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, Thursday, September 10, 2020.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Jordan Mallory (via email), or at 404-446-2589.

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 requirements of the same standard, and from standard to standard, has the potential to create confusion and unnecessary complexity and administrative cost burdens 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 within scope of the 2019-03 SAR.

Questions

1. The SDT is proposing to restore CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and Applicable Systems. In addition, the SDT is proposing the newly formed Requirement R3 be dedicated to addressing vendor remote access for EACMS and PACS, specifically. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☒ No

   Comments:

   We thought a CIP Modification SDT goal was to remove this language to assist the coming virtualization updates.

   Request clarification on why CIP-005 R2 Parts 2.4 & 2.5 use the phrase “vendor remote access” while CIP-013 R1 Part 1.2.6 uses the phrase “vendor-initiated remote access” We are concerned that omitting “initiated” may introduce unintended requirements in CIP-005.

2. The SDT is proposing to remove the references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-005-7 Requirements R3 Parts 3.1 and 3.2 to clarify Intermediate Systems are not required for EACMS or PACS, and to address industry’s concerns about recursive requirements (‘hall of mirrors’). Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☒ No

   Comments:

   We agree with the SDT on removing the hall of mirrors. But the “authentication” clarification below is necessary.

   We request clarification of authenticating. The Technical Rationale, page 11 under R3, says this “authenticating” means authenticating the connection, not authenticating the user. This clarification should be in this Standard. This clarification is needed to avoid confusion with CIP-004.

   We request clarification on the distinction between “connection” and “access.”

3. The SDT is proposing to remove references to Interactive Remote Access (IRA) and the undefined term system to system from CIP-013-2 Requirement R1.2.6 to clarify that CIP-013-2 is about the Supply Chain Cyber Security Risk Management Plan and associated higher-level procurement processes and not the operational requirements implemented through CIP-005-7 and CIP-010-4. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☒ Yes

   ☐ No

   Comments:
   We agree that CIP-013 should remain the Plan while CIP-005 and CIP-010 are technical.

4. 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 by fine tuning the scope of the modified requirements to vendor-initiated remote access. 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:

5. Provide any additional comments for the standard drafting team to consider, if desired.
   Comments:

   In the Technical Rationale for Reliability Standard CIP-013-2 document (page 11), “Requirement R2” should read “Requirement R3”. The text indicates “The proposed requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P.46) “. 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.