference to 'all interconnected Critical Cyber Assets within the security perimeter'. We agree with maintaining documents depicting the Electronic Security Perimeter(s) and all electronic access points, however, documents depicting interconnectivity within the security perimeter changes often and is captured in design and maintenance documents.

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.

The WECC EMSWG is deferring this section to the WECC Physical Security Working Group chaired by Tom Glock.

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.

Introduction/Purpose:

The sentence that reads, 'A System Security Management Program is necessary to minimize or prevent the risk of failure or compromise from misuse or malicious cyber activity' should read 'A System Security Management Program is necessary to ensure system availability and integrity by minimizing or preventing malicious and non-malicious activity and misuse, whether authorized or unauthorized. This includes measures necessary to detect, document, and counter such threats.'

Requirements:

R1 – In some cases production systems are taken off-line and removed from production mode and used for testing. We feel that this needs to be permitted and clarified within this requirement.

R2 – The second sentence in this requirement is not clear. It needs to either be clearly reworded or removed.

R3 – Instead of requiring the entity to '…establish an account password management program' it should require the entity to 'perform account management'.

- End the first sentence at 'unauthorized system access.' striking 'by compromised account passwords.'

- Replace 'not limited to' with 'must meet' or 'at a minimum'

R3.1 – Replace 'shall use accounts that have a strong password' with 'shall use strong passwords'.

R4.2 – Remove the first sentence in this requirement.

R5.1 – In this requirement it isn't clear where it must be applied. If it is intended for all CCAs, regardless if at the perimeter or internal to the perimeter, it should clearly state that.

R6.3 – 'Unattended' doesn't apply, you should comply with this requirement regardless if the facility is attended or unattended.

R11 – The last sentence in this requirement doesn't make sense. Why can you not effectively test on-site at unattended facilities? Recommended removing this sentence.

Measures:

M2 – Fix typo. 'n' should read 'in'.

M10.1 – Replace 'backup data and tapes' with 'backup media'.

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.

This Section refers to the NERC Security Guidelines for the Electricity Sector: Threat and Incident Reporting that uses the term 'any suspicious event' as a requirement for incident reporting. The concern is that 'any suspicious event' could include most firewall interceptions (and there may be hundreds/day) and that we have 60 minutes to report them [day or night] or be assessed a level-3 non-compliance penalty. We need better definition here.

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.

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.

General Comments:

1. Should clearly correlate 'Requirements' to 'Measures' and 'Measures' to 'Compliance'. This way there is a clear relationship all the way from requirements to compliance. Currently it is hard to correlate this and it appears that in several cases they don't correspond with each other.

2. The term 'shall' is used in both the 'Requirements' and 'Measures' sections. The term 'shall' should only be used in the 'Requirements' section and the 'Measures' section shouldn't use 'shall' but rather performance language.

3. This standard should be broken up into two distingue standards. One with specific requirements for Control Systems and one with specific requirements for plants and sub-stations. This standard seems to be more focused on Control Systems where the requirements seem to fit very well, however, due to the technology, etc. at plants and sub-stations, these requirements don't fit as well. Also, there is a different risk model for Control Systems versus plants and sub-stations. Due to the risk difference there are should be distingue requirements for each.

4. Technical feasibility – along the lines of the comments above in 3, if this standard isn't separated between Control Centers, plants, and sub-stations it should take into consideration the technical feasibility of the requirements and annotate it so that the 'exception to standard' overhead doesn't get out of hand. We don't want to make this counter productive by creating a massive about of paperwork administration not allowing us to focus on the spirit of the standard.

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:	Edwin C. Goff III	
Organization:	Progress Energy	
Telephone:	919-546-3862	
Email:	edwin.goff@pgnmail.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.

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.

Critical Asset - clarification requested - what is meant by "significant impact", "large quantities of customers", and "extended period of time?"

Add a definition of routable protocol. FAQ 7 refers to OSI layer 3, as the definition. This could be construed to include field bus devices such as smart transmitters, and other field input devices, located through out a typical power plant or sub station. Field bus protocols such as Foundation Fieldbus, Profibus, and Device Net, which are used for communication between field instruments and Control processors should be excluded. These field devices pose no greater security threat than conventional hard wired field devices connected to a control processor or RTU.

GENERAL COMMENT FOR CIP-002-1 THROUGH CIP-009-1:

Comment 1 -- Consider using the following in all standards: The guidance included in the CIP Cyber Security Standards are applicable to Critical Cyber Assets where technically feasible and when supported by the operating system and software applications unless implementation of these controls cause system performance degradation to a level that causes adverse impact to reliable operation of Critical Assets.

Comment 2 -- Overall there appears to be significant administrative burden attributed to record keeping, largely for auditing purposes rather than enhancement of cyber security. This burden becomes significant largely due to newly defined processes and mandated frequency of reviews.

Comment 3 -- This version has introduced new processes that are far beyond those of the 1200 standards such that even entities which were substantially compliant under 1200 will find it very difficult to be compliant with the new standards given the implementation plan of these standards becoming effective October 2005 and then certifying compliance in 1st Qtr 2006.

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.

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.

R1.1.4 - If multiple generating plants are located on the same site and share a common control room, do those individual plants have to be summed when determining if they meet the 80% Regional Reliability Organization contingency? These plants may or may not be generating at the same time.

R1.1.7 - -- Clarification requested. - In the response to comments of the 1st draft of 1300, the Drafting Team indicated that NERC span of control does not include Distribution Systems. Please clarify that Distribution Systems capable of shedding in excess of 300MW of residential load control are excluded.

R2 - It is my understanding that requirement R.2.1. is intended to cover the situation where a networking capability (i.e. routable protocols) may be used to remotely access and/or control a Critical Cyber Asset in an inappropriate or unauthorized manner. A better way of defining the capability that may allow this to occur would be something like the following:

"R.2.1. The Cyber Asset that can be accessed by unauthorized personnel, either inside or outside the controlled environment, that then may be manipulated, controlled, or otherwise utilized to remotely access and/or control any Critical Cyber Asset in an inappropriate or unauthorized manner."

This definition would then cover the use of a routable protocol or any other means that may be used - with or without a routable protocol – to inappropriately access and/or control a Critical Cyber Asset. For example, this would cover the use of a wireless connection mechanism that could be used to provide inappropriate access to a Critical Cyber Asset by unauthorized personnel outside the protected perimeter of the Critical Cyber Asset. In this case there would be no need for a routable protocol to allow the inappropriate and/or unauthorized access.

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.

R2 & R3 -- These requirements to categorize information and classify/control relative to sensitivity appear to be new requirements over and above the urgent action 1200 standard. These requirements are projected to require significant effort to implement and maintain such a document control system. However, the implementation plan requires Balancing Authorities to be Audibly Compliant by 1st QTR 2006. We would request that compliance for these requirements be changed to Substantially Compliant

R2.2 - Clarification requested - Should categorizing information be based on various categories of "unauthorized personnel" that information may be disclosed? Please expand upon "relative sensitivity of information" that should not be disclosed; is this that information should be labeled "Classified", "Secret", "Top Secret", etc? Can the Drafting Team recommend an example system or process to use as a guiding reference?

R4 - Clarification requested - Does "software patches/changes" also include database changes such as adding new records or defining new tables?

This requirement to establish a governance process appears to be new requirements over and above the urgent action 1200 standard. These requirements are projected to require significant effort to establish a documented process. However, the implementation plan requires Balancing Authorities & Reliability Coordinators to be Audibly Compliant by 1st QTR 2006. We would request that compliance for these requirements be changed to Substantially Compliant

R5.1 - Clarification requested - Does this requirement include documenting access authorizations to substation IED's (if the IED is located in a Critical Asset such as blackstart substation) ? What level of documentation is required, is this a list of named individuals? Pursuant to CIP-004, R4 would these individuals be required to complete background checks or personnel risk assessments?

R-5 B Do the change management and testing requirements apply to all application software changes no mater how small. For example if an alarm set point is changed, one field in one record, does that have to be tested in a non production environment. How big would an application software chance need to be to trigger the testing requirements..

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.

I do not recommend we specify the elements of a BI in the standard, rather let each entity determine what elements will be checked based on the risk.

The criminal history check should cover a 5 year period. This is consistent with the length of time covered by the update requirements and will ensure no gaps once the initial BI is complete.

M4.4 - For identity verification and background checks, does this apply to 3rd party vendor support personnel when granting access or can this be handled through contractual wording with the vendor that they perform these verifications?

M4.1 - Clarification requested - In maintaining list of authorized personnel, is it required to list personnel that have "READ ONLY" access rights? Would this apply to IED's located in critical asset substations?

M4.4 - Clarification requested - Standard states that Entity shall conduct personnel risk assessment process for all personnel "prior" to being granted authorized access to Critical Cyber Assets… How do you handle existing employees running the system which have not had assessments in last 7 years? Suggest amending to state "...for newly hired employees or for transferring employees which require access to Critical Cyber Assets."

COMPLIANCE section 2.1.2 - Clarification requested - Statement "access control list not updated within 24 hours…" Is this referring to actual revoking of the electronic access right or does this include the paperwork must be updated as well?

Removal from access control list for external physical and external cyber access within 24 hours is feasible. Removal from all internal access control lists, all accounts on all assets within 24 hours, is not feasible.

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.

R3 - Standard should not be dictating a specific technical approach to disable dial-up modems using SCADA. This approach has the potential to add burden and distractions to transmission dispatcher duties.

R5 – Clarification needed - "detecting unauthorized access (intrusions), and attempts at unauthorized access to the electronic perimeter(s) and Critical Cyber Assets within…24/7." – use of native security logs at the host level are somewhat limited in their ability to accomplish this task – the way this reads now looks like we would need HIDS or similar technology to manage this at the asset level. Is that the intent of this requirement?

Clarification needed - Monitoring Electronic Access Control – to perform this on the scale need to meet the intent of this standard as it is written today this would require a team of highly skilled folks, using very sophisticated/costly technology and would require a significant capitol investment in network and host intrusion prevention sensors. Is that the intent of this requirement?

R6 - Eliminate the 90 calendar day review for configuration and process reviews. This should be conducted annually or upon changes to the configuration.

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.

The requirements specify physical access controls at every access point to the perimeter which can be accomplished via special locks with non-reproducible keys, which at a substation should be adequate. 24/7 monitoring to detect unauthorized entry, CCTV, alarm systems, computerized logging and procedures for manual logging access to facilities is currently not in place and not recommended based on our ability to recover, reroute, or use redundant assets. These measures may be appropriate for balancing authorities and reliability coordinators, but are excessive for transmission and generation assets. If minimum physical security standards are to be specified, a graded approach should be used based on the criticality of the asset and other factors which may mitigate the impact of access to the asset or asset loss.

M4 - "implement one or more of the following…" – this measure could drive network bandwidth requirements that may result in currently unplanned upgrades.

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.

R1 - Requiring security test procedures on a non-production environment is not practical for many installed systems. This needs to be revised to state, "when possible". Also, if a 3rd party vendor has a similar non-production environment, can the testing be performed by the vendor and a certificate of conformance be acceptable?

R3.3 Generic Account Management – unattended. Unattended access should be controlled by fob or other electronic measures in addition to key/card access control.

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.

M2 - doesn't appear to match the section. It references requirements in another standard.

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.

R5... This requirement references CIP-004-1; each standard should be self contained and not include references to other standards. Such cross-references embedded within other sections can lead to conflicts as individual standards may be at different versions or various approval stages.

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.

Many stakeholders within Progress Energy feel this implementation plan is too aggressive in general. Rightfully so the new standards have an increased scope so that when properly implemented they will afford increased reliability and security of all of our critical cyber assets. We are fully on board with this direction but fell we all need more time to implement properly. Overall, we are struggling with doing the right thing from a safety, reliabiliy and security prespective to name a few and balancing that with other business drivers like missing the 2005 budget cycle, increased personnel requirements, and proper analysis of the impact of these initiatives to ongoing operations.

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:	Lee Matuszczak	
Organization:	U S Bureau of Reclamation	
Telephone:	303-445-3718	
Email:	lmatuszczak@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.

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.

Comments based on 1/17/2005 Draft:

The definition of a Cyber Security Incident is difficult to clearly understand. As written, the definition may result in excessive data collection and unnecessary burdening of reporting offices. Consider revising the definition to address incidents as cyber-related events which (1) violate a law or policy, (2) contribute to (1), and/or (3) directly jepordize assets (personnel, infrastructure, and information). Efforts should be made to exclude cyber events such as "Internet noise" (port scans and pings) isolated inconsequential virus outbreaks, scheduled outages, support equipment failures and other events from incident reporting requirements.

The definition for Electronic Security Perimeter, while addressing the perimeter boundary, does not address the level of control (or "policy") within the perimeter that would normally establish a security baseline within the controlled area.

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.

Comments based on 1/17/2005 Draft

Do not agree with the assertion that critical cyber assets are tied to a particular entity's circumstances. Critical cyber assets are tied to the control of, stability of, protection of, and monitoring of critical non-cyber assets. Such non-cyber assets need to be identified first from the standpoint of overall "power grid" significance. Failure to examine and identify critical non-cyber assets at a higher level will lead to excessive protection of less significant but "business-essential" systems by entities. While their protection may be important to the business, they are not the subject of this standard.

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.

Comments based on 1/17/2005

R1.5 through R1.11 - Is it appropriate that critical non-cyber asset identification, included in this list, should fall under this standard? It would appear that NERC should address non-IT critical infrastructure under a separate identification and protection standard and then supplement that standard with the cyber security standard.

R1.11 - Is it appropriate for entities to conduct these risk-based assessments in isolation? To be effective, such assessments may be more useful if addressed from the perspective of the NERC Region or from from the standpoint of their significance to the overall "power grid". Failure to examine and identify critical non-cyber assets at a Regional or Grid level may lead to identification and excessive protection of less significant but "entity business-essential" systems by the entities. While the protection of these assets may be important to the individual entity, they are not the subject of this standard and will divert resources from higher priority and potentially more important assets.

C. Measures M3. - References to requirements R2 and R3 are included in this section for which no content appears to be present

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.

Comments based on 1/17/2005 Draft

Overall - Consider combining CIP-003-1 with CIP-007-1. Both standards discuss security management and management controls.

Numbering errors lend confusion to the requirements in this standard. Multiple occurances of R3, R4, and R5 are noted.

R1. - The use of the term "bulk electric system" may be more applicable to all situations if changed to "critical non-cyber assets". This term will need to be defined in terms of some criteria, however (e.g., CIP-002-1 R1.2 through R1.11.)

D. Compliance 1.3.4 - It is unclear what this item is requesting "Documented review results of this standard and mitigation strategies for the information security program." Certainly it is possible to maintain records and documents associated with reviews, but "review results of this standard?"

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.

Comments based on 1/17/2005 Draft

R2. - The second sentence should be revised to delete the reference to personnel "having authorized access to Critical Cyber Assets." All personnel, regardless of access, should be provided training regarding the protection of critical assets.

M2.3 - Revise to read "The proper control and release of critical cyber asset information." Further, consideration should be given to creating an information protection standard wherein the safeguarding of electronic, stored, written, transcribed, broadcast, and other forms of information is addressed. This would not just include cyber-related information, but information about all critical assets, including personnel.

M4.4 - The second sentence includes additional requirements (identity verification and 7 year criminal check) that may be excessive. Most federal investigations utilize a 5-year criminal check, even for Secret clearance investigations. This requirement should be reconsidered.

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.

Comments based on 1/17/2005 Draft:

R1. - Consider including the first sentence of this requirement in the definition for "electronic security perimeter."

R1. - The sentence beginning, "Access points to the …" is unclear. Consider revising to clarify or cite a representative example to illustrate.

R3. - Please reconsider the practicality of this requirement with respect to remotely-located facilities, particularly under adverse weather conditions. Other cyber security control alternatives may be preferred.

R4.3 - Provide a sample banner. More importantly, indicate information that should NOT be included on a log-in banner (e.g., name of system, name of entity, anything indicating importance of system).

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.

Comments based on 1/17/2005 Draft:

Purpose: - It is very important to limit requirements addressed in this section to defined Critical Cyber Assets. Its impact on non-cyber critical assets would be significant.

R3. - This requirement may be impractical for a remotely-located outdoor-enclosure-mounted remote terminal unit. It may be practical to detect entry into the enclosure via a door-mounted alarm, but the installation of logging equipment (assumed to be a means of identifying the individual gaining access) may be costly and difficult to support. Consider alternatives or a relaxed requirement.

R5. - This requirement can only be addressed to a certain assurance level. It should be acknowledged that it is not and cannot be made foolproof.

M4. - There is no discussion throughout this standard of appropriate or recommended response measures. Monitoring will be ineffective if no response measures are established and exercised.

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.

Comments based on 1/17/2005 Draft:

General: This standard appears to be discussing both required baseline cyber controls and foundational management practices. As presently titled it overlaps coverage provided by CIP-003-1. Consider combining it with that standard.

R1. - There is no clear discussion of the relationship between Security Tests conducted under these requirements and those in support of Acceptance Testing and Commissioning Testing. Further, it is unclear whether any sort of precautions should be in place with respect to testing production-

level systems. Consideration should be given to NOT perfoming security tests on Critical Cyber Assets that are on line and operational against critical non-cyber assets.

R3. - Consider rewording first sentence to clarify "…to provide for proper user identification and access authentication, the support of user activity audit trails, and to minimize the risk of unauthorized system resource access." This will automatically address the logging of unauthorized users, including those using compromised passwords.

R3.1. - Although they are not typically supported on legacy systems, complex 8-character passwords are readily supported on most modern systems and should be the target password security control. Consider revising the 6-character requirement.

R3.4. - The requirement for semi-annual reviews is a fairly weak control. Consider revising this for all access reviews of critical assets to monthly.

R3.5. - How often should such reviews be conducted? Once per month for physical access? How would the entity necessarily know for cyber-related access unless the

R4.1. - Consider revising the wording: "… unnecessary and excessive patching." to read "unnecessary and disruptive or potentially dangerous patching."

R4.3. - If installation of a patch is not possible, a compensating (mitigating?) measure is only necessary if the system is vulnerable to a threat agent able to exploit the vulnerability. This is aligned with proper risk-management processes. If there is no exposure, correction of a vulnerability is unnecessary.

R5.1. - It is unclear what "Integrity Software" is. Is this addressing the deployment of anti-virus / anti-spam software, or is a more active IPS-like product being suggested? Alternatively, is this requirement addressing a TripWire / file integrity product?

R5.2. - The upgrading and review of security software should be covered under a general configuration and change management process, just as all other critical cyber asset software is covered.

R5.4. - Is this a practical requirement in situations where write-once, read-many media is being employed to distribute patches? Please reconsider the practicality of this requirement.

R7.1. - This is a good idea, but it is unclear what the retention window should be. Should logs from ten days before and after the incident be retained for 3 years? It might be better to support a requirement based on the initial analysis of the event and then require that records associated with that analysis be retained for an extended period.

R11. - Provide the minimum distance that the hardened backup site must be from the critical cyber asset. Perhaps 1 mile?

R11. - Why is the testing of backup and recovery materials at an unattended site prohibitied? Perhaps the rationale should be explained.

M3. - Include Configuration Management as an additional measure under this section. It was addressed in CIP-003-1, but is probably more appropriate here.

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.

Comments based on 1/17/2005 Draft:

R1. - There is no discussion of testing or exercises throughout the standard. Perhaps this should be considered as a means of validating response plans.

R4. - The last word in this requirement is "intermediary." It is unclear what an intermediary is, what their role is and if intermediaries must be identified and authorized to prevent false reporting.

M1. - Physical incident response actions are discussed in this measure. It is unclear, however, how far this standard should attempt to go into the physical security and operational incident arena. This should probably be defined. What is a physical security incident? What is an operational incident? How do these incidents relate to cyber security incidents and who has authority and responsibility under incident conditions?

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.

Comments based on 1/17/2005 Draft:

R2 - Does NERC want to establish some baselines for contingency types to be addressed in test plans? Such events as site fires, extended loss of power, extended loss of access, loss of key staff, site destruction, armed takeover could be considered.

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.

Comments based on 1/17/2005 Draft:

No specific comments, but implementation, if accelerated too quickly, may result in poor implementation practices and improperly vetted procedures. In some instances, this could lead to counter-productive actions in times of crisis. All plans and procedures should be afforded adequate time for development, vetting and testing before penalty-based audits are started.

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:	**Scott R Mix**		
Organization:	**KEMA**		
Telephone:	**215-997-4500 x 223**		
Email:	**scott.mix@kema.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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Replace the 3rd paragraph in the Purpose section to be:

> It is recognized that not all assets are critical, and that some assets may only be critical to a limited portion of a company's system, or have limited criticality to the Bulk Electric System. In order to bound the scope of the Cyber Security Standards to those who's loss or compromise can cause widespread or cascading outages, the Critical Assets and Critical Cyber Assets subject to these Cyber Security Standards shall be identified through the application of an appropriate risk-based assessment procedure, that focuses the analysis of the impact on the operation of the interconnected bulk electric system as a result of the loss or compromise of the asset.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Now that the Cyber Security Standards have been split up and reorganized, the titles need to be structured so they stand on their own. Change the title of this standard to "Identification of Critical Cyber Assets".

There should be an obvious mapping between the Requirements and the Measures, i.e., Measure M1 should measure Requirement R1. If additional Requirements or Measures are required, they should be sub-requirements or sub-measures as appropriate. Ensure that there are no requirements in Measures and no measures in Requirements. Required timeframes for review should be specified in Requirements (not Measures). Similarly, the compliance requirements must correspond to the measures (as required in the NERC Reliability Standards Process Manual).

Requirement R1: Add the following: "The risk assessment process, and the lists of Critical Assets and Critical Cyber Assets must be reviewed annually. The lists must be updated within 30 days of the addition of, removal of or modification to any Critical Asset or Critical Cyber Asset."

Requirement R4 should read:

> A member of senior management must annually certify that an analysis of the responsible entities' assets has performed to determine what assets are Critical. If the analysis determines that either no Assets are Critical (as defined for this standard), or no Critical Assets contain Critical Cyber Assets per this standard, the member of senior management must certify that fact. If the analysis determines that the responsible entity has Critical Assets and Critical Cyber Assets per this standard, the member of senior management must approve the list.

During the web cast, a question was raised concerning "read-only terminals". It needs to be clear in the requirements and FAQ that any "computer" that is network connected (i.e., on the TCP/IP network) to the control system needs to be protected regardless of the application function used on that computer. This includes PC's and X-terminals that are administratively prohibited from entering data or controls into the control system, but are communicating with the control system. Monitors that are "slaved" to other computers via an RGB or equivalent connection are exempt, since they are not part of the communications (TCP/IP) network, but the computer driving the "controlling" monitor is subject to the requirements of standard CIP-002-1.

The measures should be re-written as being measurable. For example, M1 should be "The responsible entity shall demonstrate that it has maintained a list of Critical Assets as defined in R1."

Measure M5 and M6 should discuss time frames (that are specified in a requirement), i.e., M5 should read "The Responsible entity shall demonstrate that the list of Critical Assets required in R1 has been approved by a senior manager no more than one year after the previous approval, and within one year prior to the audit."

FAQ CIP-002-1.Q4 refers to NERC standards in development 200 and 600, which have been adopted by industry and re-named. In addition, out of date definitions are included in the response. Definitions appearing in the NERC glossary should not appear in this FAQ. Definitions not appearing in the NERC glossary should be moved to the Standard text for discussion and adoption by industry.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

FAQ CIP-002-1.Q7 refers to Token Ring as a layer 3 protocol. IEEE 802.5, which is the international standard for Token Ring, indicates that it is a layer 2 protocol. The reference to "DNP 3.0 (network mode only)" is confusing, and could be interpreted as including all DNP 3.0 traffic. DNP 3.0 is not a layer 3 protocol, nor is it a routing protocol. Replace the term with "DNP 3.0 running over IP" to clarify and limit the applicability.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

There should be an obvious mapping between the Requirements and the Measures, i.e., Measure M1 should measure Requirement R1. If additional Requirements or Measures are required, they should be sub-requirements or sub-measures as appropriate. Ensure that there are no requirements in Measures and no measures in Requirements. Required timeframes for review should be specified in Requirements (not Measures). Similarly, the compliance requirements must correspond to the measures (as required in the NERC Reliability Standards Process Manual).

Requirement R1. Add the following sentence: "This cyber security policy should address the special requirements and needs of cyber assets as defined in Standard CIP-002-1."

Requirement R1. Add the following: "This policy shall be approved and reviewed as often as determined by the responsible entity, with a period not to exceed 3 years. Any deviations or exemptions from this policy must be reviewed and approved annually by senior management to ensure the exemptions or deviations are still required and valid."

Requirement R2: Add the following: ", and review the program and assess it's effectiveness annually."

Requirement R5.1 should be split into two requirements. The first requirement should specify who is responsible to authorize individuals to access Critical Cyber Assets. The second requirement should be to maintain documentation of who is authorized to have access to the Critical Cyber Assets.

Measure M15: add "affiliation (for vendors and contractors)" after "title"

FAQ CIP-003-1.Q1 should indicate that the special needs and considerations of Cyber Security Policy for Critical Cyber Assets covered by these standards needs to be called out and specifically addressed if it is to be included in a larger corporate policy set.

In FAQ CIP-003-1.Q3, the lowest level of US Government classification is "Confidential", not "Classified".

FQA CIP-003-1.Qnew: Does the list of personnel authorized to access or approve access to Critical Cyber Assets include vendors, contractors and consultants?

In response to a question in Draft 1, it was indicated that reference to the ISA SP99 standard would be included in the FAQ portion of the standard. Please include this reference.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Now that the Cyber Security Standards have been split up and reorganized, the titles need to be structured so they stand on their own. Change the title of this standard to "Critical Cyber Asset Personnel and Training".

The compliance requirements must correspond to the measures (as required in the NERC Reliability Standards Process Manual).

Requirement R1. Insert the word "quarterly" before the word "on-going".

Requirement R1. Insert "including contactors and service vendors" after "personnel"

Requirement R1. Add the following phrase to the end of the requirement: "as the practices apply to the Critical Cyber Assets covered by this standard"

Requirement R2. Insert "including contactors and service vendors" after "personnel"

Requirement R3: replace "background screening" with "the results of the personnel risk assessment process"

Requirement R3. Insert "including contactors and service vendors" after "personnel"

Measure M2. Change to read: "Training – the Responsible Entity shall develop and maintain a company-specific cyber security training program, and review it's contents annually, that includes …"

Measure M2.1: Add the following phrase: "as developed for the Critical Cyber Assets covered by this standard"

Measure M4.1: There is no requirement in standard CIP-004-1 relating to maintenance of a list of personnel and their access rights. This should be a requirement in standard CIP-003-1.

Measure M4.4: Change the first sentence to read, "The Responsible Entity shall conduct a documented company personnel risk assessment process of all personnel covered by this standard prior to being authorized access …"

Measure M4.6 replace "conduct update screenings" with "re-evaluate personnel risk assessment results"

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Now that the Cyber Security Standards have been split up and reorganized, the titles need to be structured so they stand on their own. Change the title of this standard to "Electronic Security of Critical Cyber Assets".

The compliance requirements must correspond to the measures (as required in the NERC Reliability Standards Process Manual).

Requirement R2 is duplicated in CIP-007-1 as requirement R9. Since standard CIP-005-1 deals with the electronic perimeter, the requirement should be deleted from standard CIP-005-1 (and remain in standard CIP-007-1). (If the requirement stays in CIP-005-1, please refer to my comment concerning CIP-007-1 R9.)

Requirement R3: Replace requirement with:

R3: The Responsible Entity shall Secure dial-up modem connections.
R3.1: In unattended facilities, where remote activation of dial-up connectivity via SCADA-activated relays from the security or control center is technically feasible, the dial-up equipment shall be physically deactivated when not in approved use and remotely activated upon approval of activation.
R3.2: In all other cases, the Responsible Entity shall normally disable unneeded dial-up connectivity, and implement procedural or technical measures to enable the dial-up connectivity after ensuring the authenticity and authorization of the accessing user, device and/or application.

Measure M1. Change the first sentence to read "…all interconnected Cyber Assets (Critical and otherwise) within the security perimeter, …"

Measure M2. See comment concerning Requirement R2.

Measures M4.2.1, M4.2.3, move to standard CIP-003-1. These are procedural and belong in the Management Control section, not the technical Electronic Security section.

FAQ CIP-005-1.Q1 should be augmented to include one RTU with an electronic security perimeter surrounding it, with an explanatory note indicating that it communicates with the central site using a routable protocol.

In FAQ CIP-005-1.Q5, the sentence beginning "A strong authentication scheme is usually defined as one" appears to be missing some words.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Now that the Cyber Security Standards have been split up and reorganized, the titles need to be structured so they stand on their own. Change the title of this standard to "Physical Security of Critical Cyber Assets".

There should be an obvious mapping between the Requirements and the Measures, i.e., Measure M1 should measure Requirement R1. If additional Requirements or Measures are required, they should be sub-requirements or sub-measures as appropriate. Similarly, the compliance requirements must correspond to the measures (as required in the NERC Reliability Standards Process Manual).

Requirement R3 and R4: Please comment on the functional distinction between these requirements, and why they are specified separately.

Measures (general) There appears to be a lot of "implementation detail" included in the measures section. According to the NERC Reliability Standards Process Manual, measures are used to "assess performance and outcomes for determining compliance with the requirements. Specifying that a Responsible entity "shall implement one of the following …" sounds like a requirement, not a measure.

FAQ CIP-006-1.Q1 still refers to a "four-wall" boundary.

FAQ CIP-006-1.Q11 is a duplicate of FAQ CIP-006-1.Q10.

FAQ CIP-006-1.Q13 should be augmented to indicate that a fence provides only a "four-wall" boundary, not a "six-wall" boundary as required by the standard.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

There should be an obvious mapping between the Requirements and the Measures, i.e., Measure M1 should measure Requirement R1. If additional Requirements or Measures are required, they should be sub-requirements or sub-measures as appropriate. Similarly, the compliance requirements must correspond to the measures (as required in the NERC Reliability Standards Process Manual).

Requirement R1: Insert the following sentence between the existing first and second sentences: "These test procedures shall take into consideration the special needs and requirements of the Critical Cyber Assets covered by this standard."

Requirement R1: The requirement to test installation of security patches "for known security vulnerabilities" as discussed in the 2/2/05 web cast is excessive. On the other hand, it may be reasonable to require testing for security vulnerabilities when installing new application code to ensure that the new application does not introduce vulnerability into the system. Is a testing certificate fro the application developer sufficient? Please clarify

Requirement R3.1: add the following phrase to the end of the first sentence: ", subject to the technical limitations of the secured Critical Cyber Asset"

Requirement R6.1.2. Split into two requirements:
R6.1.2 Scanning of functionally identical test systems for open ports/services
R6.1.3 Scanning for modems

Requirement R9. Add the following sentence: "In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall use and document (a) compensating measure(s)."

Measure M8. Add the following sentence: "If unused ports and services cannot be disabled due to technical limitations of the device, documentation of other compensating measures must be provided."

In FAQ CIP-007-1.Q8, please comment on how a "security patch" is considered a "significant change" requiring testing, while a "Version *revision*" is not a "significant change" and therefore may not require testing.

FAQ CIP-007-1.Qnew Why is does requirements R6.1.2 require scanning of "functionally identical test systems", not the actual productions systems?
Answer: Scanning of production systems by vulnerability testing tools and port scanners have caused operational problems, including the complete loss of function on the systems being scanned. Scanning for vulnerabilities is important, but it cannot be done at the expense of a functioning system. The scanning of "functionally identical test systems" provides for the testing and identification of the vulnerabilities, while not impacting the production environment.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

FAQ CIP-007-1.Qnew: What is meant by “Integrity Software”?

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

There should be an obvious mapping between the Requirements and the Measures, i.e., Measure M1 should measure Requirement R1. If additional Requirements or Measures are required, they should be sub-requirements or sub-measures as appropriate. Similarly, the compliance requirements must correspond to the measures (as required in the NERC Reliability Standards Process Manual).

Measure M.2 should move to standard CIP-007-1. There is no log retention requirement in standard CIP-008-1.

In FAQ CIP-008-1.Q2, please add a clause indicating that the IAW program is voluntary from a U. S. Federal Government point of view based on the US Federal Government's ability to protect the information from disclosure under FOIA requirements, but required from a private industry point of view through this NERC standard.

FAQ-008-1.Qnew: Please describe the relationship between standard CIP-008-1 and standard CIP-001-1.

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

Now that the Cyber Security Standards have been split up and reorganized, the titles need to be structured so they stand on their own. Change the title of this standard to "Recovery Plans for Critical Cyber Assets".

Requirement R1: add the following sentence: "The plan shall address recovery from physical disruption and damage, as well as cyber disruption and damage to the Critical Cyber Assets."

Draft 2 Cyber Security Standards — Comment Form

Please Enter All Comments in Simple Text Format.

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.

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: N/A		
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: Florida Power and Light

Lead Contact: **Pedro Modia**

Contact Organization: **Florida Power and Light**

Contact Segment: **2**

Contact Telephone: **305-442-5246**

Contact Email: **pedro_modia@fpl.com**

Additional Member Name	Additional Member Organization	Region*	Segment*
Joel De Granda	**Florida Power and Light**	**FRCC**	**2**
Sergio Guzman	**Florida Power and Light**	**FRCC**	**2**
Ray Falcon	**Florida Power and Light**	**FRCC**	**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.

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.

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.

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.

The standard does not clearly indicate wheather support systems such as cooling, UPS, generators, etc. that are outside the physical security perimeter should be considered critical assets. If these systems are considered critical assets, then they should be included in the physical security perimeter. The standard must define the outermost boundery of the physical perimeter.

Is section 1.3.3 complete, inasmuch as the sentence ends in the word and?

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.

R4.1. It is not reasonable to authorize and document test results for routine maintenance changes. For example, Windows updates follow a fixed and repeatable procedure. Standard update procedures should not require formal authorization and documentation steps. Alternate wording could be

Responsible Entities shall identify the controls for testing and assessment of new or replacement systems. 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 prior to the system being promoted to operate in a production environment. Routine software patches/changes are controlled and document via procedures. Formal approval is done only for initial implementation of the procedure.

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.

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.

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.

M5. How does this measure address piggybacking?

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.

R2. The intent of this statement is not clear. Please provide clarification beginning at:

The Responsible Entity shall conduct security test procedures for Critical Cyber Assets at the unattended facility on a controlled non-production environment located at another secure attended facility.

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.

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.

The word – major, should be clearly defined as it is subject to interpretation.

R3. The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.

Does M4 speak to the attendance to the training or the drill?

M4. The Responsible Entity shall conduct drills at least every three (3) years and keep attendance records to its Recovery Plan(s) training

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.

For GOP, the schedule is too aggressive. We recommend at least 12 months from the time the standard is approved to become "Significantly Compliant" and 24 months from the time the standard is approved to become “Auditably Compliant". This will allow time for a budget cycle and planning and implementation time.

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**
☐ **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: Southern Company, Transmission, Operations, Planning and EMS Divisions

Lead Contact: **Marc Butts**

Contact Organization: **Southern Company**

Contact Segment: **1**

Contact Telephone: **205-257-4839**

Contact Email: **mmbutts@southernco.com**

Additional Member Name	Additional Member Organization	Region*	Segment*
Jay Cribb	**Southern Company Services**	**SERC**	**1**
Mike Sanders	**Southern Company Services**	**SERC**	**1**
Tom Park	**Southern Company Services**	**SERC**	**1**
Mike Oatts	**Southern Company Services**	**SERC**	**1**
Bonnie Parker	**Southern Company Services**	**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.

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.

Pg 2, Regarding Cyber Security Incident definition suspicious event: Isn't this too broad? How will we decide or know an event was an attempt to disrupt if it's only suspicious?

Since there is no place for general comments, allow us to add them here.

The standards seem to be written to reflect a perspective that all Critical Cyber Assets are under the direct control of the Responsible Entity. In some cases, the actual asset involved may be provided by a vendor that fully operates and maintains the asset under an application services agreement or merely provides bug-fix and enhancements services. Although the Responsible Entity using the asset would be responsible for the standard requirements, there are practical limitations to this in a customer vendor relationship (e.g., vendors with multiple customers have variations on procedures and minimum expectations to accommodate these standards). At a minimum, the standard does not clearly, explicitly recognize these situations and how they should be addressed.

These standards rely based on the Definitions on the direct relationship of a Cyber Asset to an identified Critical Asset when identifying a Critical Cyber Asset. It is recognized that most cyber systems that are associated with a critical asset will also be associated with non-critical assets (and thus become classified as Critical Cyber Assets. The definition of Critical Cyber Asset should not, however, ignore the fact that a cyber asset associated with only non-critical assets may effectively become a critical asset if its security compromise results in sufficient non-critical asset problems that, taken in total or cumulatively, result in Critical Asset problems or general grid reliability risk. As an analogy, if a toll-road freeway in a city was deemed a critical asset and the “Easy Pass” system was deemed the critical cyber system associated with it, the freeway would still be impacted by the compromise of the surface-road street light system as many more vehicles entered (and perhaps overloaded) the freeway to avoid malfunctioning street lights and the resulting congestion (and possible resulting accidents).

Although NERC is the sponsor and provider of the IDC, SDX and RCIS which many in the industry consider Critical Cyber Assets due to their direct and indirect influence on grid controls and decisions, it is not listed in the Applicability section of the Standards. Why is NERC not listed as having the standards apply to them? Even if NERC intends to comply, should they not be explicitly listed due to their role in the Cyber Assets just mentioned? If NERC is not held responsible for these applications' security then who should be? The same would be true for a Regional Reliability Council that operates similar systems for their Interconnection.

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.

Pg 4, R2.1, Regarding routable protocol: from the Comments & Responses document (p 446) it is clear that the drafting team wants frame relay included as a routable protocol and that frame relay access devices (FRAD's) therefore would be part of the electronic perimeter. This is a huge deal in that many substations would be added to the perimeter.

In Measure 4 – The term modification should be defined – does the replacement of a keyboard, mouse, or even hard-drive constitute a modification.

In Measure 4 – The term addition should be defined – does the connection of any new hardware inside a security perimeter constitute an addition even if the associated application software system has not been loaded at that point or is it the production use of the new cyber asset that constitutes an addition? This would not normally be an issue except the measure has a timing requirement associated with it that implies the starting of a clock to non-compliance if documentation is not updated.

In Measure 4 – The measurement refers only to modification of a Critical Asset or Critical Cyber Asset. What about the other Cyber Assets in the same Security perimeter per R3? It would seem that they would be subject to the same review and documentation per the risk they pose to the Critical Cyber Assets or why have R3 at all?

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.

R1.1 What is the definition of the "largest single contingency within the Regional Reliability Organization" as it relates to generation and how is it determined?

B.R2 Consider adding a requirement R2.3 that states the cyber asset must be controllable. If the asset uses a routable protocol or dial-up modem for data gathering purposes only, and it is not possible to initiate any change to the device, then it should be out of scope.

C.M3 The first instance of the term "Requirement R3" should be "Requirement R2"

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.

Definitions of Terms – The term Access needs to be defined and used more precisely in the associated text of this standard. Access can mean admission to physical locations, contact with information, ability to view/modify software code and/or data, authorization to log-in and execute a program, etc. The applicable access meanings should be captured more explicitly in the Definitions, and appropriate adjectives reflecting that meaning used in the text of the requirements and measures.

Definitions of Terms – The term Logical to reflect Electronic Security in the Purpose of CIP-005-1 is used in this standards R5.1 but never defined in this standard.

Requirement 2 of this standard calls for an information protection program as a control for sensitive information concerning critical cyber assets. However, several measures and non-compliance levels go off into very vague subtleties. For example, consider combining measures M5, M6, and M8 into one simple measure that calls for an annual assessment of the information protection control to insure its effectiveness. It is a source of confusion to have 3 measures around this, one calling for an annual review (M5), one calling for an annual assessment (M6), and one calling for an annual -make sure the procedures comply- (M8). Along these same lines, under Level 1 Non-Compliance consider combining 2.1.4 and 2.1.5.

Pg 3 of 8, R2.1; Regarding - could impact the reliability - This is very broad and subject to interpretation.

Pg 4, Re R4.1.: How will companies comply with this, especially for vendor supplied patches or upgrades? There is no measure associated with this requirement that the approving authority verifies a system meets minimum security configuration standards. Was this omission intentional?

In R5 – What information about a Critical Cyber Asset is this requirement referring to? Is it the information related to R2.1?

M13.2 Change -all the Responsible Entity follows- to -all the Responsible Entities follow-, or just drop the word all.

2.1.1 (Level 1 Non-Compliance) All measures must have a reasonable lower bound and not be left open-ended such as -less than 30 calendar days-. In the event of a sudden absence of the senior management official (death, severance, etc) the standard should allow for an appropriate amount of time to appoint a replacement and complete the documentation. Suggested measure for L1 non-compliance is going more than 14 days but less than 1 month in aggregate during the year without a SMO named.

2.4.5 (Level 4 Non-Compliance) There is no way to objectively measure and audit against the statement - Executive management has not been engaged in the cyber security program. These levels must be defined in such a way that an outside audit team can come in and objectively assess through observance of documentation or other factual data an appropriate non-compliance level. Delete this from L4.

In Levels of Compliance, Level 3, items 2.3.3 and 2.3.4, the Roles and Controls that are to be defined/identified for compliance were not enumerated in the data that was to be retained per the Data Retention section so how would testing of compliance occur if an entity failed to retain this needed data?

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.

Purpose – The term access is used but not defined. Is it any type access?

In R1 – The term -subject to this standard- is used. One would assume all employees of an applicable Responsible Entity would be subject to the standard but only those with some type of access to a Critical Cyber Access would actually require reinforcement of sound security practices. If the latter group is the case, say so. If the intent is all employees at a responsible entity then say that.

Under Level 3 Non-Compliance, move 2.3.3 -A personnel risk assessment program does not exist- to a Level 4 Non-Compliance. It can be argued that most of the risk is from insiders, so doing personnel risk assessments is at least at vital as the other aspects mentioned in Level 4.

Under the Levels of Non-Compliance, levels 2.1.3, 2.1.5, and 2.2.5 are too subjective in nature and need to be tightened down to more discrete and auditable measures instead of -not consistently applied- or -not properly documented-.

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.

Requirements R1 In the last sentence, where it is explaining about non-critical cyber assets within the electronic perimeter and it states -these non-Critical Cyber Assets must comply with the requirements of this standard-, please clarify the word -this-. It is unclear as to whether it is implying that they must comply with CIP-005 only or if this is a holdover from when all the standards were under the one 1300 banner.

Pg 4, R2, Regarding disabling unused network ports/services: We are very dependent on our vendors for this info and they have thus far refused to provide this kind of detail free of charge. They want to do a -security assessment- and then give recommendations. We will have to pay for this and it will probably not be cheap. Some estimates were in the low tens of thousands of dollars.

Pg 5, R5, Regarding monitoring electronic access control: See CIP-002-1 above; if FRAD's in substations are subject to this, how would companies comply with this?

In Measure 5.2 – The essence of this measure would seem to be to maintain documents to demonstrate the concept of -operational effectiveness- of the tools and procedures. Unless this concept is defined and utilized, these standards may be ineffective. Unless corroborating evidence such as detective controls is used to identify circumvention of -normal- access, logs can provide insufficient evidence of operational effectiveness because it may log only those instances when something did happen like it was suppose to and not those instances where it did not.

Measure M5.3 Consider changing -review access records for authorized access against access control rights- to -review access records for Unauthorized access against access control rights-. It is not a productive use of time to have personnel reviewing records for each and every cyber asset for authorized access. That time is better spent reviewing unauthorized access (failed logon attempts, etc) looking for suspicious -knocking on the door- type activity. Reviewing voluminous reports of legitimate access should not be a requirement.

2.1.2 (Level 1 Non-Compliance) All measures must have a reasonable lower bound and not be left open-ended. This one effectively generates non-compliance for ANY gap less than 24 hrs. It is suggested that this measure be made parallel with its physical security counterpart in CIP-006 which states -aggregate interruptions in system availability over a calendar year exist for more than 7 days but less than 1 month-. This at least allows you time to institute your backup monitoring plans should your primary fail without generating a non-compliance.

2.3 (Level 3 Non-Compliance) In 2.3.2, a non-compliance can be generated from -a record of regular audits does not exist-, but the standard only requires that all ports not used for -normal or emergency operations- be disabled. Measure M2 requires documentation of the required ports and services, but nowhere is there a requirement or measure for a regular audit.

2.3 (Level 3 Non-compliance) 2.3.3.2 needs to be deleted or clarified greatly. -Required documents exist, but records for some transactions are missing- is too vague. For example, exactly what transactions are required? How will the entity or an outside audit team know any are missing?

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.

Purpose – Define - six-wall boundary.

Pg 4, R3, Regarding monitoring physical access control, what is meant by -generally accepted industry or government risk assessment procedure-? Monitoring physical access 24/7 will be very difficult for the many locations large companies have. Again, if substations w/ FRAD's are included, this would have far-reaching implications and tremendous costs.

Pg 4, M3; Regarding special locks: could you please define what a Man-trap might be?

Pg 5, M5; Regarding monitoring & logging physical access: per above, it sounds like either CCTV or an alarm system of some kind would be required at every substation w/ frame relay communication. While some may have this already, I would guess that many/most do not.

Pg 6, Regarding levels of non-compliance: does -aggregate interruptions- refer to a centralized system, therefore assuming there is one?

Levels of Compliance, Levels 1 and 2 – Are -aggregate interruptions in monitoring system availability- intended to be for a failure a one location or an aggregate of all Critical locations? If all locations, then how can a responsible entity with many Critical locations be held to the same composite (7 days or 1 month) as a responsible entity with only 1 or 2 locations?

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.

There is much duplication between CIP-007 and CIP-003, CIP-005, and CIP-006. Either move the remaining elements from CIP-007 out and delete it or clearly delineate what belongs in it and remove the duplication. Due to the way that compliance results on these standards are reported to NERC, it is important that any one non-compliance issue not cause non-compliances across multiple standards. Entities, regions, and even the entire industry are deemed 'XX% compliant', so to keep those numbers reflecting reality it is imperative that single issues only be measured once to avoid double penalties.

R1 Combine all Testing requirements from this and R4 of CIP-003 under one standard. Regarding -significant changes- and security testing: most companies have traditionally relied on vendors to perform security testing as appropriate. We believe that to self-test and certify all -significant-changes against all known security vulnerabilities for all our systems would be a monumental task. We are trained and staffed for functional and operational testing.

In R1 – This requirement states that -The Responsible Entity shall verify that all changes to Critical Cyber Assets were successfully tested for known security vulnerabilities prior to being rolled into production-. How is this expected to happen for some vulnerability? For example, how would one verify for a known vulnerability to Internet Explorer or to the XP operating system that the fixes provided by Microsoft had indeed been successfully tested by them. As worded the only way the Responsible Entity would be able to verify success would be to try and develop a program to attack the vulnerability. In other words, as worded the responsible entity is required to verify security patches provided by a vendor do indeed fix the vulnerability. This is not practical.

In R3 – The words -end user account- are used in the last sentence but are qualified by the parenthetical statement that implies accounts other than end user (i.e. administrator accounts are not typically referred to as -end user-). Suggest just removing the words -end user-.

R3.3 Covered in CIP-006 under physical security and should not be under generic account mgt

R3.5 The electronic and physical monitoring aspects of CIP-005 and CIP-006 should cover this.

R4 - Pg 5, Regarding security patch management and performing a monthly review of security patches for each asset: What will companies do if/when a vendor announces that an older version (application, OS, etc.) is no longer supported and should no longer be used? Could companies be forced into multiple expensive upgrades?

R4 and M3 mention testing as it relates to security patches. During the NERC webcast, this testing was interpreted to mean that entities must test to insure the patch actually fixes the vulnerability. That is impractical and entities should not be in the business of developing exploit code to test vulnerabilities, nor should they be deemed non-compliant if their scanning engines do not have a signature for said vulnerability (some vulnerabilities cannot be detected via a network scan anyway). The term -testing- can also be interpreted as testing to insure that security patches do not compromise the availability of any critical cyber assets and the testing documentation would show that security patches are not blindly applied to critical cyber assets without first knowing their impact to the environment. This interpretation of -testing- seems more in line with the spirit of CIP-007 and is more reasonable.

R5.1 Delete the confusing phrase -that are connected to a wide-area network, the Internet, or to another device that is connected to a network (e.g., printer)-. Simplify this to the blanket statement -shall use integrity software on all Critical Cyber Assets to prevent, limit, ...- and let R5.3 handle the exceptions where it can't be used. The term -Integrity Software- needs to be defined in the Definitions of this Standard.

R5.2 Since the #1 integrity software tool is antivirus packages, it is unclear why this is requiring a "monthly review of the available integrity software"

R5.4 Unclear what this means

R8 Change Management requirements and measures should be combined and either placed in CIP-003 or in CIP-007 but not spread across both.

R9 Disabling Unused Ports requirements and measures should be combined and either placed in CIP-005 or in CIP-007 but not spread across both.

R10 – The implications of the words -to monitor operating state, utilization and performance, and cyber security events- is going beyond the scope of a Cyber Security Standard particularly the -operating state, utilization and performance- requirements. If the intent is to monitor these parameters for possible intrusion and security compromise through abnormal -fingerprints- in these parameters that makes sense and it should be stated that is the intent. To imply the requirement for general monitoring of these parameters for other reasons such as operational efficiency of the users due to overloaded processors, database capacity, excessive I/O due to defective coding, etc., although good practices for other reason, is beyond the scope of this standard. Perhaps the words at the end could be modified to and issue alarms for specified indications of possible intrusion and or security compromise, as implemented- could be use to be more specific and appropriate.

M2 The sentence beginning "Review access permissions within 24 hours for personnel terminated for cause..." should be deleted as this is covered in CIP-004.

M7.1 Change Mgt controls and Testing Procedures should be measured in CIP-003 or here but not both.

M7.2 Change Mgt controls and Testing Procedures should be measured in CIP-003 or here but not both.

M8 Disabling Unused Ports should be measured in CIP-005 or here, but not both.

M 10.2 – There is no requirement to document recovery procedures for reconstruction and Critical Cyber Asset from the backup data. R11 only requires storing and testing not the documentation. Although a good practice, if its expected to be documented (i.e., staff may know how to do it without documentation) then should that not be also stated in the R11 requirements.

M 10.3 - How would the documentation required verify one is -capable of recovering- from a Critical Cyber Asset failure? Is this implying that tests performed verified this capability then state that the test results should be documented? Be explicit.

In Levels of Compliance, Level 1 and Level 2 - It is stated that -two (and three, respectively) of the specific areas- in documents have not been reviewed or updated. Is this two (or three) things in any one document or in aggregate across all documents in this standard?

In Levels of Compliance, Level 3 - Remove 2.3.9 and 2.3.10 because they are -N/A- and serve no purpose.

Non-Compliance levels 2.3.8, 2.3.9, and 2.3.10 should follow their appropriate requirements and measures if they move to other 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?

☒ 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.

In Definitions – Define expected Recovery Plan content since the standard is not explicit.

In the Purpose – The Purpose needs work. Current words do not reflect the -recovery plan- purpose the standard is trying to address.

In requirements – is there an implied expectation of what an -exercise- or -drill- should entail as used in this document or is it up to the Responsible Entity to define what activities are appropriate for them?

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.

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.

The implementation plan only addresses when entities should be “auditably compliant’ but does not address the introduction of audits, sanctions, or penalties as previous implementation plans have addressed.

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:	Robert C. Webb	
Organization:	Robert C. Webb, PE	
Telephone:	650 839-1683	
Email:	rcw4@ix.netcom.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.

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.

See comments in response to CIP-002-01, Question 3.

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.

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.

I do not believe the majority of NERC's Cyber Security Standards CIP–002–1 through CIP–009–1 are ready to ballot at this time, because they do not adequately address the special considerations necessary when applying the standards to a key segment of our country's critical power infrastructure - generation control systems.

I have examined the draft standards as part of my role in developing technical reports, recommended practices, and standards for manufacturing and control systems security, as a part of the Instrumentation, Systems, and Automation Society's SP99, "Manufacturing and Control System Security" standards committee.

I am the Managing Director of that committee, and a professional engineer with considerable expereince in power plant automation. ISA is interested in consistency with other standards, where appropriate, to preclude end user confusion and an impossible challenge for manufactures of control systems equipment. To that end, we are working with Tom Flowers of your CSSWG to establish a liaison process that would allow such considerations to be addressed earlier in the process. However, you have asked for comments at this time, and we believe these issues need to be addressed now, before approval, for the standard to be effective.

In general, CIP-002-1 through CIP-009-1 do a good job of addressing the key elements of a good security program; the drafting team should be congratulated. However, without specific guidance on how to apply some of the recommendations to legacy generation control systems, the standards could be counter productive. This guidance need not be exhaustive, but can be provided at a high level, with references to additional detailed information. In other words, wholesale application of typical business systems security practices to control systems is not appropriate. SP99 was created to provide guidance on how to apply security to control systems, without adversely affecting their primary function. Substantial guidance has been published by the SP99 committee, and has been available since April of 2004. It should be referenced in the NERC standard.

In addition to the direct impact on generation, generation control systems, if not adequately addressed, become additional "back door" electronic avenues that can compromise the bulk grid that the NERC standards appear to be focused on protecting. The standards should cover such systems, regardless of generator size.

Joe Weiss, a member of ISA's SP99 , and NERC 's CSSWG, has provided specific comments and recommended revisions which address these concerns. Those comments should be responsibly addressed.

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.

See comments in response to CIP-002-01, Question 3.

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.

See comments in response to CIP-002-01, Question 3.

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.

See comments in response to CIP-002-01, Question 3.

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.

See comments in response to CIP-002-01, Question 3.

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.

See comments in response to CIP-002-01, Question 3.

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.

See comments in response to CIP-002-01, Question 3.

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.

See comments in response to CIP-002-01, Question 3.

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.

Basis for Negative Recommendation on NERC CIP-002-01 through CIP-009-01

I do not believe the majority of NERC's Cyber Security Standards CIP–002–1 through CIP–009–1 are ready to ballot at this time, because they do not adequately address the special considerations necessary when applying the standards to a key segment of our country's critical power infrastructure - generation control systems.

I have examined the draft standards as part of my role in developing technical reports, recommended practices, and standards for manufacturing and control systems security, as a part of the Instrumentation, Systems, and Automation Society's SP99, "Manufacturing and Control System Security" standards committee.

I am the Managing Director of that committee, and a professional engineer with considerable expereince in power plant automation. ISA is interested in consistency with other standards, where appropriate, to preclude end user confusion and an impossible challenge for manufactures of control systems equipment. To that end, we are working with Tom Flowers of your CSSWG to establish a liaison process that would allow such considerations to be addressed earlier in the process. However, you have asked for comments at this time, and we believe these issues need to be addressed now, before approval, for the standard to be effective.

In general, CIP-002-1 through CIP-009-1 do a good job of addressing the key elements of a good security program; the drafting team should be congratulated. However, without specific guidance on how to apply some of the recommendations to legacy generation control systems, the standards could be counter productive. This guidance need not be exhaustive, but can be provided at a high level, with references to additional detailed information. In other words, wholesale application of typical business systems security practices to control systems is not appropriate. SP99 was created to provide guidance on how to apply security to control systems, without adversely affecting their primary function. Substantial guidance has been published by the SP99 committee, and has been available since April of 2004. It should be referenced in the NERC standard.

In addition to the direct impact on generation, generation control systems, if not adequately addressed, become additional "back door" electronic avenues that can compromise the bulk grid that the NERC standards appear to be focused on protecting. The standards should cover such systems, regardless of generator size.

Joe Weiss, a member of ISA's SP99, and NERC 's CSSWG, has provided specific comments and recommended revisions which address these concerns. Those comments should be responsibly addressed.

Sincerely,
Robert C. Webb, PE

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 the 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:	**Raymond A'Brial**	
Organization:	**Central Hudson Gas & Electric Corporation (CHGE)**	
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:

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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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 devided 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.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

CHGE feels that there are many incidents that have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>.

We are concerned that "suspicious event" is too broad. We recommend changing the Cyber Security Incident definition to <<Any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.>>

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

YES

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

The CHGE's answer to question 2 is "yes."

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

CHGE strongly believes that CIP-002 is not ready for ballot. We believe it is important that this Standard specify that the Critical Assets to be considered are a subset of the Critical Assets as defined in the Definitions section.

Requirements R1.1.1 to R1.1.9, inclusive, are too prescriptive. This list belongs in a FAQ. We feel that cyber security personnel should not maintain a list of non-cyber equipment. Perhaps the FAQ should include a statement that <<the Responsible Entity should use a cross-functional team or other methods that are appropriate for that organization>>.

We suggest the Purpose be altered to

<<
This standard is intended to ensure that appropriate cyber 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.

With the increased use of standard technologies to connect Control Center computer systems to the bulk electrical systems, corporate business systems, and the internet, separation between the critical assets of the bulk electrical system and untrusted infrastructure has been dramatically reduced. This connectivity requires that the Control Center systems put in place a high level of Cyber Security measures to protect the Control Center and bulk electrical system assets.

Business and operational demands for managing and maintaining 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 Responsible Entities identify and protect Critical Cyber Assets that support the reliable operation of the bulk electric system.

The Critical Cyber Assets are identified by the application of a risk-based assessment procedure on the operation of cyber assets supporting the monitoring and control of the interconnected bulk electric system.
>>

We recommend changing Requirement R4 to <<Member(s) of senior management or designee must approve the list of Critical Assets and the list of Critical Cyber Assets.>>

We recommend changing Measure M5 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Cyber Assets must be maintained.>>

We recommend changing Measure M6 to <<A signed and dated record of the senior management officer's or designee's approval of the list of Critical Cyber Assets must be maintained.>>

Please clarify the performance reset period in Compliance 1.2. What is being reset? Why is it being reset?

Recommend that Compliance 1.2 change from 30 days back to the 90 days specified in 1200.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

CHGE feels CIP-003 needs a little more work before it is ready for ballot. This answer assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot, for more information see the response to the previous question.

We do not agree with C.M1. When a signed Compliance Submittal is sent to the Compliance Monitor, that organization implicity agrees to protect its Critical Cyber Assets. We recommend that this measure should read <<The Responsible Entity shall maintain a written cyber security policy.>>

Please explain what <<information security protection programs>> C.M5 refers to.

We feels that C.M10 is too prescriptive. The Compliance Submittal is signed by an authorized representative of the Responsible Entity. That commits the Entity to that information. If it is later discovered that person did not have authorization, then the Entity did not submit compliance on time, which makes the Responsible Entity non-compliant. This incents Entities to insure the appropriately documented information is submitted on-time.

We are concerned that C.M13 requests too much information. Some entities restructure quickly and often. This measure would force those entities to review <<the structure of internal corporate relationships>> too frequently.

We feel that C.M13.1 and C.M.13.2 are overly prescriptive and should be removed.

We question how to document continual engagement by executives. If it cannot be document, then it cannot be measured. We recommend removing <<and that executive level management is continually engaged in the process>> from C.M13.———

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

CHGE feels CIP-004 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

CHGE feels this standard is too prescriptive. NERC standards should state what the target is, not how to hit the target. We feel that quarterly is too onerous. We recommend annually instead of quarterly. This change makes this standard consistent with the standards within the Cyber Security Standard.

Measure M2.4 is a new requirement that should be specified in the corresponding Requirements section.

Measure M4.1 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.2 should be deleted since this duplicates measures M17 and M18 in CIP-003. If this measure remains, then it needs to be specified in the corresponding Requirements section.

Measure M4.3 should be deleted since this duplicates Requirement 8 in CIP-003.

Measure 4.6 should be modified. The requirement for a regular 5 year update to the security screening is not consistent with Requirement R4, which states that a risk based approach be used. The need for rescreening should be cause only.

Compliance 2.3.1 specifies that that the access control list includes service vendors and contractors. Neither group is mentioned in the Requirements or the Measures. Either remove these groups from Compliance, or specify them in the Requirements and the Measures.———

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

CHGE feels CIP-005 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

CHGE requests clarification that Requirement R2 is for ports on the perimeter. Otherwise there is duplication with Requirement R9 in CIP-007.

Requirement R4.2's third bullet is not clear. We recommend changing from
<<
Out of band authentication procedures (e.g. a phone call to verify authenticity before in-band authentication is enabled) to augment static user id and password authentication.
>>
to
<<
Out of band authentication procedures to augment static user id and password access. (e.g. Access will not be enabled via static user id and password authentication unless a telephone call is received from the entity requesting access. On receipt of the telephone call and after successful procedural authentication of the calling party, an administrator will enable access allowing the entitiy to utilize their static user id and password.)
>>

We believe that Requirement R3 is one of many solution to securing dial-in access. Other solutions are bullet items under Requirement R4.2. We recommend that Requirement R3 become another bullet item under Requirement R4.2.———

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

CHGE feels CIP-006 needs a little more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

The term "nearest six-wall boundary" is used in the Purpose. This term confuses some people. We recommend using <<bounded by the nearest walls, floor and ceiling>> instead.

Requirement R1.2 should be changed. The phrase <<and the Critical Assets within them>> should be deleted. Controlling access to the Physical Security perimeter will adequately control physical access to the Critical Cyber Assets and is consistent with R2.

Requirement 1.3 should be changed. The phrase <<and the Critical Cyber Assets>> should be deleted. Monitoring access to/through the Physical Security perimeter will adequately protect the assets. This is consistent with R3.

Requirement R6 is documenting Requirement R1. We recommend combining these into one Requirement.

Measure M1 specifies 90 days/annually. This is not specified in the corresponding the Requirement.

Measure M3 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Measure M4 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Measure M5 is too prescriptive. The first sentence and table should be deleted. The paragraph should start with <<The Responsible Entity>> instead of <In addition, the Responsible Entity>>.

Compliance 1.3 specifies a three year retention. Three years is excessive if there is no incident, especially for video images and access records.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

CHGE feels CIP-007 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Requirement R1 assumes that every Responsible Entity has a test system and test unit for every device. We do not agree that assumption. We do not agree that every patch on every device needs to be tested. If the same patch is applied to the same device, then it needs to be tested once. If the vendor approves the patch and the Responsible Entity applies that patch to all those devices, then the Responsible Entity has secured those devices for this standard. The main source of these objections is the last paragraph in this requirement. We recommend deleting that paragraph. We recommend changing the second sentence in the previous paragraph from
<<
Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment.>>
to
<<
Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment, where available.>>
We like the phrase <<as possible given the technical capability of the Critical Cyber Asset>> in Requirement R6.3. Perhaps this phrase should be used in a revised Requirement R1.

Requirement 3.3 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R1 - R3 of CIP-006.

Requirement 3.4 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.

Requirement R3.5 should be deleted. This standard is the management of Critical Cyber Assets, not access to Critical Cyber Assets. This Requirement is covered by Requirements R5 - R8 of CIP-003, R4 - R5 of CIP-005, and R2 - R4 of CIP-006.

Requirement R3.6 should be modified. The second sentence repeats the first, as such it is necessary and may confuse some.

Requirement R4 should be modified from <<critical cyber security assets>> to <<Critical Cyber Assets>>.

Requirement R4.1 is too prescriptive and should be deleted.

The <<monthly review>> in Requirement R4.2 is too presciptive. We recommend changing R4.2 from
<<
The Responsible Entity shall perform a monthly review of the security patches available for each Critical Cyber Asset. Formal change control and configuration management processes shall be used to document their implementation or the reason for not installing the patch.
>>
to
<<
The Responsible Entity shall perform a routine review of the security patches available for each Critical Cyber Asset. Formal processes shall be used to document their implementation or the reason for not installing the patch.
>>

Add <<where technically feasible>> to the end of Requirement R4.3.

Requirement R5 is called Integrity Software. This term is not defined in CIP-007 or in the FAQ. The drafting team should explain what this term means.

Requirement R5.3 allows exception to R5.1. As such, these Requirements should be combined, otherwise one could be non-compliant with R5.1 and fully compliant with R5.3 while the intent appears to be full compliance with R5.1 and R5.3.

The combined requirement should allow technically feasible alternative solutions.

Change Requirement R5.2 from
<<
The Responsible Entity shall perform a monthly review of the integrity software available for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.
>>
to
<<
Where integrity software is deemed to be technically implementable and has been implemented, the Responsible Entity shall perform a monthly review of the integrity software to ensure that the release level of the integrity software is functionally effective and maintainable for each Critical Cyber Asset. A formal change control and configuration management process shall be used to document the integrity software implementation and upgrades.

>>

We do not agree with <<site-specific installation>> in Requirement 5.4. We recommend changing from
<<
Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each site-specific installation in order to prevent manual dissemination of malware.
>>
to
<<
Where repetitious application of software updates are necessary, such as unattended facilities, the Responsible Entity shall perform integrity verification prior to each software deployment in order to prevent manual dissemination of malware.
>>

Change Requirement R6.1 from
<<
The Responsible Entity shall perform a vulnerability assessment at least annually that includes:
>>
to
<<
The Responsible Entity shall perform a vulnerability assessment at least annually or prior to deployment of an upgrade that includes:
>>

Change Requirement 6.1.3 from
<<
Factory default accounts
>>
to
<<
Scanning for factory default accounts
>>

Change Requirement 6.1.4 from
<<
Security patches and anti-virus version levels
>>
to
<<
Assessing security patches and/or anti-virus version levels, as appropriate
>>

The revised wording of Requirement R6.1 makes Requirement R6.3 unnecessary. Requirement R6.3 should be deleted. Why should an unattended facility have a different vulnerability assesssment schedule than an attended facility?

The title of Requirement R7 is too broad. We recommend changing this title from
<<Retention of System Logs>>
to
<<Retention of Appropriate System Logs>>

The last sentence of this requirement says the Responsible Entity determines its logging strategy. We believe this means the Responsible Entity decides which are the appropriate system logs to retain.

Requirement R9 should clarify that it pertains to ports inside the perimeter. Requirement R2 of CIP-005 covers ports at the perimeter.

The term <<pertinent>> in the last sentence of Requirement R10 should be clarified.

Requirement R11 belongs in CIP-009. This requirement should be moved to that standard. This requirement references Critical Assets. That is not correct. It should a requirement for the backup and recovery of Critical Cyber Assets. The requirement starts with <<on a regular basis>>, and the third sentence says <<at least annually>>. The requirement should stipulate one or the other. We recommend removing <<annually>>. The last sentence is unclear and should be deleted.

Change Measure M2. The semi-annual audit is too prescriptive. This requirements recognizes that the frequency of password changes should be determined by risk assessment.

<<where applicable>> should added to the end of Measure 4.3.

Change the Measures M5.1 - M5.3 from
<<
M5.1 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.
M5.2 The documentation shall include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found.
M5.3 The documentation shall verify that the Responsible Entity is taking appropriate action to address the potential vulnerabilities.
>>
to
<<
M5.1 The Responsible Entity shall maintain documentation identifying the organizational, technical, and procedural controls, including tools and procedures used in the vulnerability assessments.
M5.2 The documentation shall include a record of the results of the annual vulnerability assessment.
M5.3 The documentation shall include a record of the management action plan to remediate reported vulnerabilities, including a record of the completion status of these actions.
>>

Measure M8 should clarify that it pertains to ports inside the perimeter. CIP-005 addresses ports on the perimeter.

Measure M10 corresponds to Requirement R11. We recommended that R11 be moved to CIP-009. This measure should be moved to CIP-009.

Which Requirement and Measurement is Compliance 2.1 associated with?

Compliance 2.2.1.1 needs to be changed so that it is consistent with changes to the corresponding Requirement(s) and Measure(s). This compliance is restricted to <<inside the perimeter>>. There should be no stated difference in the time frames for attended and unattended facilities.

Clarify if Compliance 2.3 should be read as [2.3.1 or 2.3.2 or 2.3.3 (etc)] OR [2.3.1 and 2.3.2 and 2.3.3 (etc)]. We suggest that all of these standards include a statement regarding compliance levels with multiple items.

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

CHGE feels CIP-008 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

Requirement R1 pertains to Cyber Security Incidents, not all incidents. We recommend changing this requirement from
<<The Responsible Entity shall develop and document an incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure accuracy. The incident response plan must address the following items:>>
to
<<The Responsible Entity shall develop and document a Cyber Security Incident response plan. The plan shall provide and support a capability for assessing, mitigating, containing, reporting and responding to Cyber Security Incidents to eliminate or minimize impacts to the organization. The Responsible Entity shall conduct periodic reviews of the plan to ensure adequacy. The Cyber Security Incident response plan must address the following items:>>

Requirement R1 indicates that a list will follow. Requirements R2, R3 and R4 should be renumbered to R1.1, R1.2, and R1.3.

The new R1.3 is too broad. We do not agree with the need to look in another document for this requirement. We recommend a new R1.3 as follows
<<
The Responsible Entity must ensure that the Cyber Security Incident is reported to the ES ISAC either directly or through an intermediary. Documentation submitted is outlined in Requirement R2.
>>

Compliance 1.4 stipulates a requirement that is not in the second posting. We recommend creating a Requirement R2 as follows

<<
R2. The Responsible Entity shall keep all records related to each Cyber Security Incident for three calendar years. This includes, where appropriate, but is not limited to the following:
R2.1 System and application log file entries,
R2.2 Appropriate physical access records,
R2.3 Documented records of investigations and analysis performed, as available,
R2.4 Records of any action taken including any recovery actions initiated.
R2.5Records of all Cyber Security Incidents and subsequent reports submitted to the ES-ISAC.
>>

These changes call for a different Measure M2. <<The Responsible Entity shall retain records for each Cyber Security Incident for three calendar years.>>

We recommend changing Compliance 1.2 from
<<
The Responsible Entity shall keep data for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years. The performance reset period shall be one (1) calendar year.
>>
to
<<
The compliance monitoring period shall keep be three (3) calendar years. The performance reset period shall be one (1) calendar year.
>>

We recommend changing Compliance 1.3 from
<<
The Responsible Entity shall keep documents specified in this standard for three calendar years.
>>
to
<<
The Responsible Entity shall keep all data specified in this standard for three (3) calendar years. The compliance monitor shall keep audit records for three (3) calendar years.
>>

We recommend changing Compliance 2.1.1 from
<<
Documentation exists, but has not been updated with known changes with 90 calendar days.
>>
to
<<
Documentation necessary to demonstrate compliance with Measure M1 exists, but has not been updated within 90 calendar days of known changes.
>>

We recommend changing Compliance 2.2.1 from
<<
Incident response documentation exists, but has not been updated or reviewed within the last 12 months
>>
to
<<

Cyber Security Incident Response Plan documentation exists, but has not been updated or reviewed within the last 12 months
>>

We recommend changing Compliance 2.2.2 from
<<
Incident response documentation exists but is incomplete
>>
to
<<
Cyber Security Incident Response Plan documentation exists but is incomplete
>>

We request clarification on the threshold for Compliance 2.3.2.

Change Compliance 2.4 from
<<
No documentation exists
>>
to
<<
2.4.1 Cyber Security Incident Response Plan documentation does not exist
2.4.2 Cyber Security Incidents have occurred and none were reported to the ES-ISAC
>>

Draft 2 Cyber Security Standards – Comment Form
Please Enter All Comments in Simple Text Format.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

CHGE feels CIP-009 needs more work before it is ready for ballot. This assumes that CIP-002 is acceptable. CIP-002 is not ready for ballot.

We are not sure how broad this standard is. If this is the Recovery Plans of Critical Cyber Assets from Cyber Security Incidents, then the following comments apply.

Requirements R1 and R2 should be swapped. We recommend changing the first requirement from
<<
The Responsible Entity shall specify the appropriate response to events of varying duration and severity that would require the activation of a recovery plan.
>>
to
<<
The Responsibel Entity shall specify the appropriate response to Cyber Security Incidents of varying duration and severity that would require the activation of a Critical Cyber Asset Recovery Plan.
>>
Furthermore, we recommend changing the second requirement from
<<
The Responsible Entity shall create recovery plan(s) for Critical Cyber Assets and exercise its recovery plan at least annually.
>>
to
<<
The Responsible Entity shall create recovery plan(s) for those events and assets indentified in R1 and exercise its recovery plan(s) as defined by its risk based assessment.
>>

We believe that Requirement R3 has the right intention, but its wording is too broad. We recommend changing from

<<
The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the protection of Critical Cyber Assets.
>>
to
<<
The Responsible Entity shall update recovery plan(s) within 90 calendar days of any major change that affects the efficacy of the recovery plan(s).
>>

Requirement R5 is covered in CIP-004. R5 should be deleted.

We believe that Measures M2 and M3 are duplicates. We recommend deleting Measure M2.

Measure M3 corresponds to Requirement R3. We changed Requirement R3. Measure M3 needs a similar modification from
<<
The Responsible Entity shall review and update recovery plan(s) annually.
>>
to
<<
The Responsible Entity shall review and update recovery plan(s) as prescribed by its risk based assessment.
>>

Since Requirement R5 is deleted, the corresponding Measure M4 should be deleted. This is covered in CIP-004.

Compliance 1.3 restates Measure M1. Compliance 1.3 needs different words or should be deleted.

Compliance 2.1 should be changed from
<<
Recovery plan(s) exist, but have not been reviewed or updated in the last calendar year
>>
to
<<
Recovery plan(s) exist, but have not been reviewed or updated, if necessary, in the last calendar year
>>

As posted, if a Responsible Entity has not reviewed their recovery paln(s) in the last calendar year, they are Level 1 and Level 2 non-compliant. This is confusing. Also, training is covered in CIP-004.
Compliance 2.2 should be changed from
<<
Recovery plan(s) have not been reviewed, exercised or training performed.
>>
to
<<
Recovery plan(s) have not been exercised according to the Responsible Entity's risk based assessment.
>>

Compliance 2.3 includes specific roles and responsibilities that are not in the Requirements or the Measures. It is confusing and inappropriate to introduce new requirements in Compliance. The reference to <<types of events that are necessary>> is confusing. This standard specifies no types of events as <<necessary>>.

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.

NO

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

CHGE feels the Implementation Plan does not allow enough time for compliance. First, these standards have substantial changes from 1200. A Responsible Entity could be compliant with 1200 and require much work before they are compliant with these standards. Secondly, budgets are established months ahead of time. Some Responsible Entities have frozen their 2005 budgets. For either reason. there are enough Entities that will not meet the initial dates for auditable compliance or substantial compliance (first quarter of 2006) . We recommend that the 2006 dates change to 2007 dates, the 2007 dates change to 2008 dates, etc.

We are concerned with compliance for substations. Substations are part of the <<Other Facilities>>. We recommend the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.

Clarify what dates the compliance submittal is for. Is the first quarter submittal of 2007 for January 1, 2006 to December 31, 2006? Or is the 2007 submittal as of a year ending on the submittal date? Or is the 2007 submittal what the Entity has as of that submittal date?

If the Functional Model is not implemented according to the Functional Model schedule, what is the impact on the Cyber Security Implementation Plan?

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:	Gary Campbell	
Organization:	MAIN	
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.

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.

Responsible entity must be defined or omitted.

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.

I do not think it should be documented here that the methodology should be documented. The auditor can then use this tool to asses the Critical Assets identified.

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.

M1 - The measures should not be referencing the requirements such as " as identified in R1". The requirement should contain all the components to be measured. In M1, in could read the " the Respnsoble Entity shall maintian the list of Critical Assets"

M2 - Do not any requiremetns for measure nor is it mention that it must be used.

M3 - Is confusing in that I am not sure if I am suppose to maintain a list of other Critcal Assts only and do not have to maintain a list for anything else.

M4 This should be part of requirements and the measure should be that we look for the updates.

In levels of compliance, I am assesing non-cpomliance for a 30 day window but have stated it is required

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.

In M1, as an auditor I would only be looking for a Cyber security policy which states the commitment to protect Critical Cyber Assests, nothing more.

M2 This should be made into a requirements with the measure looking for the review times. I also think it should not be so undefinable.

M3 - M18 These measures as stated are really requirements and should be put there. The measures should be looking for these review times, documents with cetain requirement specifications, etc.

Levels of Compliance

Specifiy review times in the requirements

Reguirements should state the minimum items the entity is to address, the measures should look to measure the global items such as plans, procedures, actions, etc. And levels of compliance should asses these measures.

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.

Measures are again stating requirements and specifically setting minimum requirements. These should be redeveloped to measure the minimum requirement once stated as a requirement.
The way the measures are written, as an auditor I do not care what the requirements tell me should be in a procedure, policy etc. The measures are telling what to look for by the usage of "shall" and then specify what is to be looked for.

Levels of Compliance

Specifiy review times in the requirements and then measure

There are measures that are written but have no levels of non-compliance sush as M6. Please review all measures.

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.

Measures are again stating requirements and specifically setting minimum requirements. These should be redeveloped to measure the minimu requirement once stated as a requirement.

The way the measures are written, as an auditor I do not care what the requirements tell me should be in a procedure, policy etc. The measures are telling what to look for by the usage of "shall" and then specify what is to be looked for.

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.

Measures are again stating requirements and specifically setting minimum requirements. These should be redeveloped to measure the minimu requirement once stated as a requirement.

The way the measures are written, as an auditor I do not care what the requirements tell me should be in a procedure, policy etc. The measures are telling what to look for by the usage of "shall" and then specify what is to be looked for.

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.

Measures are again stating requirements and specifically setting minimum requirements. These should be redeveloped to measure the minimum requirement once stated as a requirement.

Level of compliance:

Level 1 - How many documents do I abosolutly have to find? Do you want me to determine as the auditor the specific items identified. What if i miss an item. I do not think I can clearly find them.

Specifiy review times in the requirements and then measure

How big is a gap? How I am to measure a gap?

Level 3

How many of the 11 items mention constitute level3 , 1 or all?

Level 4 - This is a waste of a level. The way it is worded, if I have one document I can never be found to be level 4. This does not promote compliance. You would expect entites to have some level of completion to their documentation so may be we should looking for at least half of the documentation completed to be level 4.

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.

Measures are again stating requirements and specifically setting minimum requirements. These should be redeveloped to measure the minimum requirement once stated as a requirement.

Measures should not reference other standards. If the standard can not stand on its own then then should the two be combined or is there something wrong?

Some suggestion for Measures for this Standard

The Responsible entity has an incident response plan.

The Responsible Entity has procedures on Classification of Incidents and Response Actions for Cyber Security Incidents.

The Responsible Entity has reported all incidents to ESISAC.

Levels of Compliance

Specifiy review times in the requirements

Level 4 - This is a waste of a level. The way it is worded, if I have one document I can never be found to be level 4. This does not promote compliance. You would expect entites to have some level of completion to their documentation so maybe we should looking for at least half of the documentation completed to be level 4.

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.

The standard should not reference another standard. Either R5 should stand alone inthis standard or CIP-004-1

Masures are again stating requirements and specifically setting minimum requirements. These should be redeveloped to measure the minimum requirement once stated as a requirement.

Measures

In M1, there was no mention of drills to be required for the recovery plans. If I was an sitting across from an auditor I would ask how you can measure me for something that you did not require of me.

In M2, what is it specifically that is to be reviewed or updated?

In M3, Is'nt the 90 day requirement in R3 important?

In M4, this should be a requirement.

Levels of compliance

Level 2 - The recovery plan were only to be communicated? It seems were asking for more here.

Level 3 - It seems to me that if the types of events are important then the standard would specifiy these types otherwise you have set no minumum standard. Nor does the requirements tell me that I need to addres roles and responsibilites.

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.

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**
☐ **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: Midwest Reliability Organization

Lead Contact: **Lawrence R Larson, PE**

Contact Organization: **Otter Tail Power Company**

Contact Segment: **2**

Contact Telephone: **218.739.8572**

Contact Email: **llarson@otpco.com**

Additional Member Name	Additional Member Organization	Region*	Segment*
Dan Klempel	**BEPC**	**MRO**	**2**
Al Boesch	**NPPD**	**MRO**	**2**
Terry Bilke	**MISO**	**MRO**	**2**
Dennis Florom	**LES**	**MRO**	**2**
Ken Goldsmith	**ALT**	**MRO**	**2**
Todd Gosnell	**OPPD**	**MRO**	**2**
Wayne Guttormson	**SPC**	**MRO**	**2**
Jim Maenner	**WPS**	**MRO**	**2**
Tom Mielnik	**MEC**	**MRO**	**2**
Darrick Moe	**WAPA**	**MRO**	**2**
Joe Knight	**MRO**	**MRO**	**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.

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.

Note that all referenced section numbers are with respect to the numbering found in the Standards posted as of Jan 24, not the earlier (Jan 17) version. Also note that since quotation marks are not allowed in these comment forms, we have used parenthesis in their place as needed to reference specific text.

Please clarify what is meant by Authorized Access; the term is used several times in the document.

The definition for Cyber Security Incident Should not include (was an attempt to compromise) or (was an attempt to disrupt). This is too vague and onerous. Depending on the intended meaning, such attempts are made systematically. If an attempted ping is discovered against an IP address, is that an attempt to compromise?

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.

While it indicates that an appropriate risk assessment methodology should be applied, it then also goes on to provide too much prescriptive detail about what has to be inside and outside that risk assessment. It is not up to the Standard drafting team to define what the critical assets are; each company should identify them based on their risk assessment. Much of the language under R1.1.1 - R1.1.9 should be eliminated, and the simple instructions that an appropriate assessment methodology should be developed and used should be left to stand on its own. R1.1.3 and R1.1.8 are particularly problematic. Each entity should define how they will assess risk for elements outside the control center (substations, etc), and should be able to demonstrate that they are abiding by that assessment - R1.1.3 to R1.1.9 inappropriately force particular outcomes (e.g. inappropriatly requires that many substations become Critical Assets).

The words DETRIMENTAL IMPACT in section R1.1 are problematic, because it would be definined diferently by different entities.

For Applicability (Section 4) of all the CIP(s), Nuclear facilities are exempted. The way this is phrased causes concern, because these facilities impact the grid just as other generators do. Does the NRC assure that nuclear facilities meet or exceed these cyber security standards? If so, that should be stated. If not, additional information about safeguards that do apply to these facilities should be provided.

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.

See response to Q2.

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.

CIP-003 contains language that is redundant/overlapping with CIP-007. These two should be combined into one.

Under Section 2 (Non-Compliance levels): eliminate 2.3.3 - it is too vague. Also, move the following down one level from their current position (make one level less severe): 2.3.2, 2.4.4, and 2.4.7.

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.

The Awareness aspect should be eliminated throughout CIP-004, as the additional overhead it requires is not justified for the perceived benefit. The requirements imposed by R2-R4 would do the job adequately without R1 being required. Awareness will normally be done anyway as part of a good program, but defining these specific compliance requirements for this aspect is not sufficiently beneficial to warrant the additional tracking overhead.

M4.2 requires a mandatory quarterly review of a document. No reviews of any documents on any time-frame shorter than annually should be required in any of these Cyber Security Requirements.

M4.4 mandates a seven year criminal check prior to granting access. This is not allowed by some hiring regulations. The requirement should be that each company has a policy for personnel risk assessment, and that they can demonstrate they follow that policy - no additional prescriptive requirements should be presented in this area. The company's policy should cover how contractors (vendors) with authorized access are treated, but should not prescribe how a company needs to treat such circumstances. Standards should focus on WHAT, not HOW.

M4.6 should be deleted. Such updated screenings can be provided for if a company feels they are justified. However, in some environments (low turn-over, small groups of employees, etc), such re-screens would be pointless and the overhead and inconvenience would not be justified

We suggest a wording change in Section 2.1.2 Levels of non-compliance to focus on whether the access was revoked within 24 hours (rather than focus on whether the access control list was updated).

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.

R3 should be modified by deleting all the langauge except the first sentence and the last sentence. In particular, the reference to technically feasibility is too vague. It is adequate to require that entities implement proceedures they have defined as appropriate based on their risk analysis.

The reference to "Document(s)" in the Levels of non-compliance is too vague - which documents specifically?

M2 and 2.3.2 - disabling unused ports - this is redundant with language in 007, put in one or the other but not in both.

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.

It should be clarified that the Requirements herein do not necessarily apply to substations. Separate language should be added that indicates that, in regards to physical security for substations, each entity should establish and follow its own risk assessment policy as they deem appropriate. The prescriptive measures defined here are too much overhead to require for substations.

Under Levels of Non-Compliance, 2.1.2, 2.2.2, and 2.3.2 should be eliminated or modified, as there is no reasonable way to track (aggregate interruptions). It is not clear what this term means, and it is introduced in the Compliance Section while it was not discussed in the Requirements or Measures Sections.

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.

R5 should be deleted. No definition is provided for exactly what is meant by INTEGRITY SOFTWARE, which is a problem. This section should be replaced by a general requirement to address the appropriate use of such software in a security plan. However, requiring the use of such software categorically is not justified; its deployment should be weighed and purused as appropriate by each entity.

R6.3 is vague; it should be eliminated.

R9 is redundant with CIP-005; it should be eliminated from CIP-007

Again, CIP-003 and CIP-007 should be combined (ie R3.4 3.5Access reviews also included in 003; R8 Change control also located in 003; R9 Disabling unused host ports also included in 005).

Levels of non-compliance - there is a lot under Level 3 - some of these should be moved to Level 2.

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.

Note that, as NERC has already indicated, these should not be approved separately, (should not stand alone), so they are not ready until the others are.

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.

Note that these should not be approved separately, (should not stand alone), so they are not ready until the others are.

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.

All compliance requirements should be delayed an additonal year. Starting the first quarter of 2006, NERC should work with the industry to gather examples of documents that would fulfill the requirments of this Standard - that is, to gather best practices examples. In mid-2006, NERC should host industry training sessions to review this material. This would give companies the last half of 2006 to review their current documentation as compared to these examples, and make adjustments as required. Field testing should also be provided for. The phased-in (AC vs SC and Control Center vs Other Facilities) approach, as defined in the Implementation plan, should then commence in 2007. This assumes the schedule proceeds as defined in the assumptions bulleted at the beginning of the Implementation Plan.