Unofficial Comment Form
Project 2020-03 Supply Chain Low Impact Revisions

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on the Project 2020-03 Supply Chain Low Impact Revisions Standard Authorization Request (SAR). Comments must be submitted by 8 p.m. Eastern, Wednesday, May 6, 2020.

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
On July 21, 2016, FERC issued Order No. 829, directing NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system (BES) operations. Following the issuance of this order, NERC staff initiated Reliability Standards Project 2016-03 Cyber Security Supply Chain Risk Management to address supply chain risk management in the CIP Reliability Standards. The project resulted in the development of the Supply Chain Standards that consist of new Reliability Standard CIP-013-1 and revised Reliability Standards CIP-005-6 and CIP-010-3.

In adopting the Supply Chain Standards in August 2017, the NERC Board concurrently adopted additional resolutions related to implementation and risk evaluation. These resolutions included preparation of a study of cyber security supply chain risks. FERC approved the Supply Chain Standards with directives for additional modifications to address electronic access or control monitoring systems (EACMS) in Order No. 850, issued October 18, 2018. In its final report accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks.1 NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, Supply Chain Risk Assessment, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through MRC Policy Input.

---
1 See NERC, Cyber Security Supply Chain Risks: Staff Report and Recommended Actions (May 17, 2019). This report, and the other materials referenced in this item, are available on NERC’s Supply Chain Risk Mitigation Program page at https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.
After considering policy input, the NERC Board adopted a resolution to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

☐ Yes
☒ No

Comments:

In the Industry Need, request replace “third party” with “vendor” for consistency with CIP-013.

In the Purpose / Goal, #1 is similar to CIP-005 Part 1.5 which is applicable to High / Medium Control Centers. Implementing Goal #1 would result in this requirement not applying to other Medium Impact assets while applying to High and Low. Next, we cannot find this concern as a recommendation in the study. So, we recommend removing Goal #1.

Goal #2 is similar to CIP-005 Part 2.4. Goal #3 is similar to CIP-005 Part 2.5. The corresponding Requirement 2 includes Technically Feasible Exception (TFE) language. If Goals #2 and #3 include TFE language, we do not believe the industry will achieve a desirable result. We recommend including a process for excluding communications based on capabilities without requiring a TFE.

CIP-005 Part 2.4 does not have the language “when initiated.” Recommend consistency with Part 2.4.

Project Scope says there are “recommendations” in the NERC Supply Chain Risk Assessment Report. That report makes only one recommendation. We request that the single recommendation be explicitly included in this Project Scope.

2. Provide any additional comments for the SAR drafting team to consider, if desired.

Comments:
Incorporating elements of CIP-005 and CIP-010 into CIP-003, when those High/Medium Requirements do not apply to Lows will create difficulty for verifying compliance. For example asset inventory, baseline configuration, patch management activities for Lows. How can the Entity demonstrate compliance for Lows?

The detection of malicious communications requirement is new. It does not tie back to the Supply Chain Standards. This new requirement will require IDS (Intrusion Detection Services). This is out of this scope.

Without the other layers of cyber security controls, the Entity may not realize they’ve been compromised.