Unofficial Comment Form

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

# 

Please **DO NOT** use this form to submit comments. Please use the [electronic comment form](https://www.nerc.net/nercsurvey/Survey.aspx?s=974b41b61f384dd89d74ca3195c3447d) to submit comments on the first formal posting of Project 2008-06 – CSO706 Version 5 CIP Standards. The electronic comment form must be completed by **January 6, 2012.**

[2008-06 Project Page](http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_Version_5_CIP_Standards_.html)

If you have questions please contact Steven Noess at [steven.noess@nerc.net](mailto:steven.noess@nerc.net) or 404-446-9691.

**Background**

In 2008, FERC Order No. 706 directed the ERO to develop modifications to Version 1 of the NERC CIP Cyber Security Standards to address a range of concerns in various areas of the Version 1 standards.

A Standards Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the [FERC Order No. 706](http://www.nerc.com/files/Order_706.pdf). The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order No. 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90 days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order No. 706 directives. An original draft version of CIP-010 and CIP-011, which included the categorization of cyber systems in CIP-010 and associated cyber security requirements consolidated into a single CIP-011, were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT developed a limited scope of requirements in Version 4 of the CIP Cyber Security Standards (CIP-002-4 through CIP-009-4) as an interim step to address the more immediate concerns raised in FERC Order No. 706, paragraph 236, especially those associated with CIP-002’s identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period.

This draft Version 5 of the NERC CIP Cyber Security Standards is intended to address the remaining standards-related issues of FERC Order No. 706.

The SDT believes the NERCVersion 5 CIP Cyber Security Standards provide a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

#### Standard CIP-002-5 requires the categorization of these BES Cyber Systems according to bright-line criteria that characterize their impact on the BES Reliability Operating Services they support to ensure the reliable operation of the Bulk Electric System. These BES Reliability Operating Services are based on the Reliability Functions provided by these applicable Responsible Entities’ Functional Registration. The “bright-line” criteria contained in Attachment 1 – Impact Categorization of BES Cyber Assets and BES Cyber Systems of the draft CIP-002-5 standard provide the basis of the categorization.

* CIP-003-5 through CIP-009-5, CIP-010-1, and CIP-011-1 in the Version 5 CIP Cyber Security Standards define the cyber security requirements to be applied to the BES Cyber Systems according to the categorization performed in CIP-002-5.
* CIP-003 through CIP-009 generally follow the organization of Versions 1 through 4 of CIP-003 through CIP-009.
* CIP-010-1 is a new standard that contains the Configuration Management and Vulnerability Assessment requirements previously defined across several CIP standards in Versions 1 through 4.
* CIP-011-1 is a new standard that defines Information Protection and Media Sanitization requirements previously defined across many standards in Versions 1 through 4.

The Implementation Plan for Version 5 CIP Cyber Security Standards describes the proposed effective dates for Version 5 CIP Cyber Security Standards.

The Team 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 is providing this form for industry participants to offer their comments on this posted draft of Version 5 of the CIP Cyber Security Standards.

For each question, please indicate whether or not you agree with the modification being proposed. If you disagree with the proposed modification, please explain why you disagree and provide as much detail as possible regarding your disagreement including any suggestions for altering the proposed modification that would eliminate or minimize your disagreement. The SDT would appreciate responses to as many of these questions as you are willing to supply.

**You do not have to answer all questions. Enter all comments in Simple Text Format.**

**Questions**

1. Many definitions in the Definitions document contain modified definitions from existing terms and new definitions for terms used in these standards. Do you have any suggestions that would improve the proposed definitions? If so, please explain and provide specific suggestions for improvement.

Yes

No

Comments:

1. CIP-002-5 Attachment 1 contains criteria that provide the basis for the categorization of BES Cyber Systems and BES Cyber Assets. Most of these criteria are similar to those already approved by the industry as part of Version 4. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

Yes

No

Comments:

1. Requirement R1 of draft CIP-002-5 states, “Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I* – *Impact Categorization of BES Cyber Assets and BES Cyber Systems.* All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification.” Further, part 1.1 of R1 states “Update the identification and categorization within 30 calendar days of a change to BES Elements and Facilities is placed into operation, that is intended to be in service for more than 6 calendar months and that causes a change in the identification or categorization of the BES Cyber Assets or BES Cyber Systems from a lower to a higher impact category.” Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

Yes

No

Comments:

1. Requirement R2 of draft CIP-002-5 states, “The Responsible Entity shall have its CIP Senior Manager or delegate approve the identification and categorization required by R1 initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between approvals, even if it has no identified High or Medium BES Cyber Assets or BES Cyber Systems.” Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

Yes

No

Comments:

1. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-002-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

No

Comments:

1. CIP-003-5 R1 states “Each Responsible Entity shall identify, by name, a CIP Senior Manager.” Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

Yes

No

Comments:

1. CIP-003-5 R2 states “Each Responsible Entity shall implement one or more documented cyber security policies that represents the Responsible Entity’s commitment to the protection of its BES Cyber Systems and addresses the following topics:” and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

Yes

No

Comments:

1. CIP-003-5 R3 states “Each Responsible Entity shall review each of its cyber security policies and obtain the approval of its CIP Senior Manager, initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews and between approvals.” Do you agree with the proposed Requirement R3? If not, please explain why and provide specific suggestions for improvement.

