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

Comment Form C
CIP-008, CIP-009, CIP-010 and CIP-011

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 responsibly. 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.

C. CIP-008, CIP-009, CIP-010 and CIP-011 Questions:

1. CIP-008-5 R1 states “Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?
   - ☐ Yes
   - ☑ No

2. CIP-008-5 R2 states “Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?
   - ☐ Yes
   - ☑ No

3. CIP-008-5 R3 states “Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?
   - ☐ Yes
   - ☑ No

4. CIP-008-5: If you disagree with the changes made to CIP-008-5 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 EOP-004-2 reference in the R1 Rational. The previous version of EOP-004-2 was not accepted by the industry. What is the plan if future versions of EOP-004-2 are not accepted?

Recommend changing the first bullet in R2 Part 2.1 from “By responding to an actual Reportable Cyber Security Incident;” to “By responding to a Cyber Security Incident” since this covers the Reportable Incidents plus the non-reportable incidents.

Recommend updating R2 Part 2.3 since the existing language does specify a retention period.

Recommend changing R3 Part 3.1 from “Review and update” to “Review and update, as needed,” since some years the Cyber Security Incident response plan will not need updating.

Recommend changing R3 Part 3.3 from “Update the Cyber Security Incident response plan” to “Update, as needed, the Cyber Security Incident response plan”.

For R1.3, and R1.4 wording needs to be added to state that physical security incidents need to be included as well as for Cyber Security Incidents.

5. CIP-009-5 R1 states “Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

☐ Yes
☒ No

6. CIP-009-5 R2 states “Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

☐ Yes
☒ No

7. CIP-009-5 R3 states “Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and
Communication.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

☐ Yes
☒ No

8. CIP-009-5: If you disagree with the changes made to CIP-009-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments: Recommend removing R1 Part 1.5 since this Requirement is forensics and/or Lessons Learned. The priority is Reliability or recovery, forensics. The title of this Standard is Recovery Plans for BES Cyber Systems.

Request clarification on R2 Part 2.2. Is this a media test? Can the test be on a sample BES Cyber System?

Recommend updating the Measure for R2 Part 2.3 to reference an updated Implementation Plan’s Initial Performance of Certain Period Requirements. This Requirement – Part combination is not identified in the existing Periodic Requirements. As requested in the first posting, request removing these bookends from this Measure.

Recommend changing from the reference from “R1.2” to “Part 1.2” in R3 Part 3.4 for correctness.

9. CIP-010-1 R1 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

☐ Yes
☒ No

10. CIP-010-1 R2 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

☐ Yes
☒ No
11. CIP-010-1 R3 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

☐ Yes
☒ No

12. CIP-010-1: If you disagree with the changes made to CIP-010-1 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 of R1 Part 1.1.2. Does “applications” mean “SCADA, EMS, State Estimator, IDC, etc.” instead of “device drivers, DLL, applications included in an operating system or package, etc.”?

Request clarification of R1 Part 1.1.3. Would a version control tool/system (like CVS) demonstrate the custom software’s version?

Request clarification on R1 Part 1.3. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005 and CIP-007?

In R1 Part 1.3, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations.

Recommend removing the 30 day time frame in R1 Part 1.3 that applies to CIP-005 and/or CIP-007. Those Standards should specify their time frames. Recommend that the 30 days apply to only updating the baseline configuration (this Part).

Request clarification on R1 Part 1.4.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007?

In R1 Part 1.4.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations.

Recommend removing R1 Part 1.4.2 because “availability” has not been part of the Requirements in the past, is not a FERC requirement and can be interpreted multiple ways.

In R1 Part 1.5, recommend changing from “Where technically feasible, for each change that deviates from the existing baseline configuration” to “Testing cyber security control, where technically feasible, for each change that deviates from the existing baseline configuration” for clarity.

For R2 Part 2.1, recommend the previous Version 5 words since this updated Part is not understandable.
Request clarification on R3 Part 3.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007?

In R3 Part 3.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations.

Recommend that R3 Part 3.1 start with its purpose – for example, Active vulnerability assessment.

Request clarification on R3 Part 3.2. If this is a paper exercise it should be performed once every 36 months.

Recommend that R3 Part 3.2 start with its purpose – for example, “Perform active vulnerability assessment, where technically feasibly….”.

Recommend that R3 Part 3.3 start with “Perform an active vulnerability assessment, of the new cyber assets prior to business deployment, except for CIP Exceptional Circumstances and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset).”

Recommend updating CIP-010 R1’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures shows R1 as “low”.

Recommend updating CIP-010 R2’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures shows R2 as “low”.

13. CIP-011-1 R1 states “Each Responsible Entity shall implement an information protection program that includes each of the applicable items in CIP-011-1 Table R1 – Information Protection.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

☐ Yes
☐ No

14. CIP-011-1 R2 states “Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

☐ Yes
15. CIP-011-1: If you disagree with the changes made to CIP-011-1 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments: The second paragraphs of R2 Parts 2.1 and 2.2 are the same, Recommend removing them from Parts 2.1 and 2.2, and make a new Part 2.3 for clarity.