NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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 **Project 2020-03 Supply Chain Low Impact Revisions** by **8 p.m. Eastern, Monday, and October 11, 2021.**

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

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. 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.

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 the language proposed in Attachment 1 Section 6 addresses the risk of malicious communication and vendor remote access to low impact BES cyber systems as directed by the NERC Board resolution?

   ☒ Yes
   ☐ No

   Comments:

   Yes, Attachment 1 Section 6 addresses the NERC Board resolution. We are concerned with the adequacy of implementing and auditing. See the response to question 6 for more details.

2. Is it clear that Attachment 1 Section 6 only addresses vendor's access to Low Impact assets containing BES cyber systems from remote locations?

   ☐ Yes
   ☒ No

   Comments:

   Request clarification on "remote" since Section 6 does not define remote and remote is not defined in the NERC Glossary of Terms. "Remote" could be defined as being separate from the BCS and not separate from the asset. Clarifying remote must allow the use of CIP-003-8, reference model 3.

   Request clarification on "remote location." The question includes "remote location" which is not defined. Is the generation switch yard a different location than the generator?

   Request consistent use of "Low Impact" or "low impact."

   The term "mitigate" in CIP-003-X Section 6 is used in the requirement language and appears to be more stringent than CIP-013. CIP-013 does not use the term "mitigate" in the requirement language; but only within the CIP-013 Purpose statement. This would appear the Low Impact requirement is more stringent than the higher impact levels.

3. Do you believe the language in Attachment 1 Section 6 limits the scope to low impact BES cyber systems?

   ☐ Yes
   ☒ No

   Comments:

   Section 6 includes "vendor remote access" which is inconsistently applied to 6.1 through 6.3. Section 6.2 does not include "vendor remote access". This creates confusion concerning the scope and application of 6.2 as compared to 6.1 and 6.3.

   Recommend adding "vendor remote access sessions" to 6.2. For example, "Having one or more method(s) for detecting known or suspected malicious communications for both inbound and outbound communications for vendor remote access sessions; and"

   For example, 6.2 could be interpreted to mean that method must be in place to detect all known or suspected malicious communications which would therefore include malicious communication associated with vendor remote access to BCS. This interpretation would require the application of 6.2 even if vendor remote access is not allowed.

   Request a Section 6 scoping mechanism other than asset level or more specific than the asset level. We recommend language similar to the Applicable Systems for CIP-005-5 R1.5 – "Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers." Another possibility is to leverage CIP-003 Section 3 "Electronic Access Control" scoping / boundary language.

   CIP-005 R1.5 also does not include all Medium Impact due to only including EAPs for Medium Impact BES Cyber Systems at Control Centers. The language in 6.2 is identical to CIP-005 R 1.5's Requirement but R1.5 is applicable to High Impact EAP's and Medium Impact EAPs at Control Centers. 6.2 does not include R1.5's Applicable Systems. We recommend updating 6.2 so that 6.2 clearly applies to the Electronic Access Controls defined in Section 3 and limit the scope to Control Centers identified under CIP-002 Attachment 1 Section 3.1 Low Impact Rating as per the bright line criteria.

4. The SDT proposes that the modifications in CIP-003-X meet the NERC Board resolution 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:

5. The SDT is proposing an 18-month implementation plan. Would this proposed timeframe give enough time to put into place process, procedures, or technology to meet the proposed language in Section 6? 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:

Recommend a 24-month implementation due to the significant scale of Low Impact.

As written, some entities may opt for compliance over security and operational reliability. Based on the scope of the requirement, the scale of BES Assets, and the proposed 18-month implementation time, it appears Responsible Entities would be incentivized to not utilize or disconnect technology solutions to avoid compliance risks. Avoiding compliance risks may result in Responsible Entities reducing capabilities that support reliability or security functions, such as managed (security and operational) support and response functions.

6. Provide any additional comments for the standard drafting team to consider, including the provided technical rationale document, if desired.

Comments:

1) Vendor remote access (VRA) is not a defined term. The CIP-003-X technical rationale (TR) does not provide any information or relate the term to the defined Interactive Remote Access. It does include the guidance in CIP-013 for defining Vendor, as footnote 1. The CIP-003-X TR also equates 3rd party access with vendor access.
    a. "Remote" would need to be defined. An auditor could define remote to be any access outside the BCS. This would cause vendor Transient Cyber Asset access to be VRA.
    b. VRA needs to be limited to access to BCS.
    c. VRA must allow the use of CIP-003-8, reference model 3.

2) There are a number of issues with the CIP-003-X Technical Rationale
    a. Request clarification on CIP-003-X TR, what is the difference between 3rd party access and vendor access.
    b. Does CIP-003-X TR expand scope? Specifically, the last paragraph on page 4 seems to expand vendor remote access with the 3rd party language. We do not find "3rd party" in the CIP-013 documents.
    c. Where is the rest of the old "Guidelines and Technical Basis (GTB)?" We understand that GTB should move to the new TR in a separate section. We request retaining the old reference models.

3) 6.1 - 6.3 are required even if the entity does not allow vendor remote access. It seems that the entity would have to perform these functions for unauthorized vendor remote access if that can even exist.
    a. The technical rational (TR) for 6.2 states: "The obligation in Section 6.2 requires that entities which allow vendor remote access." We request updating the Requirement by adding "vendor remote access." To be consistent with 6.1 and 6.3.

4) Request consistent language between 6.1 / 6.3 and CIP-005-6 R2.4 / R2.5. 6.1 and 6.3 are almost the same as CIP-005-6 R2.4 and R2.5 but R2.4 and R2.5 uses the phrase "active vendor remote access sessions". 6.1 and 6.3 do not include the word "active". Without the word 'active', 6.1 and 6.3 could include or maybe be limited to "capability" of the vendor or the BES configuration and electronic access controls.
    a. The TR for 6.1 uses "that are taking place" and the TR for 6.3 uses "active". Sections 6.1, 6.3 and the TR should consistently use the word "active".
    b. R2.4 and 2.5 are only applicable to High Impact and Medium Impact with ERC. Both include PCA's. This makes Low Impact more stringent than Medium Impact (non-ERC).

5) As written in 6.2, Lows will be a higher bar than Medium which seems to be in contrast to the intent of current CIP Standards risk-based approach (High – Medium – Low). CIP Standards start in CIP-002 with system and asset categorization that establishes a risk-based approach (impact levels) as per the bright line criteria with controls commensurate of the risk (impact levels). There is no corresponding requirement for non-Control Center, Medium Impact. This makes Low Impact more stringent than Medium Impact (non-Control Center).

6) Request the retention of the Guideline and Technical Basis. It appears that some information is moved to the proposed Technical Rationale. But the diagrams and their explanations seem to be struck out of CIP-003 and not moved elsewhere. Request clarification – will the CIP-003-8 reference models continue to be valid?