Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards | Virtualization

**Do not** use this form for submitting comments. Use the [Standards Balloting and Commenting System](https://sbs.nerc.net/) to submit comments on the **Virtualization Updates for CIP-004, CIP-005, CIP-006, CIP-007, CIP-010, and Associated Definitions**. Comments must be submitted by **8 p.m. Eastern, Tuesday, December 18, 2018**

**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 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 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 standard drafting team (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.”

As the SDT investigated these issues, it found that virtualization affects most of the technical definitions used within CIP 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 and focusing on routable protocol level only, 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 is at a point where enough work has been accomplished to post the SDT’s work in progress and get industry feedback on the direction. The SDT has progressed from a general direction of “cyber system orientation and objective-level requirements” to now having many of these concepts drafted into these standards. During this informal comment period, the SDT recognizes that this is a work in progress and is not ready for a formal posting and ballot and is seeking industry feedback on the direction and concepts of these definitions and requirements.

The remaining CIP standards are not directly affected by virtualization or technology changes and the SDT believes only conforming changes will be required in those standards. As part of our Standard Authorization Request, the SDT also addressed the addition of CIP Exceptional Circumstances allowances where needed. Therefore, the SDT is also posting CIP-004 and CIP-006 for three reasons:

* to show what the conforming changes from the SDT’s virtualization work may look like;
* to begin to show how the EACMS split into EACS and EAMS would affect these standards;
* to show the new CIP Exceptional Circumstances additions within these standards.

**Summary of Definition Changes**

The following provides rationale and updates the associated definitions.

| **Term to be retired**  | **Rationale for Retirement**  |
| --- | --- |
| BES Cyber Asset | This term is proposed for retirement and the foundational definition is established at the system level. |
| Electronic Access Control or Monitoring Systems | Term is proposed for retirement and split into two new proposed terms; Electronic Access Control Systems (EACS); and Electronic Access Monitoring Systems (EAMS).  |
| Protected Cyber Asset | This term is proposed for retirement and the concepts of the term are incorporated into the proposed definition of Protected Cyber System (PCS). This change takes advantage of the more objective-based requirements at the system level. |
| Electronic Access Point | With the proposed retirement of CIP-005-6 Part 1.2 this definition is no longer required. The isolation concepts in proposed requirement Part 1.1 address the necessary controls previously defined in the concept of an identified Electronic Access Point. |
| Electronic Security Perimeter  | This term is proposed for retirement. The concepts of the ESP have been incorporated into the definition of a Logical Isolation Zone (LIZ) |

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.

* **Cyber Asset –** The SDT is proposing to retain the Cyber Asset definition with updates to incorporate virtual hardware. With the proposed updates, it is only used in places where it did not make sense to upgrade the term to cyber system. Cyber Asset can be located in the TCA and Removable Media definitions and in a small number of locations in the CIP-010 standard. The goal is to limit the use of ‘Cyber Asset’ to areas where the upgraded term ‘Cyber System does not apply.
* **BES Cyber System –** This term was updated toaccommodate the cyber system concept. The hardware portions of the new definition were incorporated from the Cyber Asset definition and qualifying language (15 mins, etc.) included from the BES Cyber Asset definition. The term no longer relies on the word “programmable” and uses new language to classify devices.
* **EACMS to EACS and EAMS –** To support wider correlation of events and data sharing with government agencies and other security vendors to more quickly detect cyber-attacks, the SDT is proposing to split off cyber systems that do electronic access monitoring but perform no electronic access control. The new terms, EACS and EAMS will allow changes within the applicability for the monitoring portion to allow third party monitoring systems. This allows adjustments to the applicability of requirements that are appropriate to the different risks associated with EACS and EAMS.
* **Physical Access Control System (PACS) –** During the process of evaluating the split in applicability for EACMS the SDT determined that the PACS definition would need the same considerations to ensure consistency for monitoring systems. The alerting and logging definition parts were removed from the definition and moved to a new proposed term, Physical Access Monitoring Systems (PAMS). The SDT is seeking input from industry on whether or not having PACS and PAMS as two separate definitions is a positive path for the future.
* **Logical Isolation Zone (LIZ) –** The SDT is proposing this new term which transitions to a new zone-based protection model to control communications to and from BES Cyber Systems and Protected Cyber Systems taking advantage of advances in cyber security. The SDT intends for this concept to be backwards compatible with the ESP while also being non-prescriptive to the communications protocol and layer of the Open Systems Interconnection (OSI) model in which they are implemented.
* **Physical Security Perimeter (PSP) –** In concert with the changes to EACMS and PACS, the SDT is proposing the removal of the requirement for monitoring systems to be kept inside of a PSP. This change would allow flexibility for security monitoring services to be outsourced where these types of controls are currently not available.

**Summary of CIP-005 Changes**

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

* **ESP transition to Logical Isolation Zone** **–** To accommodate advances in network security that go beyond routable protocol address filtering at perimeters, the SDT is proposing a transition to the zone concept while retaining backward compatibility with ESPs.
* **Super ESP, 4.2.3.2 and 4.2.3.3 Exemptions, and R1.2** **–** As it addresses virtualization, the SDT is concurrently addressing the V5TAG issue known as the “Super ESP,” where BES Cyber Systems may be split across different geographic locations within a single ESP.
* **Management Plane isolation –** Virtualization allows BES cyber systems with a 15 minute impact to share infrastructure with systems that do not share that time constraint (e.g., a control system and its historian). The SDT has added a new requirement (R3) to bring the management plane and its isolation controls into scope of the CIP standards.

**Summary of CIP-007 Changes**

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

* Made conforming changes to applicable systems column: (PCS, EACS, etc.)
* Made conforming changes to ensure the requirements are at the system level (per system capability, remove references to Cyber Asset, etc.)
* Added security objectives to the “Big R” main requirements. Example: Each Responsible Entity shall implement one or more documented process(es) *to mitigate the risk posed by uncontrolled logical and physical connectivity* that collectively include each of the applicable requirement parts in…”
* Modified R1.1 (ports/services) to be more objective oriented. Permits use of east/west IDS, baselining logical connectivity, etc. in addition to documenting required network accessible ports.
* Introduced new requirement for installing only essential software and executable scripts on high and medium impact BES Cyber Systems, EACS, PACS, and PCAs.
* Moved CIP-007 R2 patching requirement to CIP-010 vulnerability management program requirement
* Added CIP Exceptional Circumstances language to apply to all of Requirement 4 (Security Event Monitoring)

**Summary of CIP-010 Changes**

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

* Made conforming changes to applicable systems column (PCS, EACS, etc.)
* Made conforming changes to ensure the requirements are at the system level (per system capability, remove references to Cyber Asset, etc.)
* Added security objectives to the “Big R” main requirements. Example: Each Responsible Entity shall implement one or more documented process(es) *to mitigate the risk posed by insecure system configuration* that collectively include each of the applicable requirement parts in…”
* Removed the requirement to develop a baseline configuration
* Introduced the concept of a secure configuration. This new concept requires the collective identification of the methods used to comply with the security requirements in CIP-005 R1, CIP-007 R1, R2, R3, R4, R5, and CIP-010 R3.
* Replaced prescriptive timeframes with a risk based evaluation for entity determined timeframes.
* Added specification to the configuration monitoring requirement for hash monitoring, configuration monitoring, or configuration auditing.
* Split obligation to investigate detected unauthorized changes to its own requirement part. Added obligation to remediate detected unauthorized changes.
* Moved patch management requirement from CIP-007 to the CIP-010 Vulnerability Management program. Rephrased requirement in terms of identifying and mitigating software vulnerabilities. Added risk-based entity defined timeframes for implementation.
* Added CIP Exceptional Circumstances to apply to testing of changes prior to implementation

## Questions

1. The proposed BCS definition no longer relies on the term Cyber Asset. The SDT asserts that the proposed BES Cyber System definition describes the BCS adequately without the use of the word “programmable” in the definition. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

[ ]  Yes

[ ]  No

Comments:

1. The SDT asserts that the proposed Cyber Asset definition provides clarity around virtual hardware. (Cyber Assets revised definition: Programmable electronic devices, including the physical or virtual hardware, software, and data in those devices.) Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

[ ]  Yes

[ ]  No

Comments:

1. The SDT asserts that the term Cyber Asset should continue to be used within the NERC Glossary of Terms for: Removable Media and Transient Cyber Asset. Due to the nature of that type of hardware, these devices do not lend themselves to the systems approach. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing to retire EACMS and develop two new terms: EACS and EAMS. These terms will allow changes within the applicability for the monitoring portion to allow third party monitoring systems. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

[ ]  Yes

[ ]  No

Comments:

1. The SDT realized through the process of splitting EACMS that the same considerations apply to PACS, which will allow changes within the applicability for alerting and logging (PAMS is not reflected within the applicability section at this time). The SDT is considering splitting the PACS term into PACS and PAMS to allow third party monitoring or event correlation to be performed without carrying the PACS classification. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing to move away from the more prescriptive ESP/EAP model to logical isolation through the higher level objectives provided by the BES Cyber System concept and its Logical Isolation Zone. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

[ ]  Yes

[ ]  No

Comments:

1. The SDT is considering taking qualitative language out of the Intermediate System definition and using it to clarify requirements. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

[ ]  Yes

[ ]  No

Comments:

1. The SDT is considering changes to the ERC and IRA definitions to address V5TAG issues (see the CIP-005 Technical Rationale document for detailed information). ERC will have conforming changes only and will continue its use as a scoping mechanism. The proposed modifications to IRA will apply to certain non-routable to routable protocol conversion scenarios. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

[ ]  Yes

[ ]  No

Comments:

1. To the extent possible, the SDT intends its modifications to permit approaches to compliance that are “backwards compatible” with compliance approaches within the currently approved versions of the CIP standards. (Notable exceptions include CIP-005 R3, CIP-007 R2, and Secure Configurations – CIP-010). Do you agree the modifications are backwards compatible? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

[ ]  Yes

[ ]  No

Comments:

1. The SDT has not yet determined a proposed timeframe to include in the Implementation Plan. How long would you as an entity need to implement the proposed modifications? Please provide your implementation timeframe and justification for why that amount of time would be needed.

Comments:

1. The SDT is proposing conforming modifications to CIP-004. Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:
	1. Modifications related to CIP Exceptional Circumstances
	2. Use of newly proposed terms EACS and EAMS in the Applicable Systems column
	3. Addition of PCS to the Applicable System column for Parts in CIP-004 to mitigate security risks associated with individuals not needing authorization or PRAs when granted access to systems inside the Logical Isolation Zone

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing modifications to CIP-005 (see the CIP-005 Technical Rationale document for detailed information). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:
	1. The replacement of the ESP concept with Logical Isolation Zone (LIZ).
	2. Is the backward compatibility clear as existing ESPs and EAPs move to the new LIZ concept?
	3. The addition of the 4.2.3.3 exemption in the standard along with the addition of Requirement part R1.2 to address the V5TAG concern of “Super ESPs” or single networks within or between BES Cyber Systems that span more than one geographic location.
	4. As differing forms of shared infrastructure come into play with virtualization, Requirement R3 has been added to include the management plane and its isolation controls as a part of the CIP standards. Is this concept clearly and widely understood?

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing conforming modifications to CIP-006. Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:
	1. Modifications related to CIP Exceptional Circumstances
	2. Use of newly proposed term EACS in the Applicable Systems column

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing modifications to CIP-007 (see the CIP-007 Technical Rationale document for detailed information.). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:
	1. The SDT is proposing adding the security objectives throughout the Requirements in CIP-007. Do you agree that the proposed security objectives add clarity to the reason the requirement exists?
	2. The SDT is proposing the security objective in CIP-007 R1, “to mitigate the risk posed by uncontrolled logical and physical connectivity”. Do you agree that the modifications to CIP-007 R1 Part 1.1 fulfill this security objective for systems where connectivity is not limited to TCP/IP port service combinations, as in virtualized systems and SAN based storage?
	3. Do you agree that the modifications to CIP-007 R1 Part 1.1 add necessary flexibility to fulfill the security objective of CIP-007 R1 for virtualized systems and provides a degree of future proofing?

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing modifications to CIP-010 (see the CIP-010 Technical Rationale document for detailed information.). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:
	1. The SDT is proposing adding the security objectives throughout the Requirements in CIP-010. Do you agree that the proposed security objectives add clarity to the reason the requirement exists?
	2. The SDT is proposing to modify the referenced baseline configuration from CIP-010-3 R1 Part 1.1 to a ‘Secure Configuration’ which is made up of the implemented controls that fulfill requirements within CIP-005 and CIP-007. Do you agree that this set of controls supports managing change under CIP-010 R1 Part 1.1?
	3. The SDT is proposing to modify the current CIP-007 R2 requirements and move them to CIP-010 R3. The SDT believes that the software vulnerability management found within this set of requirements fits logically within the security objective of CIP-010 R3 “to mitigate the risk posed by system vulnerabilities” and has moved it there. Do you agree?
	4. The SDT is proposing CIP-010 R3 Parts 3.5 and 3.6 to replace the current CIP-007 R2 Parts 2.1 – 2.4. Do you agree that the proposed CIP-010 R3 Parts 3.5 and 3.6 offer the additional flexibility needed when implementing virtualized systems that can be dormant for a period, and for which security patches have become available?

[ ]  Yes

[ ]  No

Comments:

1. Provide any additional comments for the SDT to consider, if desired.

Comments: