NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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) to submit comments on **CIP-005-7, CIP-010-4, and CIP-013-2** by **8 p.m. Eastern, Monday, June 22, 2019.**

Additional information is available on the project page. 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 Electronic Access Control and Monitoring Systems (EACMS) that provide electronic access control and excluding monitoring and logging. The standard drafting team (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 Physical Access Control Systems (PACS) and excluding alerting and logging. The 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 SDT 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 is proposing language in CIP-005-7 in the newly formed R3 to include EACMS as an applicable system to address industry concern during the initial ballot concerning the required use of Intermediate Systems and EACMS. This proposed requirement has modified language from CIP-005-6 Requirement R2.4 and R2.5 and is not a wholly new requirement from the previous version of the standard. Do you agree that this proposal makes it clearer that Intermediate Systems are not required? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   □ Yes

   ☒ No
   Comments:

   Vendor remote access is part of remote access. It is not clear why these are separated.

   Additional confusion caused by another SDT will modify the "interactive remote access" definition. That update will happen after this update. We recommend this definition change needs to happen as part of this project.

   More confusion from the "hall of mirrors" – intermediate systems for intermediate systems. We are not advocating for this hall of mirrors.

   Is this change in scope? SDT moved this language <<active vendor remote access (including system-to-system remote access, as well as Interactive Remote Access, which includes vendor-initiated sessions)>> from the Requirements to the Measures

   For Interactive Remote Access consistency, we expected EACMS and PACS to be added to Requirement 2, Part 2.1.

2. The SDT is proposing language in CIP-005-7 in the newly formed R3 to clarify remote session conditions. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   □ Yes

   ☒ No
   Comments:

   As written, see comments to question 1.

3. The SDT is proposing removing the exception language in CIP-010-4 “Applicable Systems” for PACS which stated “except as provided in Requirement R1, Part 1.6.” This reverts the language in this section back to what is in CIP-010-3. Do you agree with this proposed modification? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☒ Yes

   □ No

   Comments:

   The redline-to-last-posted does not show any changed to Part 1.6.

   We agree that the SDT followed the Directive’s instructions.

4. To address comments the SDT reconstructed the wording in CIP-013-2 Requirement R1, Part 1.2.6 to clarify that all types of vendor-initiated remote access needs to be considered. Do you agree that these changes clearly define the types of remote sessions that are covered by the standards? If you do not agree, please provide your recommendations and if appropriate, technical or procedural justification.

   □ Yes

   ☒ No

   Comments:

   We recommend that any changes to CIP-005 need to be consistent with changes here.

   CIP-005 moved system-to-system from the Requirements to the Measures, while CIP-013 leaves system-to-system in the Requirements. We recommend consistency between these Standards.

5. The SDT is proposing an increase from 12 to 18 month implementation plan in response to industry comment. Do you agree this strikes a balance between appropriate risk mitigation and giving the industry time to implement changes?

☒ Yes

☐ No

Comments:

6. 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:

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

Comments:

Request that NERC notify the industry when posting an update or an additional document after announcing that project's comment and/or ballot period. We suggest that industry wants to provide feedback on the corrected, up-to-date documents.

In the Technical Rationale and Justification for Reliability Standard CIP-013-2 document, "General Considerations for Requirement R2" should read "General Considerations for Requirement R3". The text indicates "The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls ". R2 requires the responsible entity to implement its supply chain cyber security risk management plan specified in R1, R3 requires that the responsible entity review the plan specified in R1 every 15 months.