

Comment Form – Cyber Security Standards CIP-002 through CIP-009

**COMMENT FORM
Cyber Security Standards CIP-002 through CIP-009**

This form is provided for review purposes only. To submit comments, please use the form available at <http://www.nerc.net/cyber-security/>. If you have questions please contact Gerry Cauley at gerry.cauley@nerc.net or by telephone at (609) 947-3885.

Individual Commenter Information		
(Complete this page for comments from one organization or individual.)		
Name:	P. D. Henderson	
Organization:	Independent Electricity System Operator (IESO), Ontario	
Telephone:	905 855-6258	
Email:	Peter.Henderson@ieso.ca	
NERC Region	<input type="checkbox"/>	Registered Ballot Body Segment
<input type="checkbox"/> ERCOT	<input type="checkbox"/>	1 - Transmission Owners
<input type="checkbox"/> ECAR	<input checked="" type="checkbox"/>	2 - RTOs, ISOs, Regional Reliability Councils
<input type="checkbox"/> FRCC	<input type="checkbox"/>	3 - Load-serving Entities
<input type="checkbox"/> MAAC	<input type="checkbox"/>	4 - Transmission-dependent Utilities
<input type="checkbox"/> MAIN	<input type="checkbox"/>	5 - Electric Generators
<input type="checkbox"/> MAPP	<input type="checkbox"/>	6 - Electricity Brokers, Aggregators, and Marketers
<input checked="" type="checkbox"/> NPCC	<input type="checkbox"/>	7 - Large Electricity End Users
<input type="checkbox"/> SERC	<input type="checkbox"/>	8 - Small Electricity End Users
<input type="checkbox"/> SPP	<input type="checkbox"/>	9 - Federal, State, Provincial Regulatory or other Government Entities
<input type="checkbox"/> WECC		
<input type="checkbox"/> NA		

Comment Form – Cyber Security Standards CIP-002 through CIP-009

Question 1: Do you agree with the definitions presented in these standards?

Yes

No

If no, please identify those with which you do not agree and please suggest alternative wording.

Critical Assets — Comments

Cyber Assets — Comments

Critical Cyber Assets — Comments

Cyber Security Incident — Comments

Electronic Security Perimeter — Comments

Physical Security Perimeter — Comments

Additional Comments

We suggest that definitions should be revised and be consistent with NERC Glossary of Terms (under development and/or approved). This is necessary to avoid any confusion and/or inconsistency in definitions and for their uniform application to the Industry.

Comment Form – Cyber Security Standards CIP-002 through CIP-009

Question 2: 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.

General Comments on CIP-002-1

Requirements

Comments – R1

1. Remove R1.1

Rational

NERC Standards must fall within NERC's scope which is the Bulk Electric System. Some of these requirements are beyond the BES definition.

Comments – R2

Comments – R3

Measures

Comments –M1

Comments –M2

1. Delete the word “approved” in M2 as Requirement R2 does not impose a requirement for the list of Critical Cyber Assets to be formally approved. Alternatively, delete M2 all together as the requirement for a formally approved list of Critical Cyber Assets is specified in R3 and M3.

Comments – M3

Compliance

Comment Form – Cyber Security Standards CIP-002 through CIP-009

Comments – C1.1

Comments – C1.2

Comments – C1.3

Comments – C1.4

Comments – C2.1

Comments – C2.2

Comments – C2.3

Comments – C2.4

Question 3: Do you believe that 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 Comments on CIP-003-1

The requirement to document non-conformance with an Entity's cyber security policy is sensible, but the requirement for a senior manager to approve all of those non-conformances is not. Some non-conformances may occur for reasons that are understood and knowingly tolerated for valid reasons. One could reasonably require the senior manager concerned to approve these, which effectively signals informed consent. However, there may be instances where a non-conformance occurs which represents an error that is not acceptable to the Entity concerned – one which needs correcting rather than approval.

Comment Form – Cyber Security Standards CIP-002 through CIP-009

Consider the wording, “Instances where the Responsible Entity accepts non-conformance with its cyber security policy.....” .

Requirements

Comments – R1

1. R1 should be rewritten to "each Entity shall have a Cyber Security Policy that includes the following." NERC Standards should be focused on Reliability not management structure.

Comments – R2

1. Change R2 to "The Responsible Entity shall assign a senior manager or delegate(s) with responsibility"

Comments – R3

Comments – R4

1. R5 and R4 should be combined. Both talk about requirements to protect information about Critical Cyber Assets.

2. In R4.3, it is unclear what is meant by the phrase, “cyber security protection controls”. This could be taken as a reference to the sum-total of controls in place to ensure compliance with CIP-002 through CIP-009. If this is actually intended, the requirement to assess and document these controls annually appears to overlap many similar requirements throughout the standards (eg. – the requirements in R1.3, R5.2, R5.3, and R6.1 of CIP-003, R3 and R4, of CIP-005, R7 of CIP-006, and R9 of CIP-007)

3. The minimum should not include everything. Remove ", and any related security information".

Comments – R5

Requirements 5.1, 5.1.1, 5.1.2, and 5.1.3 are about managing access to the assets themselves, yet they appear as sub-bullets of a requirement to manage access to information about Critical Cyber Assets. This is confusing, particularly as there is no measure that relates to the management of access to the assets themselves.

Comments – R6

1. R6.2 appears to require that testing be performed prior to promoting systems to production. It is unclear what the purpose and scope of that testing needs to be, and where those dimensions are documented. If this is a reference to testing required in CIP-007, this should be noted, or the reference to testing deleted in favour of a more thorough treatment in CIP-007.

2. In R6.3, it is unclear what is meant by the qualifier “supporting” when referring to configuration management activities.

3. R6.3 is redundant given the text of R6, and overlaps with the requirements of R6.2.

Measures

Comments –M1

Comments –M2

Comments – M3

Comments –M4

1. Measures M4 and M5 should be reviewed in light of comment 1 on R4 & R5 above.

Comments – M5

1. Measures M4 and M5 should be reviewed in light of comment 1 on R4 & R5 above.
2. M5 refers to a policy for management of access to information. There is no corresponding requirement (R5 requires the establishment of a program)

Comments – M6

1. Measure M6 should be reviewed in light of comments on R6 above.

Compliance

Comments – C1.1

Comments – C1.2

Comments – C1.3

Comments – C1.4

1. Section 1.4 under “Compliance” is somewhat unclear. The text appears to suggest that a Responsible Entity that does not fulfill one or more of the Standard’s requirements should actually claim that it is fully compliant with the Standard if it has a properly documented exception to those requirements approved by the designated senior manager at the time of compliance reporting. Is this the intent?

Comments – C2.1

1. Requirement R 2.2 requires that changes to the designated senior manager must be documented within 30 days of the effective date. Compliance statement 2.1.1, however, states that an entity that fails to do so within 10 days is in non-compliance. This inconsistency should be resolved.

2. Compliance statement 2.1.1 imposes a requirement that is not identified in the requirements section. Specifically, 2.1.1 effectively imposes a requirement that the gap in designating a senior management representative be less than 10 days, which is not specified in the requirements section.

3. Requirement R1.4 requires annual review of the cyber security policy. This is not consistent with compliance statement 2.1.2 which suggests that an entity that reviews its policy every three years would be fully compliant.

4. Compliance statement 2.1.3 imposes a requirement that is not identified in the requirements section.

Comments – C2.2

1. Compliance statement 2.2.3 should refer to access privileges to information associated with Critical Cyber Assets to more clearly correspond to R5.2 and to avoid imposing a requirement to review access privileges to the Critical Cyber Assets themselves that is not identified in the Requirements section.

Comments – C2.3

1. Compliance statement 2.3.2 imposes a requirement that is not identified in the Requirements section. The compliance statement refers to access to the Critical Cyber Assets themselves, whereas the requirements refer to access to information about the assets.

2. Furthermore, compliance statement 2.3.2 imposes a new requirement that the roles and responsibilities of personnel with access to the assets must be documented (requiring a mapping of role/responsibility to access privilege), whereas the Requirements section asks only that access privileges correspond to roles and responsibilities (which is a looser requirement needing far less documentation and simpler business processes).

3. Failure to document the roles and responsibilities of personnel with access to Critical Cyber Assets (compliance statement 2.3.2) should result in a lower level of non-compliance than failure to review access privileges (Compliance statement 2.2.3).

4. Compliance statement 2.3.2 imposes a requirement that does not appear in the Requirements section (viz. a requirement to document controls for testing and assessment of new or replacement systems and software patches/changes). Compliance statements should not impose new requirements.

