Unofficial Comment Form

Project 2019-03 Cyber Security Supply Chain Risks

**Do not** use this form for submitting comments. Use the [Standards Balloting and Commenting System (SBS)](https://sbs.nerc.net/) to submit comments on **CIP-005-7, CIP-010-4 and CIP-013-2** by **8 p.m. Eastern, Wednesday, March 11, 2019.**

Additional information is available on the [project page](http://nercdotcomstage/pa/Stand/Pages/Project2019-03CyberSecuritySupplyChain-Risks.aspx). If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

## Background Information

Project 2019-03 is in response to FERC Order 850 and the NERC Supply Chain Report to make modifications to the Supply Chain Standards, CIP-005-7, CIP-010-4, and CIP-013-2.

The NERC supply chain report recommended including EACMS that provide electronic access control (excluding monitoring and logging). The SDT considered excluding monitoring and logging however, operationally classifying assets using multiple definitions under different requirement of the same standard, and from standard to standard, has the potential to create confusion and unnecessary complexity in compliance programs.

The NERC supply chain report recommended including PACS (excluding alerting and logging). The Standard Drafting Team (SDT) considered excluding alerting and logging however, operationally dealing with separate functionalities within the same asset definition has the potential to create confusion within the other standards that reference the current PACS definition in the applicability column.

In conclusion, the team has decided to use the currently approved glossary definitions of EACMS and PACS in modifications to the Supply Chain Standards. The currently approved glossary definitions are all inclusive of the functionality of the systems and do not separate any subset of functions. Any modification to the existing definitions would have a wide impact on the CIP standards outside of the Supply Chain Standards.

## Questions

1. The SDT added EACMS, with the currently approved definition as explained in the above Background section, to CIP-005, CIP-010 and CIP-013 where the SDT believed is consistent with the FERC Order. Do you agree with FERC’s justification of adding EACMS, FERC Order 850 P57? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

[ ]  Yes

[ ]  No

Comments:

1. The SDT added PACS, with the currently approved definition as explained in the above Background section, to CIP-005-7, CIP-010-4 and CIP-013-2. Do you agree with adding PACS? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

[ ]  Yes

[ ]  No

Comments:

1. Based on the addition of PACS to CIP-005 R2.4 and R2.5 and the lower risk they pose to the BES, the SDT has modified the associated VSL’s. A violation of failing to have a method for determining **OR** disabling for PACS is listed as a Moderate VSL, and a violation of failing to have a method for determining **AND** disabling is listed as a High VSL. Do you agree with the modified VSLs? If you do not agree, please explain and provide your recommendation.

[ ]  Yes

[ ]  No

Comments:

1. The SDT is proposing a 12 month implementation plan. Do you agree with the proposed timeframe? If you think an alternate timeframe is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

[ ]  Yes

[ ]  No

Comments:

1. The SDT proposes that the modifications in CIP-005-7, CIP-010-4 and CIP-013-2 meet the FERC directives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

[ ]  Yes

[ ]  No

Comments:

1. Provide any additional comments for the standard drafting team to consider, if desired

Comments: