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

Comment Form D
Definitions and Implementation Plans

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.

D. Definitions and Implementation Plan Questions:

1. Do you agree with the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset?
   - Yes
   - No

2. Do you agree with the proposed definition of Control Center?
   - Yes
   - No

3. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager?
   - Yes
   - No

4. Do you agree with the proposed definitions of Physical Access Control Systems and Physical Security Perimeter?
   - Yes
   - No

5. Do you agree with the proposed definitions of Electronic Access Control or Monitoring Systems, Interactive Remote Access, and Intermediate Device?
   - Yes
   - No
6. Do you agree with the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset?

☐ Yes
☒ No

7. Do you agree with the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident?

☐ Yes
☒ No

8. Definitions: Do you have any comments on the changes to the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset? If you voted “negative” on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an “affirmative” vote.

Comments: For clarity, suggest changing the BES Cyber Asset definition from "it is directly connected to a Cyber Asset within an ESP" to "it is directly connected to a network, or to a Cyber Asset within an ESP".

9. Definitions: Do you have any comments on the changes to the proposed definition of Control Center? If you voted “negative” on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an “affirmative” vote.

Comments:

10. Definitions: Do you have any comments on the changes to the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager? If you voted “negative” on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an “affirmative” vote.

Comments:

11. Definitions: Do you have any comments on the changes to the proposed definitions of Physical Access Control Systems and Physical Security Perimeter? If you voted “negative” on any ballot
because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an “affirmative” vote.

Comments:

12. Definitions: Do you have any comments on the changes to the proposed definitions of Electronic Access Control and Monitoring Systems, Interactive Remote Access, and Intermediate Device? If you voted “negative” on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an “affirmative” vote.

Comments:

13. Definitions: Do you have any comments on the changes to the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset? If you voted “negative” on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an “affirmative” vote.

Comments: Request clarification on the definition of EAP. Must it be routable protocol on both sides?

14. Definitions: Do you have any comments on the changes to the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident? If you voted “negative” on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an “affirmative” vote.

Comments: The definition of Reportable Cyber Security uses the terms "compromised" and "disrupted" plus the phrase "reliability tasks of a functional entity". All three need their own definition/clarification.

15. Do you agree with the changes made to the proposed implementation plan since the last formal comment period?

☐ Yes
☒ No
16. Implementation Plan: If you disagree with the changes made to the Implementation Plan since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments: Although the proposed Version 5 Implementation Plan states that “Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan,” there are concerns that need clarification. The concerns refer to the transition from the currently effective Version 3, through Version 4 and finally to Version 5.

Given that (a) the Version 4 Standards and associated Implementation Plan were recently approved by FERC; (b) the proposed Version 5 Implementation Plan contains a minimum 24-month period for enforcement means that there will be a period of time during which Version 4 would be effective; and (c) when Version 4 becomes effective there will be newly identified CAs that will have to be made compliant.

In order to comply with Version 4 requirements, entities will need to allocate funding and resources to perform work necessary to become compliant at newly identified facilities. Much of this work must be performed in anticipation of the enforcement date. Once Version 5 becomes effective, application of the proposed categorization of BES Cyber Systems may very well result in much of the work done for Version 4 compliance being in the end unnecessary.

Request clarification on the Disaster Recovery's "completion of the restoration activities" (top of the clean version's page 5). What event/action/etc. signifies this completion?

17. If you have comments or specific suggestions that you have not been able to provide in response to the previous questions, please provide those comments here. Please provide specific suggestions or proposals for any alternative language.

Comments: Section 5 for CIP-003-5 is the only place that explains how to read the bullets and numbers in the Measures. From the second paragraph of Section 5, "Measures provide examples of evidence to show documentation and implementation of the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence." Request clarification this bullets and numbers explanations applies to the Requirements and Applicability sections of each of CIP-002-5 - CIP-011-1. If this was the SDT's intent, then recommend this clarification be added to Section 5 of each of CIP-002-5 - CIP-011-1.

General comment--recommend that each Requirement’s Part identify that Part’s goal.