Comments – C2.4

1. Compliance statement 2.4.3 should be revised to more clearly refer to a program for the identification and classification of information about Critical Cyber Assets.

Comment Form – Cyber Security Standards CIP-002 through CIP-009

2. Compliance statement 2.4.5 appears to duplicate 2.2.3 but at a different level of non-compliance.

3. Compliance statement 2.4.6 imposes new requirements not specified in the Requirements section – specifically to document access revocations and changes. The requirements only specify the need to confirm that access privileges that prevail at the time of review are appropriate, without reference to maintaining a history of how those privileges came about.

Question 4: 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 below.

General Comments on CIP-004-1

Change the purpose to "This standard requires that personnel having access to Critical Cyber Assets, including contractors and service vendors, have a higher level of personnel risk assessment, training and security awareness than personnel not provided access."

Comment - access could be electronic, physical or both.

Requirements

Comments – R1

Comments – R2

1. R2.1 should be reworded to state "All personnel having access to Critical Cyber Assets shall have received cyber security training or shall be escorted by personnel who have had such training."

Comments – R3

1. The text of R3.1 and R3.2 overlap somewhat. The two requirements should be combined into one statement and the remaining sections re-numbered.

2. R3.1 and R3.2 should be reworded to be applicable only to personnel, vendors and contractors who are granted unescorted access to Critical Cyber Assets.

Comments – R4

Comment Form – Cyber Security Standards CIP-002 through CIP-009

1. R4 requires quarterly review of access lists, where as M4 suggests that annual review is sufficient. The discrepancy should be resolved.
2. Add R4.3 Unauthorized personnel must be escorted by authorized personnel

Measures

Comments –M1

1. Reorder to stay consistent with R1 - R4

Comments –M2

Comments – M3

Comments –M4

Compliance

Comments – C1.1

Comments – C1.2

Comments – C1.3

Comments – C1.4

Comments – C2.1

1. Update 2.1.1 to remain consistent with R4.1 and M4. Change the words from "for more than three months but less than six months;

to

annually.

2. Failure to document the personnel risk assessment gives rise to both Level 1 non-compliance (2.1.3) and Level 3 non-compliance (2.3.3). This is confusing and should be resolved.

3. If documentation of the personnel risk assessment program reveals that the program fails to require risk assessment updates every 5 years, a Responsible Entity could legitimately claim non-compliance at Level 1 (2.1.3) whereas 2.3.7 characterizes this as Level 3 non-compliance. This is confusing and should be resolved.

Comments – C2.2

1. Remove 2.2.1 since it is covered by the updated 2.1.1.
2. Failure of the Training program to address two or more required items gives rise to non-compliance at Level 2 (2.2.3) and Level 3 (2.3.4). This is confusing and should be resolved.

Comments – C2.3

1. Failure to document the personnel risk assessment gives rise to both Level 1 non-compliance (2.1.3) and Level 3 non-compliance (2.3.3). This is confusing and should be resolved.
2. Failure of the Training program to address two or more required items gives rise to non-compliance at Level 2 (2.2.3) and Level 3 (2.3.4). This is confusing and should be resolved.
3. If documentation of the personnel risk assessment program reveals that the program fails to require risk assessment updates every 5 years, a Responsible Entity could legitimately claim non-compliance at Level 1 (2.1.3) whereas 2.3.7 characterizes this as Level 3 non-compliance. This is confusing and should be resolved.

Comments – C2.4

1. Eliminate 2.3.7 since it is covered by 2.1.3.

Question 5: 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.

General Comments on CIP-005-1

Requirements

Comments – R1

1. R1.4 is unclear when one considers requirements statements in CIP-005 that refer explicitly to Critical Cyber Assets rather than to the more generic “cyber assets”. For instance, R1 requires the Responsible Entity to identify the electronic security perimeter around its “Critical Cyber Assets”. On one hand, the wording of R1.4 could be taken to mean that one should replace the words “Critical Cyber Assets” by the words “Critical and Non-Critical Cyber Assets” when interpreting the standard. Under this interpretation, the Responsible Entity should identify the electronic security perimeter around non-critical cyber assets even if there are no Critical Cyber Assets within that perimeter. Alternatively, one could argue that the wording of R1 explicitly excludes non-critical cyber assets, and therefore failure to consider non-critical cyber assets is not a cause for concern.

2. Please clarify. Given R1.5 and given that this standard focuses on the definition and management of the electronic security perimeter, it is suggested that R1.4 can be deleted without any ill effect.

Comments – R2

Comments – R3

1. R3.2 should be clarified by rewording it as, “The Responsible Entity shall implement a procedure to verify authorized access to the protected Critical Cyber Assets on a periodic basis as determined and documented by the Responsible Entity’s risk based assessment.

2. Logs can be very large. People review reports that use logs as input. R3.3 should be changed to "At least every ninety calendar days assess access logs for unauthorized access or attempts."

Comments – R4

Comments – R5

Comment Form – Cyber Security Standards CIP-002 through CIP-009

Comments – R6

1. This Standard has no R6.

Measures

Comments –M1

1. Measure M1 effectively imposes a new requirement - the need to identify all non-critical cyber assets within the security perimeter. If this is a requirement it should be identified in the Requirements section of the Standard. Note that such a requirement would be redundant given R1 of CIP-007.

Comments –M2

Comments – M3

Comments –M4

Comments – M5

Comments – M6

1. There is no M6

Compliance

Comments – C1.1

Comments – C1.2

Comments – C1.3

Comments – C1.4

Comments – C2.1

Comment Form – Cyber Security Standards CIP-002 through CIP-009

1. Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2

Comments – C2.2

1. Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2

Comments – C2.3

1. Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2

Comments – C2.4

Question 6: 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 Comments on CIP-006-1

Requirements

Comments – R1

1. Requirement R1.4 is too prescriptive. R3 covers several possible access devices.

Comments – R2

Comment Form – Cyber Security Standards CIP-002 through CIP-009

Comments – R3

1. R3 should read, “the Responsible Entity shall document and implement”. Otherwise, M 3 establishes a new requirement not identified in the Requirements section of the Standard.
2. R3.1 - R3.4 are too prescriptive. They should be removed.

Comments – R4

1. R4 should read, “the Responsible Entity shall document and implement”. Otherwise, M 4 establishes a new requirement not identified in the Requirements section of the Standard.
2. R4.1 - R4.3 are too prescriptive. They should be removed.

Comments – R5

1. R5 should read, “the Responsible Entity shall document and implement”. Otherwise, M 5 establishes a new requirement not identified in the Requirements section of the Standard.
2. R5.1 - R5.3 are too prescriptive. They should be removed.

Comments – R6

Comments – R7

Measures

Comments –M1

Comments –M2

Comments – M3

Comments –M4

Comment Form – Cyber Security Standards CIP-002 through CIP-009

Comments – M5

Comments – M6

Comments – M7

Compliance

Comments – C1.1

Comments – C1.2

Comments – C1.3

Comments – C1.4

Comments – C2.1

Comments – C2.2

Comments – C2.3

In Compliance statement 2.3.1, please clarify what is meant by “record”. If the reference is really to a “document”, then Compliance statement 2.3.1 appears to contradict Compliance statement 2.4.3 in cases where one of the missing documents is the security plan. Note also that no non-compliance level has been defined for cases where one required document (or record) is missing unless that document is the security plan.

Comments – C2.4

Question 7: Do you believe Standard CIP-007-1 is ready to go to ballot?

Comment Form – Cyber Security Standards CIP-002 through CIP-009

Yes

No

If 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 on CIP-007-1

It is unreasonable to require that documents referenced in this standard should be revised within 30 days of a change to the systems or controls. Even minor changes to network configurations or the addition of a single hardware element could require updating the large number of documents specified in this standard. The sheer volume of work involved is very likely to take considerably more than 30 days.

Furthermore, since this standard applies to all cyber assets within the electronic security perimeter, the frequency of change could be high for organizations with large numbers of assets within the security perimeter. It is conceivable that the documentation required would be under constant revision (hence making it effectively impossible to establish a measurable date on which the revision is complete). A requirement to update the documents at least annually would be more sensible.

It is unclear in the Compliance section what is meant by the terms “system security controls” or “documented system security controls” since these terms are never defined in the standard. If the intent is to refer to M1 through M10, this should be clearly stated.

Compliance levels in this Standard are not consistent with those established in CIP-005 and CIP-006 for similar levels of logging system unavailability.

Remove the first sentence of the purpose since it is redundant with the rest of the purpose. We prefer the second and third sentence of the purpose.