Yes

No

Comments:

1. CIP-003-5 R4 states “Each Responsible Entity shall make individuals who have access to BES Cyber Systems aware of elements of its cyber security policies appropriate for their job function.” Do you agree with the proposed Requirement R4? If not, please explain why and provide specific suggestions for improvement.

Yes

No

Comments:

1. CIP-003-5 R5 states “The CIP Senior Manager shall be responsible for all approvals and authorizations required in the CIP standards. The CIP Senior Manager may delegate the authority for any approvals and authorizations required in the CIP standards with the exception of the approval of the Cyber Security Policy required in CIP-003-5 R3. The authority for subsequent delegations may also be delegated. These delegations shall be documented (by position or name of the delegate), dated, and approved and shall specify the authority that is being delegated.” Do you agree with the proposed Requirement R5? If not, please explain why and provide specific suggestions for improvement.

Yes

No

Comments:

1. CIP-003-5 R6 states “Changes to the CIP Senior Manager and any delegations shall be documented within thirty calendar days of the change.” Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

Yes

No

Comments:

1. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-003-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

No

Comments:

1. CIP-004-5 R1 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-004-5 Table R1 – Security Awareness Program*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-004-5 R2 states “Each Responsible Entity shall have a role-based cyber security training program for personnel who need authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in *CIP-004-5 Table R2 – Cyber Security Training Program*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-004-5 R3 states “Each Responsible Entity shall implement its documented cyber security training program for each individual needing authorized electronic or unescorted physical access that includes each of the applicable items in *CIP-004-5 Table R3 -* *Cyber Security Training.”* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-004-5 R4 states “Each Responsible Entity shall have one or more documented personnel risk assessment programs for individuals needing authorized electronic or unescorted physical access that collectively includes each of the applicable items in *CIP-004-5 Table R4 – Personnel Risk Assessment Program*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-004-5 R5 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable elements in *CIP-004-5 Table R5* – *Personnel Risk Assessment.”* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-004-5 R6 states “Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in *CIP-004-5 Table R6* – *Access Management Program.”* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-004-5 R7 states “Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in *CIP-004-5* *Table R7 – Access Revocation*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-004-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

No

Comments:

1. CIP-005-5 R1 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-005-5 Table R1 – Electronic Security Perimeter*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-005-5 R2 states “Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in *CIP-005-5 Table R2 – Remote Access Management*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-005-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

No

Comments:

1. CIP-006-5 R1 states “Each Responsible Entity shall implement one or more documented physical security plans that include each of the applicable items in *CIP-006-5 Table R1 – Physical Security Plan*.*”* The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-006-5 R2 states “Each Responsible Entity shall implement its documented visitor control program that includes each of the applicable items in *CIP-006-5 Table R2 – Visitor Control Program.*” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-006-5 R3 states “Each Responsible Entity shall implement one or more documented maintenance and testing programs that collectively include each of the applicable items in *CIP-006-5 Table R3 – Maintenance and Testing Program*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-006-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

No

Comments:

1. CIP-007-5 R1 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-007-5 R2 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-007-5 R3 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R3 – Malicious Code Prevention*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-007-5 R4 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R4 – Security Event Monitoring*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-007-5 R5 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-007-5 Table R5 – System Access Controls*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-007-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

No

Comments:

1. CIP-008-5 R1 states “Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – BES 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-008-5 R2 states “Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 Table R2 –BES 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-008-5 R3 states “Conduct sufficient reviews, updates and communications to verify the REs response plan’s effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-008-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

No

Comments:

1. 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-009-5 R2 states “Each Responsible Entity shall implement one or more processes that collectively address 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-009-5? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

No

Comments:

1. 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP010-1 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. 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 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-010-1? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

No

Comments:

1. CIP-011-1 R1 states “Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in *CIP-011-5 Table R1 – Information Protection*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. CIP-011-1 R2 states “Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-011-5 Table R2 – Media Reuse and Disposal*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2 and its parts? If not, please explain why and provide specific suggestions for improvement with reference to the appropriate main requirement or part number.

Yes

No

Comments:

1. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels for CIP-011-1? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Yes

No

Comments:

1. Do you agree with the proposed implementation plan? If so, please explain and provide specific suggestions for improvement.

Yes

No

Comments: