NPCC, Inc.
NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Compliance Bulletin

July 2020

NPCC publishes compliance bulletins as a means to engage and inform NPCC entities on aspects of Bulk Power System security, reliability, and compliance.

CIP-013 – Supply Chain Risk Management Resources and FAQ

This Compliance Bulletin is a summary of the various documentation surrounding CIP-013 and gives a quick answer guide while also providing justifications. Each answer is summarized, but the topic header will provide the source information. Additionally, this document includes above and beyond practices that were demonstrated by NPCC entities. Although CIP-013 also has impacts on CIP-005 and CIP-010, questions related to CIP-005 and CIP-010 are not addressed in this bulletin.

Background and Helpful Resources

FAQs: Implementation of these responses to the frequently asked questions are not a substitute for compliance with NERC's Reliability Standards requirements.

- **Supply Chain – Small Group Advisory Session (SGAS)**
  - 2018 FAQ
  - 2019 FAQ

Implementation Guidance and Guidelines: Provides considerations for implementing the requirements in CIP-013-1 and examples of approaches that responsible entities could use to meet the requirements. The examples do not constitute the only approach to complying with CIP-013-1. Responsible Entities may choose alternative approaches that better fit their situation.

- **North American Transmission Forum (NATF)**
  - Cyber Security Supply Chain Risk Management Guidance
  - ERO Endorsed Guidance
- **Edison Electric Institute (EEI)**
  - Procurement Contract Language
- **NERC Resources**
  - Cyber Security Supply Chain Risk Management Plan
  - CIP-013 RSAW
- **Critical Infrastructure Protection Committee (CIPC)**
  - Risk Management – An overview of topics such as identifying, assessing, and mitigating threats and procurements, installations and updating the risk management plan.

- Secure Equipment Delivery – Highlights some of the aspects to consider regarding secure transportation and delivery of systems and components, from component manufacturers to integrators, to vendors, and ultimately to the Bulk Electric System (BES).
- Risk Considerations for Open Source Software – An overview defining open source software and risks to consider if your entity has open source software
- Best Practices for Small Entities – Although CIP-013-1 is not applicable to low-impact BES Cyber Systems, this white paper identifies a catalog of supply chain risk management practices for consideration by small registered entities with low-impact BES Cyber Systems.

NPCC Questions from Outreach

Reminder:
All ERO responses are identified in **GREEN** and referenced in the footnotes
All NPCC stances are identified in **RED**

1. Is an entity a "vendor" only if you have a contract with that entity? Is a procurement in scope of CIP-013-1 if you purchase a BES Cyber Asset from a supplier without a contract (e.g. credit card purchase made during an emergency)? What is considered a service?

   - Under the Rationale Section, the term vendor(s) as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A vendor, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.[1]
   - 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.[2]
   - NPCC considers credit card procurements of High & Medium BCS and related services to be in scope of R1.
   - NPCC recommended that the documented supply chain cyber security risk management plan(s) include provisions documenting emergency procurements, this should include one or more process(es) that address the 1.2 requirement parts.
   - NPCC recommended some alternate risk identification and assessment means, because it may not be practical to have the reseller complete a questionnaire
   - NPCC recommends the following Potential Approach to address Credit Card Procurements
     - Verify that the reseller (Staples, for example) does not tamper with any products (we could probably do this with an attestation from the reseller)
     - Only buy whitelisted products from the reseller whose manufacturer(s) we have already assessed (Cisco, Microsoft, etc.)

[1] CIP-013-1_Standard_Page12
[2] SGAS2018_Page2

2. If an entity contracts with a reseller (Company A) that sells Original Equipment Manufacturer (OEM) products of another company (Company B), is the entity required to identify and assess the risks associated with Company B's products and services?

   - Product resellers are cited in the CIP-013-1 Supplemental Material section as potential vendors, "A vendor, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers [emphasis added]; or (iii) system integrators" (p. 12). Depending on the specific reseller and the item(s) procured through the reseller, there may be additional cybersecurity risks associated with such procurements beyond those identified and assessed for the product manufacturer(s) or the product type(s) in the Part 1.1 cybersecurity risk identification and assessment (i.e., hardware and/or software obtained through a reseller). A registered entity would identify and assess any cybersecurity risks that may be involved in purchasing such applicable hardware or software from resellers. [3]
   - NPCC will review the risk assessment and will review the documented supply chain cyber security risk management plan. NPCC would expect the risk management plan to have a process for evaluating the risk associated with hardware and/or software obtained through a reseller. NPCC would expect the risk assessment of such procurements to identify risks (e.g., if the reseller alters the product), and would expect the plan to address the identified risks.

3. Do all procurements made after October 1, 2020 need to comply with CIP-013-1 even if the procurement was made under a contract that was in place before October 1, 2020. What is NPCC's opinion on renegotiating terms and conditions with vendors for existing contracts?

   - Under the "Supplemental Information" section of the standard, Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan.[4]
   - NPCC considers procurements against contracts in place before 10/1/2020 out of scope.

4. If the entity were to procure a BES Cyber Asset or related service, and subsequently find out (before that BCA or service was deployed in a BES Cyber System) that the risk identification and assessment was not done, can the risk identification and assessment be performed at that point? Would performance at that point be a compliance violation, even if the identification and assessment of risk was performed **before** that BCA could affect the BES?

   - CIP-013-1 is applicable to any procurement regardless of the scenario, including an emergency. CIP-013-1 is silent to any special provisions such as emergency procurements. A registered entity may identify certain hardware, software or services that may be used during emergencies and perform risk assessments in planning for these situations to

[3] SGAS2019_Page7
[4] CIP-013-1_Standard_Page14

mitigate the supply chain risk. Although the CIP-013-1 Standard does not directly address emergency procurements, the registered entity could consider including language in its R1 SCRM procurement plan that addresses the potential for the use of purchasing cards in emergency situations. The registered entity should document the emergency procurement process in the R1 SCRM procurement plan, along with documentation that registered entity personnel or approved contractors verified after-the-fact risks and mitigations of the procurement.[5]

- NPCC will review the documented supply chain cyber security risk management plan and will confirm the entity followed its process. NPCC may identify a potential noncompliance if the entity fails to follow its plan.

5. Are procurements of Transient Cyber Assets (TCAs) and Removable Media (RM) subject to CIP-013-1?

- CIP-013-1 R1 states, "Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems." Transient Cyber Assets are currently not included in the CIP-013-1 requirement language. The NAGF Cyber Security Supply Chain Management White Paper identifies examples to consider when developing and implementing a cyber security risk management plan that includes Transient Cyber Asset considerations.[6]

6. CIP-013-1 requires identification and assessment of risk to the supply chain during planning for procurement. The requirement does not mention mitigation of that risk. Does a failure to perform risk mitigation constitute a violation? Are entities allowed to accept the risk or are entities required to mitigate all risks?

- A vendor's intentional or unintentional ability to adhere to the conditions of an agreement as it relates to CIP-013-1 should be identified and assessed as a risk. As with all of the risks, it is the responsibility of the registered entity to mitigate them accordingly. As an example, the registered entity may address this risk by the implementation of internal controls and processes such as using reputable shippers, tracking shipments, and requiring signatures on delivery.[7]
- Paragraph 17 of the FERC Order approving the Standard states that entities are required to mitigate. Mitigation is mentioned in the purpose of the standard and not mentioned in the Requirement. NPCC auditors will ask about mitigation in an audit. Failure to perform mitigation could result in an Area of Concern (AOC). Failure to implement the documented supply chain cyber security risk management plan will result in a Potential Noncompliance (PNC). The assessment, acceptance, mitigation, and transfer of risk is part of what the

[5] SGAS2019_Page4
[6] NAGF, Cyber Security Supply Chain Management White Paper (2018)
[7] SGAS2019_Page5

entity will work through in developing the supply chain cyber security risk management plan(s). NPCC recommends categorizing risk (e.g. high, medium, low) and then performing the risk management processes.

7. How should auto renewals be handled, sometimes products and services are auto renewed and entities just get an invoice that the maintenance has been renewed.

   - Under the "Supplemental Information" section of the standard, Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan.[8]
   - NPCC recommends entities identify products or services that are set for auto renewal and perform a risk assessment on that product or service prior to the next auto renewal to identify risks and determine if continuing to auto renew that product or service is in the best interest for the entity, reliability, and security.

8. The CIP-013-1 R1 requirement includes language associated with "transitions from one vendor(s) to another vendor(s)." Does this language apply to the product, parts and services vendors may procure to create the product prior to delivery to the Entity or does the language refer to contractual or master agreement transfers?

   - If a vendor is purchased by another vendor, the entity's plan may include controls to maintain awareness of vendor acquisitions and a process to re-evaluate or reassess the vendor.[9]
   - NPCC considers the language to apply for both scenarios. A stronger SCRM may include sections to address the vendor's inherent risk if they utilize other manufacturers to create their product. The SCRM should address the risk posed by the vendor. When transitioning from an old vendor to a new vendor, apply your CIP-011-2 Information Protection Program and CIP-004-6 access revocation program.. The registered entity should treat the new vendor as such, with a complete Part 1.1 risk identification and assessment process of the vendor and applicable products or services.

9. Does a new Scope of Work (SOW) post October 1, 2020 under a master agreement established prior to the October 1, 2020 effective date trigger the need to negotiate new terms and conditions to account for CIP-013-1?

   - Under the "Supplemental Information" section of the standard, Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan.[10]
   - Entities are required to follow their SCRM process on the new SOW.

[8] CIP-013-1_Standard_Page14
[9] SGAS2019_Page3
[10] CIP-013-1_Standard_Page13

10. Does a new SOW post October 1, 2020 under a master agreement established prior to the October 1, 2020 effective date trigger the need to perform a supply chain cyber security risk assessment?

    - A SOW post October 1, 2020 with an established master agreement prior to the effective date triggers the need to perform a supply chain cyber security risk assessment.

11. If an Entity chooses to address CIP-013-1 R1.2.1 – R1.2.6 with the terms and conditions of a procurement contract and existing contracts do not need to be renegotiated, does an Entity need to supply evidence of R1.2.1-R1.2.6 in R2 for existing vendors? If so, what evidence is expected?

    - The entity is expected to provide evidence of compliance related to 1.2.1 – 1.2.6 for all contracts in scope of CIP-013-1. Although existing contracts do not need to be renegotiated, products or services procured after October 1, 2020 are required to follow the entity's SCRM. For a list of specific examples, please refer to the M2 within the standard.

12. What are the qualities of a successful supply chain cyber security risk management plan?

    - NPCC will be presenting a CIP-013-1 webinar that includes recommended practices. Additionally, please see the resources section of this FAQ for more information or review the NERC website page dedicated to CIP-013-1. Again, the guidance and implementation plans do not constitute the only approach to complying with CIP-013-1. Responsible Entities may choose alternative approaches that better fit their situation.

13. Is it acceptable for an entity to leverage the CIP standards and requirements in their process for assessing risk, determining mitigation, and implementing mitigation actions? For example, if the entity can determine and disable remote or onsite access can this be used to assess risk and mitigate the risk?

    - It is the entity's responsibility to determine risk and implement mitigation actions to address the risk. In NPCC's opinion, the provided example is a control to mitigate a risk posed by an outside threat but may not be a way to mitigate a different threat.

14. Is it acceptable for contract language to be less stringent than the EEI model if the effect is to increase likelihood of acceptance, so long as the language is still robust?
    - ❖ Where time periods are blank in the EEI model language, does NERC expect a baseline time period for minimal compliance, or are these time periods expected to be negotiated on a case-by-case basis? Ex: Under R1.2.2, the number of days the vendor has to develop a prevention of recurrence plan is blank

- NPCC considers the EEI model as a guidance tool. NPCC will be monitoring for compliance to the Standard and requirement language. Currently, CIP-013-1 does not provide specific timeframes, for example, the EEI model states "Within [insert number of] days of notifying company of the security incident…" or "Contractor shall provide summary documentation of vulnerabilities and material defects in the procured product or services within thirty (30) calendar days after such vulnerabilities and material defects become known to Contractor." A stronger SCRM will consider the risk associated from a longer duration to disclose a vulnerability.

15. What evidence will be required to show the process of negotiating CIP-013-1 language with vendors, particularly if security terms are less stringent than the EEI model and a vendor is still selected for commercial reasons?

- The procurement documents (e.g., RFP and vendor response evaluation matrices) used for a specific applicable procurement, along with any contract language connected to the procurement can serve as primary evidence the registered entity pursued its due diligence for the R1 Part 1.2 Requirement Parts, when the vendor failed or refused to comply. As stated in R2, vendor performance and adherence to a contract is beyond the scope of R2, so the responsibility of compliance rests on the registered entity to demonstrate it implemented its Part1.2 processes as far as it could reasonably go without negating the procurement. Since the registered entity identified risk, it is incumbent on the registered entity to enact mitigating measures that would address the vendor's refusal to meet the Requirement Parts.[11]
- NPCC considers the EEI model as a guidance tool. In the event that contract negotiations fall short of adhering to the subparts of CIP-013-1 R1, NPCC will review the entity's correspondence, policy documents, or working documents that demonstrate use of the SCRM.

[11] SGAS2019_Page5-6

Practices Demonstrated by NPCC Entities

NPCC has compiled a list of recommended and above and beyond practices demonstrated during the course of assisting our registered entities. Please also refer to the resources section to supplement your compliance program regarding CIP-013.

CIP-013 Supply Chain Risk Management Webinar	Recommended Practice(s)	Above and Beyond Practices
R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems.	1. Consider including Emergency Procurements within the SCRM or whitelisting vendors	1. Apply the documented supply chain cyber security risk management plan for all procurements 2. Consider a Risk Score process to evaluate vendors 3. Consider identifying and developing supply chain risk strategies for creating an overarching cyber supply chain risk management plan. 4. Consider identifying and assessing interdependent processes.
R1.1. 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 from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).	1. Consider including a form/questionnaire for procurements to identify if the purchase will be used in High/Medium BCS. 2. Consider developing a process which includes updating, communicating, and documenting vendor relationships	1. Allocate dedicated resources familiar with the standard to review procurements specific to CIP-013. Utilize any NERC compliance groups to review procurements and vendor transitions.
1.2. One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:	1. Consider EEI's procurement language when negotiating contracts. (EEI Procurement Guidance)	1. Pre-authorize all vendors no matter if they are "grandfathered"

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;	1. Consider defining methods of notification and qualifying vendor incidents.	Subscription to Threat Intelligence services
1.2.2. 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;	1. Consider defining incident coordination methods.	
1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;	1. Consider a method to track and manage vendor remote or on-site access	Remote vendor access is disabled by default and only enabled for assigned / scheduled work.
1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;	1. Consider establishing vendor reporting obligations and define “known vulnerabilities”	Subscription to Threat Intelligence services
1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and	1. Consider classifying software (custom/open source/commercially available) 2. Consider managing and recording exceptions to this process when there is not a method to verify the identity of the software source or the integrity of the software obtained from the source. 3. Consider managing and tracking software source changes	After software integrity and authenticity is performed, entity places approved software in internal repository. IT staff use approved internal repository for installation of software.
1.2.6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).	1. Consider defining or applying vendor access protocols.	

ERO Will Evaluate Effectiveness of CIP-013-1

NERC plans to measure the effectiveness of the Supply Chain Standards by performing the following actions during the first two years of implementation:

ERO staff will conduct surveys on supply chain awareness, compiling statistics on identified key risk indicators. These indicators include software validation discrepancies, information on vendors that support supply chain frameworks, entities who performed vendor risk assessments in the prior 24 months, and analysis of vendor vulnerability and cyber security incident notifications. Information compiled will be examined for trends and reported periodically to the Reliability and Security Technical Committee and posted on the website.

ERO staff will solicit comparative contractual language (pre and post Supply Chain Standards implementation) voluntarily from entities to determine whether entities have been able to successfully negotiate contracts that include required supply chain controls, or whether other controls have been required to manage the risk. This will include entities not subject to the Supply Chain Standards to determine whether there has been any incidental benefits derived from the implementation of the Supply Chain Standards.

ERO staff will compile audit and compliance information on the Supply Chain Standards to determine whether the language is clear, whether entities understand what is expected, and whether there are any reliability gaps in the standards.

Finally, ERO staff will analyze supply chain communications, education, outreach, and training to determine whether vulnerabilities have been identified and successfully communicated. This will include inquires to the E-ISAC on supply chain issues and requests for training and outreach.

Periodically during the two years of analysis and at the conclusion of the two years, NERC staff will report to the Board on its analysis of the effectiveness and provide any recommended actions that may be determined to be necessary. [12]

[12] NERC Evaluation of CIP-013-1

Future plans for CIP-013-2

FERC Order 850 (October 18, 2018)

- FERC directs NERC modify CIP-013 to include EACMS associated with medium and high impact BES Cyber Systems.
- FERC accepted NERC's commitment to evaluate the risks of PACSs and PCAs (in addition to low impact BES Cyber Systems)

NERC Cyber Security Supply Chain Risks Report (May 17, 2019)

- NERC recommends CIP-013 to address Physical Access Control Systems (PACSs) to high and medium-impact BES Cyber Systems.
- NERC recommends additional studies for low-impact BES Cyber Systems and PCAs.
- NERC recommends CIPC Supply Chain Working Group develop a guideline to assist entities in applying supply chain risk management plans to low impact BES Cyber Systems and PCAs.

Standards drafting team (September 2019)

- Creation of CIP-013-2 to include EACMS and PACS.
- Final ballot approval estimated November 2020

2020 Current Events and Predicted Future

- Send to BOT for Approval
- Send to FERC for Filing
- FERC approval estimated 2021
- Estimated Effective date in 2022