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

Please **DO NOT** use this form for submitting comments. Please use the electronic form to submit comments to the revisions to outstanding Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs). The electronic comment form must be completed by **October 10, 2012**.

If you have questions please contact Steven Noess at steven.noess@nerc.net or 404-446-9691. All project-related documents are available on the project page.

**Background Information**
The Project 2008-06 Standard Drafting Team (SDT) is seeking industry feedback on this Version 5 of the CIP Cyber Security Standards and its Implementation Plan for consideration by the SDT in finalizing Version 5 and related documents.

The SDT has carefully considered several thousand pages of formal comments as well as extensive informal stakeholder feedback from drafts 1 and 2 of Version 5 of the CIP Cyber Security Standards. There were, understandably, varied perspectives and suggestions, often including divergent views on how to address the same standard or Requirement. After thorough review of all of the previous feedback, the SDT believes that the set of standards now posted represent significant improvement and incorporation of those viewpoints in such a manner as to reflect the industry’s consensus position. The SDT encourages stakeholders to read the General Summary Consideration of Comments as it provides a high level overview of the feedback and the efforts the team has made to incorporate stakeholder viewpoints to produce a quality set of consensus standards.

The SDT thanks you for your continued participation and interest in the development of Version 5 of the CIP Cyber Security Standards. At this stage of the development process, the SDT has considered several very specific alternatives to almost all requirements and proposed definitions. In each case, the SDT thoroughly considered proposed changes and evaluated them carefully by considering several important variables, such as, but not limited to, whether such changes were in the interest of cyber security and reliability, whether they would improve or reduce consensus, whether they had unintended consequences for other types of entities, and whether they were in support of the SDT’s obligation to respond to directives in FERC Order No. 706.

**Instructions:**
At this point, the SDT believes that the industry has made a significant investment in improving the CIP Version 5 standards, and the drafting team has done its best to be responsive to all inputs, recognizing that it is not possible to adopt every suggestions and also recognizing the considerable diversity of entities and assets to which the standards will apply. Therefore, in response to the brief questions below, please limit your comments to those topics or issues for which a change would be essential as a
condition to change your vote to an affirmative vote. Also, please refrain from providing duplicates of
detailed comments that have already been provided in response to draft 1 and draft 2 (you may simply
say “See comments on draft 2.”)

**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.

**Questions:**

1. If, after reviewing the posted standards and General Summary of Consideration of Comments, you
do not support one or more of the 10 standards, the implementation plan or set of definitions,
please indicate the specific item you do not support (the standard and Requirement number,
specific defined term, or implementation plan) and the specific reason you cannot support it here.

   **Comments:** We support these 10 Standards, the Implementation Plan and the
   set of Definitions but have the following comments

   For clarification, suggest adding “mimic display” to the second paragraph of
   CIP-007 R5 Rationale, resulting in “Interactive user access does not include
   read-only information access in which the configuration of the Cyber Asset
cannot change (e.g. front panel displays, web-based reports, mimic
   displays etc.).”

   CIP-008 R1 Part 1.2 requires reporting to the ES-ISAC which may not
   acceptable to the Canadians. Recommend new words that are acceptable to
   the Canadians.

   For consistency, recommend changing CIP-008 R2 Part 2.1 from “at least once
   every calendar year, not to exceed 15 months” to “at least once every 15
   calendar months”

   For clarity, recommend changing CIP-009 R1 Part 1.5 from
   “One or more processes to preserve data for determining the cause of a Cyber
   Security Incident that triggers activation of the recovery plan(s), per device
   capability. Data preservation should not impede or restrict recovery.” to “One
or more processes, per device capability, to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), except where data preservation impedes or restricts recovery."

2. If you have a brief comment you would like to provide that has not already been provided among the previously submitted feedback in response to draft 1 and draft 2, please provide it here. Please limit your comment to 200 words or less.

Comments: