NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Supply Chain Security Gap Assessment

Performing a gap analysis of the NERC CIP Supply Chain Standards

Tobias Whitney, Gap Assessment Project Lead
March 2024

RELIABILITY | RESILIENCE | SECURITY




Key Updates: CIP-013-2 SAR

Update from NERC Director of Standards & Development:

- The Standards Committee is asking the SCWG to review the SAR and provide them feedback by the March SC meeting.
- The Supply Chain SAR should be reviewed separately from other CIP Standards development activities.
- FERC is aware and would like to see how the SC addresses the SAR

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

January 30, 2024

Michaelson Buchanan

Dear Sir:

Thank you for submitting a Standard Authorization Request (SAR) dated September 18, 2023 titled CIP-013-2 Supply Chain Risk Management with the purpose to revise CIP-012-3 to have complete and accurate assessments of supply chain security risks that reflect actual threat(s) posed to the entity, provide triggers on when the supply chain risk assessment(s) should be performed and require a response to risks identified.

Pursuant to Section 4.1 of the NERC Standard Processes Manual (SPM), Appendix 3A to the NERC Rules of Procedure, I am writing to inform you that on September 20, the Standards Committee (SC) reviewed the submitted SAR and voted to delay action pending consultation with the Reliability and Security Technical Committee (RSTC) to determine if there is another approach to addressing the issues laid out in the SAR.

For additional information on this matter, please see the attached background document and the SAR. These documents were considered at the September 20, 2023 SC meeting.

Sincerely,

Todd Bennett
Chair, NERC Standards Committee

cc:
Michaelson Buchanan, NERC Compliance
Holly Peterson, NERC Compliance
Rich Hydzik, Chair, RSTC
John Stephens, Vice Chair, RSTC
Stephen Crutchfield, Secretary, RSTC

Enclosures:
Standards Committee Background Document
CIP-013-2 Supply Chain Risk Management SAR

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

FERC Staff Feedback

- Audit staff observed that some entities lacked consistency and effectiveness when evaluating vendors and procuring vendor-supplied equipment and software.
- Audit staff observed that other audited entities' supply chain risk identification and assessment processes were unclear and generally lacked rigor.
- Staff also observed multiple instances where entities failed to properly implement their own supply chain risk management plans.
- In some cases, staff found that entities' supply chain risk management plans did not include processes or procedures to respond to risks once identified, specifically for "grandfathered' contracts that existed prior to the effective date of the Reliability Standard.
- In some circumstances where these contracts were considered in the risk management plans, there was minimal consideration given to mitigation and response strategies.
- Audit staff recommends that entities include responses to every risk event identified in their supply chain risk management plans to ensure that appropriate mitigations are employed such that the entity has no "blind spots" in its operations
- Commission staff observed on several occasions unmitigated risk that was present in a BES Cyber System due to assets that had been integrated during the contract term that would have otherwise been minimized if managed within the framework of the supply chain risk management plan parameters required by CIP-013-1, Requirement 1

NERC Staff Feedback (SAR)

- Require entities to create specific triggers to active the supply chain risk assessment(s).
- Include the performance of supply chain risk assessment(s) during the planning for procurement, procurement, installation of procured equipment/software/services, and post procurement assessment.
- Include steps to validate the completeness and accuracy of the data, assess the risks, consider the vendor's mitigation activities, and document and track any residual risks.
- Track and respond to all risks identified.
- Re-assessment of standing contracts risks on a set timeframe.
- Re-assessment of time delay installation beyond a set timeframe.

Supply Chain Working Group Actions

1. Interviewed representatives from NERC CIP Compliance Staff to understand the challenges faced by industry and how the auditors accounted for them during CMEP Activities

2. Performed a “guidance gap analysis” to determine existing guidelines and documented practices from NATF, EEI, EPRI and the RSTC that could address the identified deficiencies in the Supply Chain Standards

3. Identified key recommendations for the Standards Committee to consider when evaluating changes to Supply Chain Standards.

Gap Assessment Team Recommendations

How to respond to the Standards Committee's request for input regarding the Supply Chain SAR:

Option 1 – refer Standards Committee to mapped guidelines developed by NATF, EEI, EPRI, APPA and RSTC and direct compliance monitoring staff to consider them during the CMEP processes.

- Direct CMEP staff give deference to Registered Entities implementing best practices
- Encourage industry's use of the best practices, highlight and give due credit for activities

Option 2 – recommend a process like the DHS/OMB/NIST Secure Software Development Framework to provide more consistency and clarity to suppliers through a digital supplier attestation process/format.

Option 3 – suggest to SC that to refer to the guidelines developed by NATF, EEI, EPRI, APPA and RSTC as recommended language for Standard's enhancements.

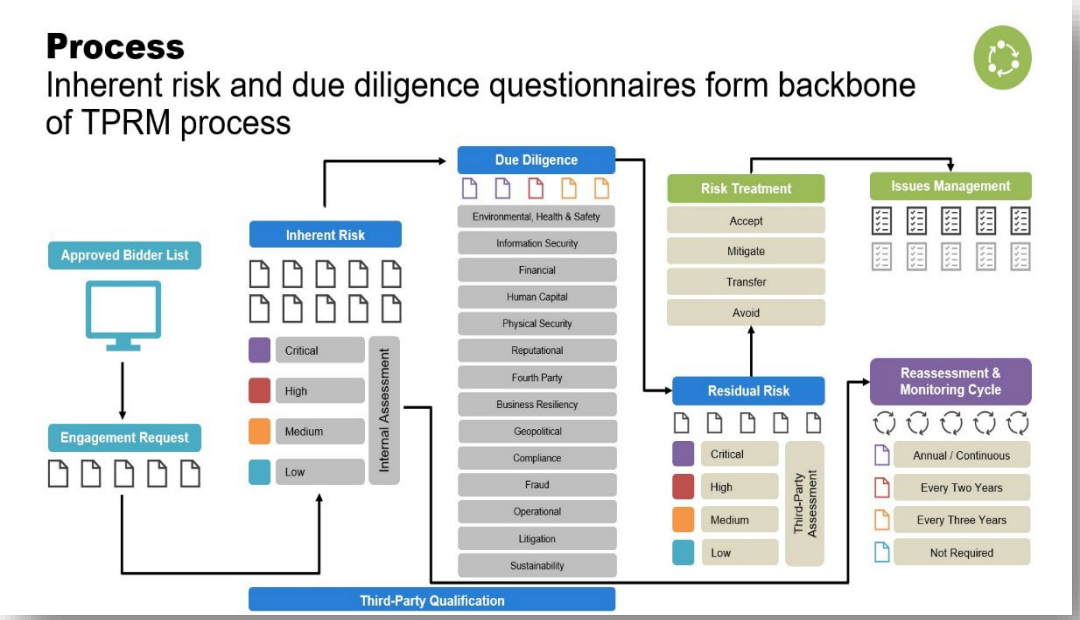
Option 4 - adopt a comprehensive SCRM/3rd Party Risk Plan to increase the level and rigor of the operational execution of supply chain risk management

Next Steps for the Gap Assessment Team

1. Consolidation: the gap assessment team will pursue a single workstream to address both the gap assessment project and the SAR.

2. Concerns: The SAR opening paragraph starts as follows: "The language in CIP-013-2 Requirement R1 lacks specificity to properly identify, assess, and respond to supply chain security risks."

3. Comprehensiveness: Develop a comprehensive third-party risk management program (TPRM) or supply chain risk management program (SCRM) that identifies, assesses, and responds to supply chain risks across multiple risk domains, which in turn would address the core concerns expressed in the SAR (see Option 4 from the previous slide).



Questions and Answers

Key References

- FERC Staff Report Offers Lessons Learned from 2023 CIP Audits | Federal Energy Regulatory Commission

- https://www.cisa.gov/resources-tools/resources/secure-software-self-attestation-common-form