Unofficial Comment Form
Request for Comments Regarding the Draft of CIP Cyber Security Standards Version 5

Comment Form A
CIP-002 and CIP-003 Questions

Please DO NOT use this form to submit comments. Please use the electronic comment form to submit comments on the second formal posting of Project 2008-06 – CSO706 Version 5 CIP Standards. The electronic comment form must be completed by May 21, 2012.

2008-06 Project Page

If you have questions please contact Steven Noess at steven.noess@nerc.net or 404-446-9691.

Background
The Project 2008-06 Standard Drafting Team (SDT) is seeking industry feedback and suggestions on this Version 5 of the CIP Cyber Security Standards and its Implementation Plan. The industry feedback will be considered by the SDT in revising and refining Version 5 and related documents.

The SDT thanks stakeholders and other commenters for the extensive and thoughtful comments received during the previous posting period. The volume and quality of the comments provided significant input into many of the changes the team made in response. The SDT also thanks the many observers who attended several comment resolution and discussion sessions—both electronically and face-to-face—that the SDT conducted to prepare the drafts that are currently posted.

The SDT expended considerable work in reviewing, discussing, and responding to all of these inputs, and it believes that the major issues from these inputs have been addressed responsively in this posted draft CIP Version 5 package. As a result, the changes have been significant and substantive in all of the draft CIP Version 5 standards and Implementation Plan.

- Many entities expressed concern over the expanded scope of these standards. The SDT has drafted these standards in response to directives from FERC Order No. 706, and believes that the changes in CIP Version 5 are necessary to address all of those directives responsively. The number of requirements in Version 5 is not substantively higher than previous versions.

- There are many substantive changes in the Applicability section of the standards in response to concerns regarding Distribution Providers and Load Serving Entities. The changes ensure that only those systems owned by those functional entities that are material to BES reliability are within the scope of these standards.
• The SDT also made several substantive changes in CIP-002-5 to address stakeholders’ preference for a facilities-based approach to the identification and categorization process for BES Cyber Systems and BES Cyber Assets. In addition, in response to concerns to overall reliability in the restoration facilities area, the SDT made substantive changes to the categorization of those facilities. The SDT made several changes in response to comments in the “bright-line” criteria in Attachment 1 as well.

• In standards CIP-003-5 through CIP-011-1, the SDT made substantive changes in the applicability of requirements to the medium impact category in response to concerns of practical application in field assets. The SDT also addressed many of concerns on requirement clarity and language in the standards. In addition, the SDT moved all low impact requirements and grouped them as policy/program requirements in CIP-003 (Security Management). Requirements in CIP-004-CIP-011 only apply to high and medium impact systems.

• In response to comments, the SDT extended the Implementation Plan’s effective date to 24 months after approval in most cases, with up to 36 months for implementation for low impact systems. In addition, the initial required performance of those requirements with periodicity is moved into the Implementation Plan and removed from the requirements in the standards, since the initial performances are one-time requirements tied to the effective date.

In summary, the SDT believes this posting package addresses all of the substantive issues received from the comments and various other inputs.

The Project 2008-06 – Cyber Security Order 706 SDT was appointed by the NERC Standards Committee on August 7, 2008 to review each of the CIP reliability standards and develop the modifications necessary to address the directives in the FERC Order No. 706. Please see the Project 2008-06 background document that accompanies the other posted material.

Instructions:
The SDT is providing this form for industry participants to offer their comments on draft 2 of Version 5 of the CIP Cyber Security Standards.

Questions that ask for a “yes” or “no” response are separated from questions that ask for a narrative response. The drafting team considers each comment received irrespective of whether that comment accompanies a “yes” or “no” response to a particular question or is associated with an “affirmative” or “negative” ballot.

For each question that you provide a comment, please provide specific suggestions that would eliminate or minimize any concerns you have with the item in question. A comment or response to every question is not required.
**VERY IMPORTANT:**
Please note that the official comment form does not retain formatting (even if it appears to transfer formatting when you copy from the unofficial Word version of the form into the official electronic comment form). If you enter extra carriage returns, bullets, automated numbering, symbols, bolding, italics, or any other formatting, that formatting will not be retained when you submit your comments. Therefore, if you would like to separate portions of your comment by idea, e.g., the drafting team requests that each distinct idea in the same comment block be prefaced with (1), (2), etc., instead of using formatting such as extra carriage returns, bullets, automated numbering, bolding, or italics.

**A. CIP-002 and CIP-003 Questions:**

1. Requirement R1 of draft CIP-002-5 requires the identification of high and medium impact BES Cyber Systems as described in Attachment 1. Further, it requires a Responsible Entity to review (and update as needed), the required identification within 60 calendar days of when a change to BES Elements or Facilities is placed into operation, which is planned to be in service for more than 6 calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category. Do you agree with the proposed Requirement R1?
   - ☐ Yes
   - ☑ No

2. Requirement R2 of draft CIP-002-5 states, “The Responsible Entity shall have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once each calendar year, not to exceed 15 calendar months between approvals, even if it has no identified items in Requirement R1, Parts 1.1, 1.2, or 1.3.” Do you agree with the proposed Requirement R2?
   - ☐ Yes
   - ☑ No

3. CIP-002-5: If you disagree with the changes made to CIP-002-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

   Comments: Request clarification on the Applicability of Distribution Providers (DP) and Load Serving Entities (LSE).

   1. Does 4.1.2 mean that any DPs owning assets in 4.2.2 need to comply with these CIP Standards?
   2. Does 4.1.6 mean that LSEs owning assets in 4.2.1 need to comply with these CIP Standards?
3. Does 4.2.2 mean that only these DP assets are covered by these CIP Standards?

4. Does 4.2.1 mean that only these LSE assets are covered by these CIP Standards?

5. Does the DP’s third bullet in 4.2.2 apply to only protection systems, not UFLS or UVLS since those load shedding systems are covered by the DP’s first bullet? Note the NERC definition of “protection systems” includes load shedding systems, which generates this last question.

6. Section 4.2 should explicitly state that UFLS Systems that perform automatic load shedding of less than 300 MW are specifically excluded.

   Request clarification on High Impact 1.3 and 1.4’s use of “associated data centers”. Are these the “computer rooms” that service a Control Center?

   Request clarification on the Standard Drafting Team (SDT) expectations on Medium Impact 2.1. Does the SDT expect that the “aggregate highest rate net Real Power capability of the preceding 12 months” will not flip flop on this threshold? In other words, does the SDT expect these asset to remain on one side or the other of this threshold?

   Recommend a change to R1’s VSLs since Lower and Severe use 100 or more High and Medium BES Cyber Systems while moderate and High uses BES Cyber Assets. Request clarification and consistency. Recommend BES Cyber Assets so that ISOs can easily hit their thresholds.

   Requirement 1.2 of CIP-002-5 should be revised to use the same language as Attachment 1. The wording presently reads:

   “Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria; “

   Suggested rewording:
   Identify each high impact BES Cyber System and its associated BES Cyber Asset(s) used BY AND LOCATED AT the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;

   Requirement 1.3 of CIP-002-5 should be revised to use the same language as Attachment 1. The wording presently reads:
“Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) used for the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;”

Suggested rewording:
Identify each medium impact BES Cyber System and its associated BES Cyber Asset(s) ASSOCIATED WITH the Facilities, Systems, or equipment identified in Requirement R1 Part 1.1 according to the criteria contained in CIP-002-5, Attachment 1 – Impact Rating Criteria;

4. CIP-003-5 R1 states “Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall implement one or more documented cyber security policies that address the following topics;” and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R1?

☑ Yes
☐ No

5. CIP-003-5 R2 states “Each Responsible Entity for its BES Cyber Systems not identified as high impact or medium impact shall implement one or more documented cyber security policies to address the following topics;” and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2?

☑ Yes
☐ No

6. CIP-003-5 R3 states “Each Responsible Entity shall identify a CIP Senior Manager by name.” Do you agree with the proposed Requirement R3?

☑ Yes
☐ No

7. CIP-003-5 R4 states “Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals.” Do you agree with the proposed Requirement R4?

☑ Yes
☐ No
8. CIP-003-5 R5 states “Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate and the date of the delegation, and approved by the CIP Senior Manager.” Do you agree with the proposed Requirement R5?

☐ Yes
☒ No

9. CIP-003-5 R6 states “Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegations within thirty calendar days of the change. Delegation changes do not need to be reinstated with a change to the delegator.” Do you agree with the proposed Requirement R5?

☐ Yes
☒ No

10. CIP-003-5: If you disagree with the changes made to CIP-003-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments: Recommend changing M5 from “signed” to “approved” since some companies use other approval processes. Also these Measures criteria need to be aligned with the Requirements. Measure M5 includes “to approve or authorize specifically identified items” while R5 states “and approved by the CIP Senior Manager”.

Request a re-written M6 since it appears to add a new Requirement--“that within 30 days of discharging the delegated authority”.

Recommend updating CIP-003 R2’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures show R2 as “low”.
