Unofficial Comment Form
Project 2014-02 CIP Version 5 Revisions - Cyber Security Standards

Please DO NOT use this form for submitting comments. Please use the electronic form to submit comments on the proposed draft CIP standards. The electronic comment form must be completed by 8 p.m. Eastern, July 17, 2014.

All documents and information about this project are available on the project page. If you have questions please contact Marisa Hecht at marisa.hecht@nerc.net or by telephone at 404-446-9620 or Ryan Stewart at ryan.stewart@nerc.net or by telephone at 202-644-8091.

Background Information

On November 22, 2013, FERC issued Order No. 791, Version 5 Critical Infrastructure Protection Reliability Standards. In this order, FERC approved version 5 of the CIP standards, and also directed that NERC make the following modifications to those standards:

1. Modify or remove the “identify, assess, and correct” language in 17 CIP version 5 requirements.
2. Develop modifications to the CIP standards to address security controls for Low Impact assets.
3. Develop requirements that protect transient electronic devices.
4. Create a definition of “communication networks” and develop new or modified standards that address the protection of communication networks.

FERC directed NERC to submit new or modified standards responding to the directives related to the “identify, assess, and correct” language and communication networks by February 3, 2015, one year from the effective date of FERC Order No. 791. FERC did not place any time frame for NERC to respond to the Low Impact and transient electronic devices directives.

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.
Questions

1. The Standard Drafting Team (SDT) developed objective criteria in the processes in CIP-003, Requirement R2 to address the directive in FERC Order No. 791. Do you agree with the approach to meeting this directive? If not, please offer suggested revisions.

Yes:
No: X

Comments: We recommend common control objectives. Language inconsistencies create confusion and compliance risks. Here are some examples:

Example 1 – Request a definition (CIP-003-6 Rationale R2 and Part 2.4) of “external routable protocol paths” so that Entities and Auditors clearly understand the differences with External Routable Connectivity. We recommend avoiding the earlier CIP-001 confusion between Facilities and facilities. We believe “external routable protocol paths” creates a similar interpretation risk.

Example 2 – security awareness (Part 2.6) is more stringent than the High / Medium in CIP-004-6 R1

Example 3 - the Low Incident Response Plan in Part 2.5 is inconsistent with High / Medium Incident Response Plan in CIP-008-5 R2

Example 4 – policy requirements for Low Impact creates different set of Requirements for Entities with Low, Medium or High.

There are inconsistencies in the language of this requirement, which causes confusion to entities. Why is LOW impact rating requirements addressed in this standard versus in the applicable standards such as for High & Medium impact ratings? Example: the security awareness should be addressed in CIP 004 as it is for High & Medium.

Whether the all-in-one requirement approach or the spreading out into all the standards approach is taken, the most important thing is that there is consistency between the standards and requirements and maintaining the tiering of activities to the risk.

2. The SDT developed CIP-006, Requirement R1, Part 1.10 and revised CIP-007, Requirement R1, Part 1.2 to meet the directive in FERC Order No. 791 to address protections for nonprogrammable components of communication networks. Do you agree with the approach to meeting this directive? If not, please offer suggested revisions.

Yes: X
No:
Comments: Request CIP-007 R1 Part 1.2 Rationale be added to the Guidelines and Technical Basis section.
Suggest illustrative examples be included in the Measures and Technical Guidelines so that entities and auditors have the same interpretation.

3. The SDT developed CIP-010, Requirement R4 and revised CIP-004, Requirement R1, Part 2.1.9 to meet the directive in FERC Order No. 791 to address transient devices (Transient Cyber Assets and Removable Media). Do you agree with the approach to meeting this directive? If not, please offer suggested revisions.
   Yes: X
   No: 
   Comments:

4. The SDT proposed new definitions for Transient Cyber Assets and Removable Media and revised definitions for BES Cyber Asset and Protected Cyber Assets. Do you agree with the new and revised definition? If not, please offer suggested revisions.
   Yes: X
   No: 
   Comments:

5. The SDT removed the Identify, Assess, and Correct (IAC) language from 17 requirements to meet the directive in FERC Order No. 791 to remove or modify the IAC language. Do you support this revision approach? If not, why not and what alternative approach do you recommend?
   Yes: X
   No: 
   Comments: How does NERC intend to address an internal controls program? What is the time line?
   Refer to the comment for Question 8.

6. The Implementation Plan uses the existing effective date of the FERC approved CIP V5 Standards for CIP-003-6 Requirement R2 and provides additional time for compliance for CIP-006-6, Requirement R1, Part 1.10; CIP-007-6, Requirement R1, Part 1.2; and CIP-010-2, Requirement R4. Are the timeframes reasonable and appropriate? If not, please explain.
   Yes: 
   No: X
   Comments: Request a clear, concise table of all proposed Implementation Plan updates. Ensure that all new effective and mandatory dates are after their CIP V5 dates.
The current format is confusing. Please provide a clear and consistent time line for implementation of these requirements.

7. Are there any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

Yes:
No: X

Comments:

8. Do you have input on other areas, within the scope of the Standards Authorization Request, for the standards or implementation plan not discussed in the questions above? If so, please provide them here, recognizing that you do not have to provide a response to all questions.

Yes: X
No:

Comments: More clarity and scenarios should be provided on how RAI and CIP will work together.

The NERC Project 2014-02 CIP Version 5 Revisions Standard Drafting Team should be allowed to help clarify and provide guidance for industry issues and items discovered in the pilots. In particular the following should be addressed by NERC with the SDT representing industry:

1. Transfer Trip: CIP-002-5 R1, ‘transmission stations and substations’ for medium category assets, what some refer to as the “transfer trip” issue.
2. Clarify the term “programmable devices” which is an undefined term open to strongly differing viewpoints.
3. Clarify “effect within 15 minutes” issue and the burden of evidence for proving that something does not exist. Please clarify if diversity vs redundancy can be considered as part of the Entity’s impact assessment (i.e. separate system using a different technology).

Recommend adding “or” to CIP-010 R4 Part 4.1.4 to make this Part consistent with CIP-010 R1 Part 1.1.1.1. Part 1.1.1 requires a baseline of Operating system(s) (including version) OR firmware where no independent operating system exists; while Part 4.1.4 requires Authorization to include Operating system, firmware, and intentionally installed software on Transient Cyber Assets (per Cyber Asset capability). Part 4.1.4 requires Authorization of both Operating System AND Firmware for a transient device while Part 1.1.1 requires baseline of Operating System OR firmware. We suggest the proper approach is to retain the OR. When applying R4 to a laptop we normally record the OS and version and not look to the firmware BIOS.