Requirements

Comments – R1

1. The wording of R1 requires clarification given that some requirements in this standard refer specifically to Critical Cyber Assets rather than to the more generic “cyber assets”. For instance, R8 requires data destruction or removal prior to disposal of a Critical Cyber Asset. On one hand, the wording of R1 could be taken to mean that one should replace the words “Critical Cyber Assets” by the words “Critical and Non-Critical Cyber Assets” when interpreting the standard. Under this interpretation, the Responsible Entity should wipe data on all assets prior to disposal. Alternatively, one could argue that the wording of R8 explicitly excludes non-critical cyber assets, and therefore failure to consider wipe data from non-critical cyber assets does not give rise to non-compliance. Please clarify.

Comments – R2

1. R2 requires that testing be done but it is unclear what that testing is to accomplish.

Comments – R3

Comments – R4

Comments – R5

1. R5 requires that virus signatures must be explicitly assessed for applicability, installed under change management and configuration management control, and that all of this must be documented. This is overly prescriptive as it does not contemplate Responsible Entities employing auto-update services commonly offered by service providers.

Comments – R6

1. R6.1.1 should be reworded to state, “Wherever technically practical,
2. There is a verb missing in R6.1.5.
3. R6.1.5 is redundant given the requirements of CIP-003 R5 and CIP-004 R4. R6.1.5 should be deleted.
4. There appears to be overlap between R6.2.2 and R6.1.1. To avoid confusion, the wording of R6.1 should be modified to include coverage of factory default accounts, and R6.2.2 deleted.
5. The requirement for an audit trail of account use in R6.2.4 overlaps the audit requirement in R6.2.5. These requirements should be combined in R6.2.4, and R6.2.5 deleted to avoid confusion.
6. In R6.3.2 – the special character requirement should be removed. This is not enforceable on many systems including AD. (AD allows enforcement of only 3 of 4 items).

Comments – R7

Comments – R8

Comments – R9

1. R9 should read as Critical Cyber Assets throughout.

Comments – R10

Measures

Comments –M1

Comments –M2

1. Measure M2.1, as written, specifies a requirement. Requirements should be specified only in the Requirements section of the document.

2. Measure M2.3 establishes a requirement new to this standard – to formally accept test results indicative of successful completion of changes to Critical Cyber Assets. This new requirement should not be established in the Measures section. Consider moving this measure to CIP-003 and associating it with R6.2

3. Measures M2.1, M2.2 and M2.3 should be rephrased as measures.

Comments – M3

Comments –M4

Comments – M5

Comments – M6

Comments – M7

Comments – M8

Comments – M9

Comments – M10

Compliance

Comments – C1.1

Comment Form – Cyber Security Standards CIP-002 through CIP-009

Comments – C1.2

Comments – C1.3

Comments – C1.4

Comments – C2.1

1. Compliance statement 2.1.4 effectively establishes a new requirement for annual review of access privileges and authorization rights. If this is a requirement, it should be established in the Requirements section. Furthermore, this compliance statement should be reviewed for consistency against compliance statements 2.1.1 and 2.2.1 of CIP-004

Comments – C2.2

Comments – C2.3

Comments – C2.4

Question 8: 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.

General Comments on CIP-008-1

Requirements

Comments – R1

Comments – R2

1. The final sentence of Requirement R2 should be reworded as, “ this documentation must include, where relevant, the following:.....” . This change is needed since not all relevant incidents will give rise to all of the types of documentation listed. For instance, physical security incidents will generally not give rise to system or application log file entries and cyber incidents will not give rise to video and/or physical access records.

2. R2 Retention period should be 2 years. The utility of a 3 year retention period is unclear.

Measures

Comments –M1

Comments –M2

Compliance

Comments – C1.1

Comments – C1.2

Comments – C1.3

Comments – C1.4

Comments – C2.1

Comment Form – Cyber Security Standards CIP-002 through CIP-009

Comments – C2.2

Comments – C2.3

Comments – C2.4

Question 9: 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.

General Comments on CIP-007-1

Requirements

Comments – R1

Comments – R2

Comments – R3

Comments – R4

Comments – R5

Measures

Comments –M1

Comments –M2

Comments –M3

Comments –M4

Comments –M5

Compliance

Comments – C1.1

Comments – C1.2

Comments – C1.3

Comments – C1.4

Comments – C2.1

Comments – C2.2

Comments – C2.3

Comments – C2.4

Question 10: Does draft 2 of the Implementation Plan for the Cyber Security Standards allow enough time for compliance?

Yes

No

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

Comments

Since the standard will not become official before October 1, 2005, it is unrealistic to expect an acceptable level of auditable compliance in 2007 for the following reasons:

1. NERC CIP-002 through CIP-009 establish requirements which are new and/or requirements of broader scope or much greater detail than those of NERC 1200 (See attached table). A significant amount of work will be needed to come into compliance with these new/extended requirements, even for Responsible Entities that are currently compliant with NERC 1200.

2. Most, if not all, Responsible Entities will require significant expenditure to perform the work needed to come into compliance.

3. It is unreasonable to expect that Entities will have budgetted on the basis of standards which are still in flux, the approval of which is not a given. Some Entities may feel that approving funds to satisfy a standard which is not yet approved is unacceptably speculative, bordering on the imprudent.

4. The implementation plan should recognize typical corporate fiscal planning processes. Most Entities are already well into their business planning/budgeting cycle for establishing budgets for 2006. Many, if not most, entities will have finalized their budgets for 2006 well before this set of Standards is ratified by the NERC Board of Trustees.

Comment Form – Cyber Security Standards CIP-002 through CIP-009

5. Even if budgets are approved for 2006 for provisions to come into compliance with the as yet un-approved standards, the scope of CIP-002 through CIP-009 is so much greater than the scope of NERC 1200 that completing the work needed to come into full compliance could take more than a year to complete.

6. We suggest that the earliest date at which Responsible Entities should be required to have processes and technology in place to come into Auditable Compliance should be Q2 2008. This is based on an assumption that the Standards will be approved in October, 2005 and the comment appearing below (#8) is adopted. Should the approval date slip beyond October 2005, the date for Auditable Compliance should be deferred correspondingly.

7. The draft Implementation Plan specifies the year in which entities must be "Auditably Compliant". In the WEBEX conference call of June 1, clarification was sought as to whether this means that entities must have the processes and provisions required to meet the Standards first in place no later than that date, or whether entities must also have at that time the historical records required to withstand a full audit. It was clarified that where the Implementation Plan specifies "Auditable Compliance" in year "X", the Responsible Entity is expected to be able to produce the historical records required by the Standards at that time. In effect, because some Standards require up to one year's worth of historical records be kept, this means that the Responsible Entity needs to have the processes and provisions needed to meet the Standards' requirements in place up to one year earlier than the date of the first audit.

For instance, an entity which has to be "Auditably Compliant" to CIP-006 R7 in the second quarter of 2007 would have to have provisions in place to begin fulfilling that requirement in the second quarter of 2006. An entity which must be auditably compliant with CIP-008 R2 in 2007 must, in fact, have begun collecting the required records in 2004. Both of these requirements are unreasonable.

In keeping with the comment above, the first date Responsible Entities should be required to have processes and technology in place to meet the standards should be no sooner than Q2-2008. The earliest date for auditable compliance should be Q2-2009.

8. Alternatively, the wording of the standards or of the implementation plan should contemplate that entities may legitimately not have historical records to submit until some time after they are required to come into Auditable Compliance. It is suggested that the pre-ambles to the compliance sections of each standard could include text which makes it clear that Responsible Entities which retain necessary documentation from the date that the Standards first come into force will be deemed to be in compliance with requirements to maintain historical records. If this approach is adopted, the earliest date for auditable compliance should be Q2 2008 consistent with the comment above.

The following requirements are either new or substantially greater in scope than those appearing in NERC 1200:

Standard	Requirement Number
CIP-002	R1
CIP-003	R4

Comment Form – Cyber Security Standards CIP-002 through CIP-009

	R5
	R6
CIP-005	R1.1
	R1.2
	R1.3
	R1.4
	R1.5
	R2.3
	R2.4
	R2.5
	R3.1
	R3.3
CIP-006	R1
	R1.4
	R7
CIP-007	R1
	R6.1
	R6.2
	R6.3
	R7
	R8
CIP-008	R1.1
	R1.2
	R1.5
CIP-009	R4

Question 4: Do you have any additional comments on CIP-002 through CIP-009?

Yes

No

If yes, please share those comments below.

Comments

1. The IESO believes there is an unnecessary complexity that exists in the levels of non-compliance.

-
2. The Standard seems to be more process oriented as opposed to goal oriented.