

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2014-02 CIP Version 5 Revisions

Consideration of Comments
Additional Comment Period

October 28, 2014

RELIABILITY | ACCOUNTABILITY



Table of Contents

Table of Contents	2
Consideration of Comments: Project 2014-02 CIP Version 5 Revisions.....	3
Introduction.....	4
Background	4
Question 6: Version X	5
Support IAC Removal but Comments on Zero Tolerance and Lows	5
Expectations for RAI and its Fulfillment of the IAC Intent	6
Does Not Support Removal	6
Completing Revisions to all Four Directive Areas	6
Question 7: Other Areas Within SAR.....	7
Communication Networks	7
Version X.....	7
General.....	7

Consideration of Comments: Project 2014-02 CIP Version 5 Revisions

The Project 2014-02 Drafting Team thanks all commenters who submitted comments on the Critical Infrastructure Protection Version 5 standards. The standards were posted for a 45-day public comment period from September 3, 2014 through October 17, 2014. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 70 responses, including comments from approximately 164 different people from approximately 117 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

This consideration of comments is responding to the comments received on the standards and implementation plan balloted as Version X, which was posted for a 45-day comment period and ballot. There was a concurrent 45-day comment period and ballot for CIP-003-6 and CIP-010-2, which included revisions to address the low impact and transient device directives. The response to the comments received regarding those revisions will be posted when the revisions are posted for an additional comment period and ballot.

All comments submitted may be reviewed in their original format on the standards' [project page](#).

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Director of Standards, Valerie Agnew, at 404-446-2566 or at valerie.agnew@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.¹

¹ The appeals process is in the Standard Processes Manual: http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

Introduction

The SDT appreciates industry comments on the revisions to the CIP Reliability Standards. During the development of the revised standards prior to posting, the SDT made it a priority to conduct outreach as modifications were made to the standards. The SDT conducted one face-to-face meeting to revise the standards, Implementation Plan, Violation Risk Factors (VRFs), and Violation Severity Levels (VSLs) in order to appropriately consider all comments received. The SDT continues its rigorous conference call schedule as it understands the importance of getting these standards to steady state.

Background

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” (IAC) language in 17 CIP version 5 requirements.
2. Develop modifications to the CIP standards to address security controls for to assets containing low impact BES Cyber Systems.
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 IAC language and communication networks by February 3, 2015, one year from the effective date of Order No. 791. FERC did not place any time frame for NERC to respond to the low impact and transient electronic devices directives. The purpose of the proposed project is to address the directives from FERC Order No. 791 to develop or modify the CIP standards.

Question 6: Version X

6. *The results of the initial CIP V5 Revisions ballot showed industry support for the new Communication Networks requirements and the removal of the Identify, Assess, and Correct (IAC) language from 17 requirements. These two directive areas have a FERC filing deadline of February 3, 2015. Meanwhile, the CIP-003-6 and CIP-010-2 revisions proposed to address the Low Impact and Transient Devices directives did not pass initial ballot.*

In order to separate approval of the IAC and Communication Networks revisions from the Low Impact and Transient Device revisions where they occur within the same standard, the relevant standards are posted separately. This separate posting provides additional options to meet the FERC filing deadline of February 3, 2015 in the event Low Impact or Transient Device revisions do not obtain industry approval in the current ballot. (Please see explanatory document on the CIP Version 5 Revisions project page for more information)

Do you support removal of the IAC language from the 17 Requirements across CIP Version 5 Standards? If not, please explain why.

Many commenters expressed support for the removal of the IAC language through a 'yes' response to Question 6 without any additional comments. Those commenters include American Transmission Company LLC, FirstEnergy, Tennessee Valley Authority, Northeast Power Coordinating Council, Dominion, MRO NERC Standards Review Forum, Duke Energy, Iberdrola USA, PJM Interconnection LLC, Edison Electric Institute, Oncor, Arizona Public Service Company, Encari, Luminant Generation Company, LLC, ATCO Electric, Idaho Power, Manitoba Hydro, Independent Electricity System Operator, Texas Reliability Entity, Entergy Services, Inc., Southern California Edison Company, Pepco Holdings Inc., Hydro-Quebec Production, Kansas City Power & Light, Consumers Energy Company, NV Energy, Massachusetts Municipal Wholesale Electric Company, and Tri-State Generation and Transmission Association, Inc.

Support IAC Removal but Comments on Zero Tolerance and Lows

Florida Municipal Power Agency (FMPA), BC Hydro, Indiana Municipal Power Agency (IMPA), and ACES Standards collaborators supported the removal of the IAC language but expressed concern over zero tolerance requirements. While the removal of the IAC language returns the requirements to a zero tolerance construct, NERC is implementing risk-based compliance monitoring and enforcement processes to address the zero tolerance concerns. The SDT will forward concerns raised with compliance and enforcement to the relevant NERC departments. In response to IMPA, NERC is making an informational filing with FERC regarding the risk-based Compliance Monitoring and Enforcement Program on or about October 31, 2014. In response to ACES Standards collaborators, the risk-based compliance monitoring and enforcement processes will all be implemented by January 1, 2015.

Calpine agrees with removing IAC from the standards for high and medium impact categories but recommended keeping IAC for the low impact category. In response, Calpine did not further explain its rationale for its recommendation, but the SDT determined that using the IAC language for different classification levels would not appropriately address the FERC directive.

FMPA requested additional clarity in the Reliability Standard Audit Worksheets (RSAWs) as the currently posted RSAWs do not provide enough clarity and guidance on compliance expectations to understand if zero tolerance concerns have been addressed. NERC is reviewing the comments made to the RSAWs. In response, while the removal of the IAC language returns the requirements to a zero tolerance construct, NERC is implementing risk-based compliance monitoring and enforcement processes to address the zero tolerance concerns. The SDT will forward concerns raised with compliance and enforcement to the relevant NERC departments.

Expectations for RAI and its Fulfillment of the IAC Intent

SPP and specific members commented that the RAI program is not complete and has not been used in the audit and enforcement process, and it requires a significant amount of trust. In response, while the removal of the IAC language returns the requirements to a zero tolerance construct, NERC is implementing risk-based compliance monitoring and enforcement processes to address the zero tolerance concerns. Risk-based compliance monitoring and enforcement processes are already in use.

CenterPoint Energy Houston Electric LLC supported this revision approach for IAC. As proposed by NERC, the Company looks forward to the concepts of IAC being implemented within the final framework of the RAI. MISO, Occidental Chemical Corporation, Sacramento Municipal Utility District (SMUD), MidAmerican Energy Company, American Electric Power, and Xcel Energy supported the removal of IAC in the timeframe ordered by FERC and supported the continued work by NERC to develop RAI. In contrast, Rutherford EMC commented that the IAC language provided a more proactive results-based approach to truly identify, assess, and correct problems rather than follow standards. In response to all commenters, for additional information regarding how the concepts of IAC will be implemented within the risk-based compliance monitoring and enforcement framework, please see [The Application of Risk-based Compliance Monitoring and Enforcement Program Concepts to CIP Version 5²](#), available on NERC's RAI web page.

Does Not Support Removal

Nebraska Public Power District (NPPD) and City of Austin d/b/a Austin Energy commented that they do not support the removal of the IAC language. NPPD and Austin Energy went on to suggest that either the requirements containing IAC be removed entirely or to keep the IAC language as is in Version 5. As stated in the prior consideration of comments, the SDT states that FERC approved the security control requirements within Version 5, but found the IAC language related to compliance to the requirements and objected to its inclusion in the requirement itself. The SDT will forward concerns raised with compliance and enforcement to the relevant NERC departments.

Completing Revisions to all Four Directive Areas

Exelon Companies commented that it strongly supports the SDT's efforts to complete revisions in all four directive areas by the February 3, 2015 filing deadline. Similarly, National Rural Electric Cooperative Association (NRECA) supported the Version X package and is hopeful the SDT can successfully complete revisions to CIP Version 5 for the four directive areas by the February 3, 2015 filing deadline. NRECA went on to state that by having the four directive areas addressed by the filing deadline will be critical to achieve a steady-state of NERC CIP standards. In response, the SDT continues its work with the intent of completing revisions responding to all four FERC directive areas.

²[http://www.nerc.com/pa/CI/tpv5impmntnstdy/Public_Final_Application_Risk-Based_CMEP_Concepts_to_CIPV5_\(10-22-2014\).pdf](http://www.nerc.com/pa/CI/tpv5impmntnstdy/Public_Final_Application_Risk-Based_CMEP_Concepts_to_CIPV5_(10-22-2014).pdf)

Question 7: Other Areas Within SAR

7. *Do you have input not discussed in the questions above on other areas relative to the revisions made to the standards or implementation plan since the initial posting and within the scope of the Standards Authorization Request? If so, please provide them here, recognizing that you do not have to provide a response to all questions.*

Some comments from this question will be addressed in a future consideration of comments from the standard drafting team. The responses below only pertain to the revisions in the Version X posting.

Communication Networks

Bonneville Power Administration (BPA) commented that CIP-007-6, Requirement R1, Part 1.2 expands the scope of the requirement to nonprogrammable communication components and suggested that Part 1.2 be revised to align with Part 1.1. In addition, BPA requested additional guidance on the specific nonprogrammable communication components located inside both a Physical Security Perimeter (PSP) and an Electronic Security Perimeter (ESP). The SDT confirms this expands the scope of Part 1.2, but it does so appropriately and in response to the Order No. 791 directive to address the security of nonprogrammable components associated with BES Cyber Systems. CIP-007-6, Requirement R1, Part 1.2 concerns the physical security of computing equipment ports. Nonprogrammable components did not previously meet the definition and applicability for Cyber Assets but they may have the same vulnerability this Requirement Part addresses. The expanded scope closes this gap in protection. In response to the request for additional guidance, the SDT added a diagram to the Guidelines and Technical Basis section of CIP-007-6 to further illustrate the intent behind including components inside both a PSP and an ESP.

FMPA and EEI requested clarification on whether an entity can violate CIP-007-6, Requirement R2, Part 2.3 while still meeting Part 2.4. The SDT appreciates the comment but notes that the SDT did not focus on this requirement during its revisions. However, the SDT notes that CIP-007-5, R2, Requirement 2, Part 2.4 allows an entity to modify an existing mitigation plan that is created in Part 2.3. The Requirement Part language allows for "an extension to the timeframe specified in Part 2.3" and have the extension "approved by the CIP Senior Manager or delegate."

Version X

NRG Energy suggested removing the word "shall" from all the sections in the attachment. The SDT appreciates the comment but notes that the attachments were not included as part of the Version X package. The SDT will respond to this comment along with other comments related to the low impact and transient devices revisions.

General

City of Austin d/b/a Austin Energy commented that the CIP Version 5 standards have been difficult to implement, and it would like the standards to get to steady-state with minimal revisions. The SDT appreciates the comment and notes that its focus was on the four directive areas for these revisions. Furthermore, the SDT continues its work with the intent of completing revisions to get to steady-state.