Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards

CIP-005 and Associated Definitions

**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 Updates for CIP-005 and Associated Definitions** by **8 p.m. Eastern, Wednesday, September 11, 2019.**

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

Project 2016-02 addresses the Federal Energy Regulatory Commission (Commission) directives contained in Order No. 822 and 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 [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) to document these issues. Among these 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.”

The SDT proposed a path through an informal posting and comment period in November 2018 that did not receive acceptance via industry comments. Backwards compatibility, especially for environments unaffected by virtualization, must be a key component moving forward. The SDT drafted a “Case for Change White Paper” explaining why modifications to allow virtualization are needed and presented at a high level a more parallel approach to handling these issues. This approach used alternative definitions for the virtualized environments coupled with more objective requirements. The SDT received a large majority of positive comments on this approach. The current informal posting and comment period is the result of the work to date with this approach within CIP-005 and related definitions.

Also included in the posting are two other items:

* Proposed work on handling the V5TAG issue of ERC/IRA clarification in instances where a serial only device is converted to a routable protocol.
* Splitting the EACMS and PACS definitions such that the access control functions are separate from those systems that only monitor or log access and can be subject to differing requirements based on differing risk.

The standards that will be primarily impacted by these modifications will be CIP-005, CIP-007, and CIP-010 with conforming changes to many other CIP standards. This posting reflects only modifications to CIP-005 and associated definitions in order to get industry feedback as work begins on the other standards. The SDT is looking for feedback on the current approach of using Virtual Cyber Assets (VCA) and Shared Cyber Infrastructure (SCI) definitions to handle virtualized platforms and the new Electronic Security Zone (ESZ) concept that is a new proposed option in CIP-005 for scenarios that no longer fit the existing ESP/EAP model.

**Summary of CIP-005 Changes**

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

## Questions

1. The SDT is proposing the new Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) definitions to allow requirements to be specifically targeted at virtualized environments. The SDT is also proposing conforming changes in several other definitions to allow VCA’s as an option. Do you agree with the development of new terms and the proposed definition of those terms? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (NOTE: Future CIP-011 requirements to be developed to address logical isolation within storage systems and will be coordinated with Project 2019-02 (BCSI)). (CIP-005 Technical Rationale pages 11-12).

[ ]  Yes

[ ]  No

Comments:

1. The CIP SDT tried to maintain backwards compatibility throughout CIP-005. However, in order to take advantage of emergent technologies the existing firewall that were associated with an EAP will now fall into the SCI definition and be subject to CIP-005 Requirement R1 Part 1.6, which requires management plane separation. What level of effort would be required to accommodate these changes? Do you agree? If not, please provide comments to support your response. (CIP-005 Technical Rationale pages 11, 13, and 29-32).

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing the new term Electronic Security Zone (ESZ) to enable future technologies such as policy based environments. Do you agree with the proposed definition? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. Note: ESP will be retained for backwards compatibility. (CIP-005 Technical Rationale pages 10, 14-18, 22-26, and 38-40).
* Electronic Security Zone (ESZ): A segmented section of a network that contains systems and components to create logical isolation.

[ ]  Yes

[ ]  No

Comments:

1. The SDT is addressing the risk of systems of different impact, trust, or security levels (“mixed trust”) environments that are possible on Shared Cyber Infrastructure by modifying the definition of Protected Cyber Asset (PCA) so that it includes those VCA’s that can share a hypervisor’s CPU or memory. Do you agree with the proposed modifications? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 8, and 14-15).

[ ]  Yes

[ ]  No

Comments:

1. The SDT proposes to address infrastructure that is shared between differing BCS impact ratings that share CPU and memory resources by aligning the CIP Requirements for all systems within an ESZ or ESP and affinity to prevent sharing of CPU and memory between Virtual Cyber Assets of differing impact ratings. Do you agree with these changes? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 11, 12, and 14).

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing the addition of exemption 4.2.3.3 and CIP-005 requirement R1 part 1.3 for “Super-ESP” scenarios where single ESP’s or ESZ’s span multiple geographic locations. Do you agree with the proposed modifications? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 18, and 25-26).

[ ]  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 applicable systems column of the relevant requirements to allow third party monitoring. Monitoring and logging data will be handled within CIP-011 in a future posting. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. NOTE: Project 2016-02 will coordinate with Project 2019-02 (BCSI) and Project 2019-03 (Supply Chain) on this topic. (CIP-005 Technical Rationale pages 9, 10, 13, and 19).

[ ]  Yes

[ ]  No

Comments:

1. The [V5TAG document](http://nercdotcomstage/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/Transfer_Issues_V5TAG-SDT_1st-final-03232016.pdf) request the SDT to “Clarify the IRA definition to address the placement of the phrase “using a routable protocol” in the definition and clarity with respect to Dial-up Connectivity.” Therefore, the SDT proposes modifications to the IRA definition and CIP-005 Requirement R2. These modifications will clarify scenarios where Interactive Remote Access applies to serial only devices. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 7, 19-21, 27, and 33-37).

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing modifications to CIP-005 Requirement R1. Do you agree with these changes? Please provide comments to support your response. (CIP-005 Technical Rational pages 22-32).

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing modifications to CIP-005 Requirement R2. Do you agree with these changes? Please provide comments to support your response. (CIP-005 Technical Rationale pages 33-37).

[ ]  Yes

[ ]  No

Comments:

1. Backwards Compatibility: What level of effort is required to migrate from existing definitions to new definitions on existing virtualized architecture?

Comments:

1. The SDT posted a draft CIP-005-7 Technical Rationale document to explain the basis behind these proposed changes. Please provide any additional comments on this document.

Comments:

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

Comments: