NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Frequently Asked Questions
Supply Chain – Small Group Advisory Sessions

Version: June 28, 2018

This document is designed to convey frequently asked questions from NERC's Supply Chain Small Group Advisory Sessions (SGAS) activities. It is not intended to establish new requirements under NERC's Reliability Standards, modify the requirements in any existing reliability standards, or provide an Interpretation under Section 7 of the Standard Processes Manual. Additionally, there may be other legitimate ways to fulfill the compliance requirement obligations that are not expressed within this supporting document. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of these responses to the frequently asked questions are not a substitute for compliance with NERC's Reliability Standards requirements.

Purpose

NERC hosted several small group advisory sessions (SGAS) with registered entities, NERC Standards Developers, and Regional Entities to discuss the preparation for and implementation of the proposed CIP Supply Chain Standards:

- CIP-013-1 (Cyber Security – Supply Chain Risk Management)
- CIP-005-6, Requirement R2, Parts 2.4-2.5 (Cyber Security – Electronic Security Perimeter(s))
- CIP-010-3, Requirement R1, Part 1.6 (Cyber Security – Configuration Change Management and Vulnerability Assessments)

Each SGAS consisted of closed one-on-one discussions between a registered entity's supply chain security experts and Electric Reliability Organization (ERO) Enterprise staff about concerns pertinent to the entity's implementation of the proposed Supply Chain Standards. This document provides responses to frequently asked questions from registered entities as they prepare for implementation of the proposed CIP Supply Chain Standards.

Supply Chain Questions/Concerns

- Will Supply Chain Standards apply in the future to low impact BES Cyber Systems, protected cyber assets (PCAs), electronic access control or monitoring systems (EACMS), or physical access control systems (PACS)?

  As proposed, CIP-013-1 and CIP-010-3, Requirement R1, Part 1.6 would apply only to high and medium impact BES Cyber Systems. CIP-005-6, Requirement R2, Parts 2.4-2.5 would apply to high impact BES Cyber Systems and their associated PCAs and medium impact BES Cyber Systems with External Routable Protocol and their associated PCAs. In its Notice of Proposed Rulemaking regarding these proposed standards issued in January 2018, however, the Federal Energy Regulatory Commission (FERC or Commission) proposed to direct NERC to modify the these CIP

Reliability Standards to add EACMS associated with medium and high impact BES Cyber Systems.[1] The Commission also directed NERC to evaluate, in its study of cyber security supply chain risks requested by the NERC Board of Trustees (BOT) in its resolutions of August 10, 2017, the supply chain risks associated with PCAs and PACS to determine whether they should be included as well. NERC will also be evaluating in that study the supply risks associated with low impact BES Cyber Systems. NERC responded to FERC's NOPR[2] with a recommendation that EACMS not be included in the supply chain requirements at this time but await the outcome of the Board-requested study. The Commission has yet to issue a final rule in this proceeding

- Is the intent of Requirement R1 of CIP-013-1 to require new or renewed contracts to include contract language that supports CIP-013? If so, that implies that our plan should be in place as of the effective date. Is this accurate?

  The intent of CIP-013-1 is to require entities to develop and implement processes that consider supply chain risks when procuring products and services. Entities are required to include specified security concepts in their procurement activities for high and medium impact BES Cyber Systems but does not mandate the inclusion of any specific provisions in new or renewed contracts to comply with CIP-013. The required process should be integrated into a registered entity's procurement practices by the effective date of CIP-013-1, if approved by the Commission.

- The drafting team stopped short of defining the term "vendor," but it could be interpreted in a number of different ways; besides suppliers, it could also apply to other providers of products or services, such as regulated/non-regulated utilities, the government, etc. Can NERC help clarify this?

  Although the term "vendor" is not defined in the NERC Glossary of Terms, the drafting team did provide guidance in the CIP-013-1 Guidelines and Technical Basis section. As discussed therein, the standard drafting team (SDT) intended the term vendor to include those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. The SDT did not intend it to include, for instance, other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services) pursuant to NERC Reliability Standards.

- What if an asset is purchased in bulk and stored as inventory, then later commissioned as a BCA?

  When purchasing cyber assets in bulk, it is suggested that an entity have a plan for tracking assets in case they end up being used in CIP-applicable roles. Such an approach would provide a means to assess/mitigate risks as necessary.

[1] Notice of Proposed Rulemaking, *Supply Chain Risk Management Reliability Standards*, 162 FERC ¶ 61,044, Docket No. RM17-13-000, at PP. 3-4 (2018).
[2] Comments of the North American Electric Reliability Corporation in response to Notice of Proposed Rulemaking, Docket No. RM17-13-000 (2018).

- The standard obliquely addresses situations where an entity cannot get a vendor to comply and may have no other options. What evidence will be sufficient to show our attempt to contract with a resistant vendor?

  The Cyber Security Supply Chain Risk Management Plans Implementation Guidance for CIP-013-1 provides guidance in this area. Entities should develop and implement a solid procurement plan and document anomalies.

- While we are comfortable that we will be able to show the starting point (contract templates), beyond that there could be confidentiality issues relating to the contract and associated communications. What evidence will be sufficient? Does an executed contract show compliance with CIP-013 R2? What evidence aside from an executed contract will be required? Attestation from vendor, internal supply chain personnel, or internal procedures additional required evidence?

  Yes, an executed contract demonstrating that the requirements of CIP-013-1 were addressed would be sufficient to demonstrate compliance if the registered entity also provides its CIP-013-1 process(es). Attestations, internal procedures, and all relevant email communications should be documented and maintained as evidence of compliance. There should be no need to reveal sensitive/proprietary information to demonstrate compliance. An entity may choose to provide documents with redacted information as audit artifacts.

- One participant explained that they are in the midst of assessing each of its identified vendors (approximately 20,000), and considering resources and time constraints, they could not be completed in the 12 months that FERC is recommending for the CIP-013-1 effective date.

  ERO Enterprise staff commented that as for scope and scale, CIP-013-1 is about modifying future contracts. In addition, there was concern on whether the participant was focusing on assets that are in scope of the Standards (i.e. High/Medium impact BES Cyber Systems and associated vendors). ERO Enterprise staff recommended a bottom-up approach to ensure Critical Infrastructure assets were addressed first based on risk. NERC also submitted comments to FERC supporting the proposed 18-month implementation period.

- What about training and/or educating field operations personnel to verify the identity and integrity of the software source and software prior to installation?

  Organizational processes can (and should) be created to ensure software is validated at a higher (centralized) organizational units (e.g. using a central repository), rather than relying on numerous field operations groups. One suggestion is to include the verification and integrity verifications in the patch management process, if possible.

- R1.1 requires: "One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System":

  Can risks be accepted, instead of mitigated, after they have been assessed and if so, does our plan have to have some formal acceptance process?

  The assessment, acceptance, mitigation, and transfer of risk is part of what the entity will work through in developing the supply chain cyber security risk management plan(s). Categorizing risk (e.g. high, medium, low) and then performing the risk management processes is a good path forward.

- R1.2.2 – Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity

  What type of coordination is expected? How is coordination to be documented? Is there any timing guidance around coordination and response?

  Whatever the notification mechanism is (e.g., email), the entity should show the processes by which the coordination takes place. Any expectations (time frame, levels of severity, etc.) should be consistent with an entity's overall incident response plan(s).

- R2 – Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1:

  The Standard does not specify a timeline for implementation. Is there any guidance on when entities will be expected to have their plan fully implemented? Can it be a phased implementation timeline?

  Review the implementation guidance document and the implementation plan for Initial performance. Once the standard is in effect, all new/renegotiated contracts are subject to the standard.

- Will NERC audit the vendors to ensure they are in compliance with CIP-013-1?

  No, the requirements of CIP-013-1 apply only to registered entities, consistent with NERC's jurisdiction. The registered entity is responsible for complying with CIP-013-1 and for ensuring the vendor is performing in accordance to any contract/agreement. Vendor performance and adherence to a contract is outside the scope of CIP-013-1.

- As the registered entity develops and implements the Supply Chain Risk Standards and Requirements, where can they reach out for additional assistance?

The ERO Enterprise recommends collaborating with peers, trade groups (NATF, NAGF, etc.), regional staff, NIST 800-161, ISO-9001, and NERC. Do not hesitate to pose questions to regional or NERC staff.