Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards

**Do not** use this form for submitting comments. Use the [Standards Balloting and Commenting System (SBS)](https://sbs.nerc.net/) to submit comments on the **Virtualization Modifications** by **8 p.m. Eastern, Monday, March 22, 2021.**

**. Eastern, Thursday, August 20, 2015**

Additional information is available on the [project page](http://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx). If you have questions, contact Senior Standards Developer, Jordan Mallory (via email) or at 404-446-2589.

## Background Information

Project 2016-02 (1) addresses the Federal Energy Regulatory Commission (Commission) directives contained in Order No. 822 and (2) considers the Version 5 Transition Advisory Group (V5TAG) issues identified in the CIP V5 Issues for standard drafting team (SDT) consideration (V5TAG Transfer Document).

The V5TAG, which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP Version 5 standards and to support industry’s implementation activities. During the V5TAG’s activities, it identified certain issues with the CIP Reliability Standards that would be better addressed by a SDT for the CIP Reliability Standards. The V5TAG developed the [CIP Version 5 Transition Advisory Group Issues for Consideration](http://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/Transfer_Issues_V5TAG-SDT_1st-final-03232016.pdf) document to formally recommend that the SDT address these issues and consider modifications to the standard language during the standards development process. Among other issues, the V5TAG stated “The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies.”

## SDT Approach

As the SDT investigated these issues, it found that virtualization affects most of the technical definitions used within the CIP Standards from the foundational “Cyber Asset” to the technical CIP standards (CIP-005, CIP-007, and CIP-010 in particular). This is due to virtualization changing fundamental assumptions, such as the standards having an “electronic device” basis, focusing on routable protocol level only, and perimeter-based security. The SDT found virtualization to be not only a driver of change, but a symptom of a larger issue with the standard’s ability to adapt to current and future technology innovation. The SDT concluded these more technical standards could benefit from removing inherent prescription of certain architectures and moving requirements to an objective or results-oriented level that do not make assumptions about architecture. In other words, the standards should not go further and prescribe how to secure today’s newer architectures but should require that certain security objectives be met and “get out of the way” of virtualization and future innovations that can increase reliability, resiliency, and security of our BES Cyber Systems.

The SDT has been addressing these issues and has gathered feedback from stakeholders through conceptual webinars and technical conferences. The SDT has progressed from a general direction of “cyber system orientation and objective-level requirements” to now having the concepts drafted into proposed technical standards (CIP-005, CIP-007, and CIP-010) and conforming virtualization revisions to the remaining CIP standards that are not directly affected by virtualization or technology changes.

As part of the Standard Authorization Request (SAR) for this project, the SDT also reviewed the addition of CIP Exceptional Circumstances (CEC) to new and existing requirements. The SDT determined that CEC could be applied to the following additional requirements, CIP-004-7 R2.2, CIP-004-7 R3.5, CIP-006-7 R1.8, CIP-006-7 R1.9, CIP-006-7 R2, CIP-010-5 R1.2, and CIP-010-5 R1.3.

Additionally, the SDT modified CIP-002 Attachment 1, Criterion 2.1 to align with a previously approved response to a Request for Interpretation (RFI) regarding “shared BES Cyber Systems.” The SDT’s response to the RFI was originally included in Appendix 1 of CIP-002-5.1a. CIP-002, Attachment 1 Criterion 2.1 was modified to align with the previously approved RFI response. The proposed revision to Criterion 2.1 now states that the only BES Cyber Systems that meet criterion 2.1 are each discrete shared BES Cyber System that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

**Summary of Proposed Definition Changes**

The following provides rationale and updates the associated definitions.

|  |  |
| --- | --- |
| Term to be Retired | Rationale for Retirement |
| Electronic Access Point (EAP) | With the proposed revisions of CIP-005-6 Requirement R1 Part 1.2 this definition is no longer required. The isolation concepts in proposed Requirement R1 Parts 1.1, 1.2, and 1.3 address the necessary controls previously defined in the concept of an identified Electronic Access Point. |
| Electronic Security Perimeter (ESP) | This term is proposed for retirement. Isolation concepts are now described in Requirement R1 Parts 1.1, 1.2, and 1.3, to enable virtualization and future technologies. The SDT modified the requirement parts to remove the direct reference to a perimeter model. |

The CIP SDT Proposed new or revised definitions to incorporate virtualization and future technology. The **bullet points below provide rationale** for a number of the definitions. Please see the CIP Definitions document for all new and revised definitions.

* **BES Cyber Asset (BCA)** – This SDT proposes to retain the BCA definition with updates to include the proposed term “Virtual Cyber Asset (VCA).” A BCA consists of a Cyber Asset or VCA that meets the qualifying language of a BCA (15 min impact, etc.).
* **BES Cyber System (BCS)** – The SDT proposes to retain the definition for BCS, with the addition of the acronym “BCS” in the Glossary of Terms used in NERC Reliability Standards (Glossary).
* **BES Cyber System Information (BCSI)** – This term was updated to add Shared Cyber Infrastructure to the scope of information covered within the BCSI definition. The SDT also proposes adding the acronym “BCSI” within the Glossary.
* **CIP Senior Manager** – This term was updated to remove the reference “CIP-002 through CIP-011” from the definition.
* **Cyber Asset** – This term was modified to ensure that Shared Cyber Infrastructure (SCI) is excluded from the Cyber Asset definition. SCI is a proposed term and is identified as a distinct applicable system throughout the CIP Standards.
* **Electronic Access Control or Monitoring Systems (EACMS)** - The SDT proposes revising this term to include applicable VCA and SCI within the definition of EACMS. The proposed revisions replace the retired term Electronic Security Perimeter (ESP) with logical isolation to transition from prescriptive technologies and conform with proposed revisions in CIP-005-8.
* **External Routable Connectivity (ERC)** – This term has been revised to include SCI and VCA. The SDT also removed the reference to ESP and added scoping language within the definition.
* **Interactive Remote Access (IRA)** – The SDT removed the reference to an ESP and added scoping language to scope remote access.
* **Intermediate Systems (IS)** – This term was revised to identify IS as EACMS that are used to restrict Interactive Remote Access (IRA). References to an ESP were removed from the definition.
* **Management Interface** – The SDT proposes adding this new term to the Glossary. A Management Interface is a physical or logical interface of a Cyber Asset or SCI that provides management and monitoring capabilities. This term is referenced as an applicable system throughout the revised standards.
* **Management Module** – The SDT proposes adding this term to the Glossary to identify autonomous subsystems of Cyber Assets or SCI that provides management and monitoring capabilities independently of the host system’s CPU, firmware, and operating system. This term is referenced as an applicable system throughout the revised standards.
* **Management Systems** - The SDT proposes adding this term to the Glossary to define any combination of Cyber Asset or VCA that establish and maintain the integrity of VCA or Cyber Asset through control of the processes for initializing, deploying, and configuring those assets and systems. This definition excludes Management Modules.
* **Physical Access Control Systems** – This term was retained and updated to include SCI.
* **Protected Cyber Asset (PCA)** – This term was retained and updated to specifically exclude SCI.
* **Removable Media** – This term was retained and updated with references to the new term SCI.
* **Reportable Cyber Security Incident** – The SDT revised this term to transition from ESP to logical isolation. The definition was also updated to include compromises or disruptions to SCI of a high or medium impact BCS.
* **Self-Contained Application** – The SDT proposes adding this definition to the Glossary to identify Self-Contained Applications as applicable systems throughout the CIP Standards. Self-Contained Applications are immutable software binaries containing operating system dependencies and application software packaged to execute in an isolated environment.
* **Shared Cyber Infrastructure (SCI)** – The SDT proposes adding this definition to the Glossary to identify electronic devices and their software that share their compute or storage resources with one or more BES Cyber Systems, or their associated EACMS, Physical Access Control Systems (PACS), and Protected Cyber Asset (PCA). The SDT proposes identifying SCI within CIP-002-7 and it is an applicable system throughout the proposed CIP Standards.
* **Transient Cyber Asset (TCA)** – The SDT retained this definition and updated it to include the proposed term VCA. The proposed definition excludes SCI associated with high or medium impact BCS.
* **Virtual Cyber Asset (VCA)** – The SDT proposes adding this definition to the Glossary to identify the logical instance of an operating system or firmware hosted on SCI or a Cyber Asset.

**Summary of CIP-005 Changes**

For a detailed explanation of these changes, please refer to the *CIP-005 Technical Rationale* document.

CIP-005 has been modified to accommodate three major areas:

1. Allow for network security models that are not perimeter-based, such as zero trust models. Perimeter-based models (such as ESP) remain a valid option, but are no longer the prescribed option.
2. Requiring the protection and isolation of the management plane of SCI.
3. Allow for single ESPs or logical isolation methods to span geographic locations by requiring the protection of the data, while keeping the Cyber Assets between the sites out of scope (e.g. carrier’s telecom equipment).

**Summary of CIP-007 Changes**

For a detailed explanation of these changes, please refer to the *CIP-007 Technical Rationale* document.

CIP-007 changes consist primarily of conforming changes that add the new virtualization types including SCI to the scope of applicable systems. It also changes the focus of “ports and services” to the services while still allowing port number’s to be tracked. Port numbers are merely pointers to a service such as SSH, web server, database server, DNP or Modbus server or client, etc. In virtualized environments, the focus moves more to what services are enabled and port numbers take on a lesser role. The language has been modified to reflect this.

**Summary of CIP-010 Changes**

For a detailed explanation of these changes, please refer to the *CIP-010 Technical Rationale* document.

The proposed changes in CIP-010-5 concern the use of several facets of virtualization technologies. Virtualization allows for such technologies as new logical isolation controls for SCI, remediation VLANs, parent/child images, dormant virtual machines (VMs), and self-contained applications (containers). Enabling and clarifying the use of these technologies is the basis of the proposed changes in CIP-010-5. CIP-010 Requirement R1 also changes focus from maintaining baseline configurations to authorizing change to an expanded list of configuration attributes that are used to secure virtualized environments.

**Summary of Conforming Changes**

For a detailed explanation of these changes, please refer to the *Technical Rationale* document for CIP-002, CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013. The conforming changes to all standards are primarily to add the new term SCI to the scope of requirements throughout the standards. The SDT also replaced TFE’s with the “per system capability” language, updated the Exemption Section in each standard to conform to the CIP-005 changes above. Also, any prescriptive references to ESP’s have been removed per the CIP-005 discussion above.

## Questions

1. The SDT added, revised, and retired several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. CIP-005 Requirement R1 part 1.1 was revised to permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. The SDT modified CIP-005 Requirement R1 Part R1.2 to establish logical isolation requirements for Management Systems, Management Interfaces, and associated SCI. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. The SDT modified CIP-005 Requirement R1 Part1.3 to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters. Does the proposed requirement fulfill the directive from FERC Order 791, paragraph 150? Please provide the basis for your response.

[ ]  Yes

[ ]  No

Comments:

1. The SDT modified CIP-005 Requirement R2 to ensure remote access management requirements align with the new and revised virtualization terms. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. The SDT revised CIP-007 Requirement R1 Part 1.1 to shift the security objective from logical network accessible ports to services. The proposed revisions require Responsible Entities to enable only network accessible services that have been determined to be needed by the Responsible Entity. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. CIP-010 Requirement R1 currently requires Responsible Entities to develop a baseline configuration, authorize changes to the baseline, and document the changes. The SDT proposes to revise Requirement R1 to remove the reference to baseline configurations. The proposed revisions require the authorization of changes to Operating System(s), firmware, commercially available open-source software, custom software, logical network accessible ports, security patches applied, and SCI configurations. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. The SDT modified CIP-010 Requirement R3 Part 3.3 to ensure that vulnerability assessments are performed prior to logically connecting Cyber Assets, VCA, and SCI. The revised requirement allows the use of remediation VLANs to perform active vulnerability assessments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. CIP-002-5.1a includes exemption 4.2.3.2, which exempted Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. In the development of conforming changes, the SDT determined that the exemption should be split into two distinct exemptions to adequately cover all cyber systems associated with conforming changes. The SDT established those conforming changes in proposed Exemptions 4.2.3.2 & 4.2.3.3. Do the changes clearly identify the exempted cyber systems? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. BCS and SCI are mutually exclusive by definition, however SCI poses a significant reliability risk to the Bulk Electric System. The SDT considered the risks associated with SCI and revised CIP-002 Requirement R1 to include the identification of SCI in Parts 1.3, 1.4, and 1.5. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. In the current enforceable standards, there are no requirements that can be used to tie a non-identification of EACMS, PACS, and PCAs to a single requirement. The SDT revised CIP-002 to include the identification of SCI associated with EACMS, PACS, and PCAs to help address this issue within the virtualization scope of the current SAR. The proposed requirement could reduce possible non-compliance to a single issue if a Responsible Entity fails to properly identify SCI associated with EACMS, PACS, or PCAs. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. The SDT modified CIP-002 Attachment 1, Criterion 2.1 to align with a previously approved Request for Interpretation (RFI) regarding “shared BES Cyber Systems.” The SDT modified the criterion to reference each discrete shared BCS. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. The SDT made conforming changes to CIP-003 and CIP-004. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. The SDT modified the Applicable Systems column in CIP-006 to include SCI hosting PACs associated with Medium Impact BCS with ERC or IRA. The SDT made the proposed revisions to clarify the scope of requirements that apply when an entity implements serial IRA. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. The SDT made conforming changes to CIP-008 and CIP-009. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. The SDT modified CIP-011 Requirement R2 part 2.1, which will allow cryptographic erasure in scenarios where BCSI can’t be mapped to particular disks in virtualized storage. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. The SDT performed a review of the CIP Standards and determined that CIP Exceptional Circumstances could be applied to the following additional requirements: CIP-004-7 Requirement R2 Part 2.2, CIP-004-7 Requirement R3 Part 3.5, CIP-006-7 Requirement R1 Part 1.8, CIP-006-7 Requirement R1 Part 1.9, CIP-006-7 Requirement R2, CIP-010-5 Requirement Part 1.2, and CIP-010-5 Requirement R1 Part 1.3. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

[ ]  Yes

[ ]  No

Comments:

1. Implementation Plan: The SDT proposes an Implementation Plan that makes the revised CIP Standards and definitions effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority’s order. However, the implementation plan allows a Responsible Entity to elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. Do you agree with this proposal? If you think an alternate effective date is needed, please provide a detailed explanation of actions and time needed.

[ ]  Yes

[ ]  No

Comments:

1. Please provide any additional comments for the SAR drafting team to consider, if desired.