NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Frequently Asked Questions
Supply Chain – Small Group Advisory Sessions

Version: May 05, 2021

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. The ERO Enterprise does not intend this to be Compliance Guidance as it was not submitted as a CMEP Practice Guide nor was it submitted by an industry group. Additionally, there may be other legitimate ways to fulfill the compliance requirement obligations that are not expressed within this document. Compliance will continue to be determined based on language in the NERC Reliability Standards and the registered entity's facts and circumstances. Implementation of these responses to the frequently asked questions are not a substitute for compliance with NERC's Reliability Standards requirements.

Purpose

In October 2019, NERC hosted several small group advisory sessions (SGAS) with registered entities, NERC Standards Developers, and Regional Entities to discuss and prepare for and implementation of the 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 registered entities and Electric Reliability Organization (ERO) Enterprise staff about concerns pertinent to the registered entity's approaches and anticipated implementation of the Supply Chain Standards. This document provides responses to frequently asked questions from registered entities as they prepare for implementation of the CIP Supply Chain Standards.

Supply Chain Questions/Concerns

What actions should a registered entity have completed on or before October 1, 2020 for CIP-013-1?

The registered entity is required to develop its CIP-013-1 R1 Supply Chain Risk Management (SCRM) procurement plan[1][2], including documented processes that address R1 Part 1.1 and Part 1.2, and for R3, CIP Senior Manager (or delegate) approval of the initial R1 plan on or before October 1, 2020.

[1] CIP-013-1, R1, R2 – Supply Chain Management (NATF)
[2] Cyber Security Supply Chain Risk Management Plans

To support compliance with CIP-013-1 after the effective date, a registered entity may consider including specific sections in the initial R1 Plan that address:

a. *An R2 implementation plan and internal controls to ensure the R1 SCRM cyber security risk identification, assessment, and mitigation processes implemented, as needed, for each applicable procurement on or after the effective date.*

b. *Defined processes and internal controls to ensure periodic reviews, updates, and approvals of the R1 SCRM procurement plan occur at least once every 15 calendar months after the required initial review and approval*

Software / Equipment

Can a registered entity provide signed software or hashes when possible but rely on attestations in some cases for both software source verification and software integrity verification (CIP-010-3 R1 Part 1.6)?

No, in general, ERO Enterprise audit teams do not accept attestations as primary evidence for performance-based Standards. Some vendors do not have the tools for end users to verify the software integrity obtained. If this were the case, the audit team likely would examine applicable mitigating measures taken for these exceptions. As CIP-010-3 R1 Part 1.6 states, "when the method to do so is available to the registered entity from the software source," the ERO Enterprise recommends registered entities consider how vendor capability may impact the development of potential internal or external mitigation controls in lieu of vendor support for Part 1.6.

The ERO Enterprise also recognizes not all software sources have secure methods for verifying the integrity of the software, so suggests the registered entity document these exceptions in the SCRM plan. If there is an instance where a method is not available to verify the integrity and authenticity of software, it is recommended to document the exception and any mitigating measures internally to reduce the supply chain risk of introduction of malware or counterfeit software. While not required, it is a best practice to retain artifacts of the vendor's available methods or lack thereof for the verification of software integrity and authenticity of all software and patches. This will provide an internal audit trail for the registered entity's records to allow easy reference and may save research time in the event any of those methods should change in the future.

For third parties performing the Part 1.6 controls, the audit team likely would expect the registered entity to demonstrate that it obtained the software update/install from the third party performing these services.

Are existing deployed BES Cyber Systems grandfathered in under CIP-010-3 and CIP-005-6?

Only procurements for applicable BES Cyber Systems that occur on or after the effective date (October 1, 2020) are in scope for the CIP-013-1 procurement planning processes. However, CIP-005-6 (R2 Parts 2.4

and 2.5), and CIP-010-3 (R1 Part 1.6) become effective on October 1, 2020 and apply to all high and medium impact BES Cyber Systems, including existing applicable BES Cyber Systems.

A registered entity buys equipment from a vendor with third-party software installed. What are your recommendations for showing evidence of due diligence?

The registered entity should use its SCRM plan to identify and assess the risks associated with the third party software installed. The results of this analysis would dictate what mitigations are appropriate to address the risks related to the third party software. Some common forms of evidence include, but are not limited to, checklists or the contents of a change ticket that documents the due diligence performed.

What should a registered entity do if a vendor is purchased by another vendor?

One approach is to ensure the registered entity's SCRM plan details the process to re-evaluate or reassess the vendor(s). This should include the controls the registered entity deploys to maintain awareness of possible vendor acquisitions.

Is open source software in scope for CIP-013-1 and CIP-010-3?

The Supply Chain Standards are silent on terms and conditions for procured products or services that registered entities may install. A registered entity should implement its risk identification and assessment methodology for all procurements and installations of open-source software on applicable BES Cyber Systems.

What compliance documentation and evidence should a registered entity create and maintain to comply with CIP-013-1 R1 Part 1.2 and its sub-parts for software that has no associated vendor, such as open source software?

The registered entity may address Part 1.2.1 and Part 1.2.4 by developing one or more internal processes to identify and monitor reputable third-party sources for assessments and reports of applicable open source software incidents or vulnerabilities. The registered entity may consider developing a modified Part 1.2.5 process for acquiring, verifying, and authenticating such software and applicable patches, as released by reputable sources (e.g., for software upgrades or security patches for identified vulnerabilities). An example of this could be a completed evaluation that specifically addresses open source technology.

How do you perform authenticity checks for open source software?

The ERO Enterprise also recognizes not all software sources have secure methods for verifying the integrity of the software, so it recommends the registered entity document these exceptions in the supply chain cyber security risk management plan. If there is an instance where a method is not available to verify the integrity and authenticity of software, the ERO Enterprise recommends the registered entity to document the exception and any mitigating measures afforded internally to reduce the supply chain risk of

introduction of malware or counterfeit software. Some examples include, but are not limited to, thoroughly research where the software is being downloaded, ensure the name of the file downloaded from the source matches what is being installed, and verify the checksum values and signature files if available. Pursuant to CIP-013-1, Requirement R1, Part 1.2.5, the registered entity should document its verification process of the authenticity of the open source software. In instances where authenticity checks are unavailable, the registered entity should consider documentation outlining the risk factors identified and security controls used to prevent impact to reliability and security. Some example evidence may include change tickets, checklists, results of the evaluation, etc.

Risk Assessment / Contractual

Can a registered entity provide redlined contracts, demonstrating contract negotiations, as a part of our evidence to prove compliance with CIP-013-1 R1 and R2? Is this a common way to show compliance and are there other considerations we should take into account?

The audit team will sample all R2 implementations, so the initial evidence request will ask for a complete list of applicable procurement(s). The audit team will sample the list in accordance with the ERO Sampling Handbook[3] and request complete implementation documentation for the sampled procurements. Keep in mind the R1 plan should provide processes and procedures to indicate how the registered entity will meet the security objectives of CIP-013-1 and address each component of R1 Part 1.1 and Part1.2. While redlined contracts may serve as evidence of R2 implementations, the R1 plans should describe the registered entity's methodology for identifying and assessing risks associated with applicable procurements. Contracts may be a component of the R1 plan, but the registered entity should ensure the procurement documents support the development of a contract that meets the CIP-013-1 security objectives.

Would a registered entity be found non-compliant if their SCRM plan included a provision for an after the fact risk assessment to be conducted for applicable medium and high impact BES Cyber Systems implemented under emergency situations?

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 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.

[3] https://www.nerc.com/pa/comp/Documents/Sampling_Handbook_Final_05292015.pdf

What if a registered entity has a master agreement effective before the effective date of CIP-013-1 (October 1, 2020) which does not include terms associated with CIP-013-1 R1 Part 1.2 and its sub-parts, and purchase products or services after October 1, 2020; do I need to conduct a risk assessment on the vendor?

The risk assessment should be performed on the vendor, product, and/or service as dictated by the SCRM plan. The registered entity's SCRM plan determines where and how the risk assessment is performed. Regarding R1 Part 1.2 and its sub-parts, while the action to renegotiate or abrogate existing contracts is not required, it is expected that mitigations are implemented to address the risks of these elements not being contractually binding on the vendor. All procurements of products or services applicable to high or medium impact BES Cyber Systems after October 1, 2020 would be applicable, under the R1 SCRM plan and R2 implementation.

What if my vendor cannot adhere to one or more sub-parts (1.2.1-1.2.6) in Part 1.2 for CIP-013-1?

The registered entities are still responsible for implementation of Part 1.2 in R1. Registered entities should have documented and implemented controls for Part 1.2 in the absence of vendor adherence. For example, if the registered entity's vendor is not notifying it of vendor-identified incidents, then it may implement a control that monitors US-CERT, ICS-CERT, E-ISAC, and NERC Alerts.

What additional frameworks did registered entities consider in development of Supply Chain Risk Management Programs? Furthermore, are entities developing one or more risk assessment questionnaires?

Entities considered NIST, NAGF guidance, NATF guidance, EEI guidance, SOC2, and ISO 27001 in developing their SCRM programs. In most cases, registered entities used two risk assessment questionnaires, one for vendors and one for products or services.

What is the registered entity's obligation to mitigate an identified risk, if the vendor does not agree under the contract, for example, shipping and delivery?

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.

Vendor / Third-party / Reseller

What is sufficient evidence to document cases in which vendors refuse to meet the CIP-013 R1 Part 1.2 Requirement Parts?

In this case, 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.

Is a registered entity a vendor if they are providing non-reliability services for another registered entity (i.e., relay technician, substation maintenance work)?

In this situation, the registered entity providing the non-reliability service could be considered a vendor providing related services. The Supplemental Material on page 12 of CIP-013-1, states, "The term vendor(s) as used in the standard is limited to those persons, companies, or other organizations with whom the registered 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 (BA) or Reliability Coordinator (RC) 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."

What if a registered entity does not allow active vendor remote access to applicable BES Cyber Systems and associated Cyber Assets, does a registered entity still have to provide anything for CIP-005-6 R2 Part 2.4 and R2 Part 2.5?

Yes, a registered entity would be required to document that it does not allow any active vendor remote access. A registered entity would include one or more methods for determining and disabling active vendor remote access sessions in the event such sessions become necessary.

What if your process(es) in CIP-013-1 R1 Part 1.1 identified cyber security risk(s) with a vendor and you still proceed with products or services from that vendor?

Any identified security risks should have some form of mitigation to reduce risk(s); simply accepting the risks is not adequate, unless the analysis performed demonstrates no other reasonable mitigations are available.

Is a registered entity a vendor if they are providing products such as hardware or software (BES Cyber Systems)?

Yes, in the Supplemental Material on page 12 of CIP-013-1, states, "The term vendor(s) as used in the standard is limited to those persons, companies, or other organizations with whom the registered 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." The definition does not exclude registered entities as vendors if they are providing products such as hardware or software.

Is it necessary to implement CIP-013-1 R1 Part 1.1 for resellers?

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.

What about a vendor-to-vendor transition? How should we handle the old and new vendors?

Consider applying your CIP-011-2 Information Protection Program to secure any BCSI on the decommissioned Cyber Assets. Once this has been documented by your control process, terminate any remaining access permissions. 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.

Cyber Asset Applicability

Although not in the requirements, what are the expectations for handling the procurement of low impact BES Cyber Systems, EACMS, PACS, and PCAs concerning supply chain risk management?

The NERC Staff Report on Cyber Security Supply Chain Risks (May 17, 2019) in regard to LIBCS. As stated in the Staff Report, "The Supply Chain Standards are applicable only to high and medium impact BES Cyber Systems" (Ch. 4: Overview section, p. 17). Reading further in the Staff Report, NERC identified several significant supply chain risks associated with LIBCS (pp. 17-19), but fell short of recommending LIBCS be added as applicable systems in the upcoming revision, "For several reasons, NERC staff does not recommend revising the Supply Chain Standards to require protections for all low impact BES Cyber Systems at this time" (p. 19). To put the citation in question in a more complete context, "NERC staff expects entities that own only low impact BES Cyber Systems to develop supply chain risk management programs tailored to their unique risk profiles and priorities. The APPA/NRECA white paper provides considerations for smaller registered entities in developing such programs. ***NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities in voluntarily applying supply chain risk management plans to low impact BES Cyber Systems*** [emphasis added]*" (p. 19).*

NERC's expectation for LIBCS, as stated in the 2019 SCRM Staff Report, is that entities will voluntarily comply with the SCRM requirements. In particular, with bulk inventory purchases, several entities have reported the cost-benefit return is not there to segregate warehouse stock, so procurement departments plan to apply the R1 plan for all BES Cyber Systems products, regardless of the final destination of a specific Cyber Asset. To support this voluntary effort, APPA/NRECA developed the white paper described in the citation above (see Staff Report, Footnote 43, p. 19 for a link to the white paper) that describes several voluntary SCRM processes a smaller registered entity can implement to provide some level of SCRM protective measures and controls to LIBCS, but it is not currently required. The ERO Enterprise strongly encourage you to download and review this white paper to see what voluntary SCRM protective measures and controls may be applicable to your LIBCS.

Addendum - December 2020

Am I expected to audit my vendors?

Within the parameters of CIP-013, the entity is expected to follow their SCRM plan. If the plan directs the entity to audit their vendors it will be an expectation that it is conducted accordingly.

CIP-013-1 is forward looking and eventually all applicable vendors will be assessed and identified cyber risks for products and/or services will be addressed. Therefore, it is prudent to continuously monitor procurement of vendor products or services. The SCRM plan should include a process for monitoring and assessing changes to identified cyber risks after an assessment has been conducted.

How much focus will be on the contracts during my audit?

Both contract language and vendor performance to a contract are explicitly taken out of scope for these Requirements by the Note to Requirement R2. As dictated in the R2 note, entities are not expected to renegotiate their contracts; however, the supply chain risk standard would apply to the procurements associated with these agreements. It is recommended that entities do not solely rely on contract language to demonstrate implementation of this Requirement. Instead, it is suggested the implementation of the processes include documentation that you have followed the processes step-by-step.

Contracts will only be considered if entities voluntarily submit them as evidence.

Procurements, including those under existing contracts, performed on or after October 1, 2020 are subject to CIP-013-1 and should be considered applicable to the Supply Chain Risk Management plan(s).

Entities are expected to demonstrate implementation of the SCRM plan on or after the effective date. Dated documentation should demonstrate the process/procedures identified in the SCRM plan were implemented and afforded the required R1 controls to assess and identify cyber security risks and mitigating identified risks as applicable.

What level of the organization is appropriate to accept security risk from a vendor?

The entity-defined SCRM plan documents what level within the organization determines if a risk is acceptable. Furthermore, in instances in which risk must be accepted, entities are expected to document and implement other mitigating controls to minimize the accepted risk, as documented in the SCRM plan.

It is incumbent that if a vendor exceeds your organization's risk threshold, a thorough review and approval should be conducted to ensure a solid understanding of the risk and the mitigating controls afforded or needed to be implemented. Particularly if the risk is identified as having a high probability of causing adverse effects.

Further, entities may want to consider including a process to frequently review and discuss these types of risk approvals.

What obligations for CIP-013 would the co-op be responsible for if any? Who would be responsible for performing the Risk Assessment, the co-op or the other company?

Under CIP-013-1, 4. Applicability, 4.2 Facilities, it states, "For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable." Additionally, R1. Is applicable to all procurements associated with high and medium impact BES Cyber Systems. As written, the compliance obligations ultimately reside with the Responsible Entity who owns the Facilities with identified high or medium impact BES Cyber Systems. It would be expected that the Responsible Entity perform the risk assessment according to their documented plan to include analyzing risks posed by the vendor, equipment, and services provided, if applicable. These risks are then to be mitigated accordingly. In the scenario where there is joint or shared ownership; it is expected that both Responsible Entities coordinate or perform joint or separate risk assessments.

Will auditors look at language within contracts or will their focus be on only the risk assessments?

Both contract language and vendor performance to a contract are explicitly taken out of scope for these Requirements by the Note to Requirement R2. It is recommended that entities do not solely rely on contract language to demonstrate implementation of this Requirement. Instead, it is suggested the implementation of the processes include documentation that you have followed the processes step-by-step.

Contracts will only be considered if entities voluntarily submit them as evidence.

Procurements, including those under existing contracts, performed on or after October 1, 2020 are subject to CIP-013-1 and should be considered applicable to the Supply Chain Risk Management plan(s).

Entities are expected to demonstrate implementation of the SCRM plan on or after the effective date. Dated documentation should demonstrate the process/procedures identified in the SCRM plan were

implemented and afforded the required R1 controls to assess and identify cyber security risks (Part 1.1) and mitigating identified risks as applicable (Part 1.2).

Will auditors have visibility to a registered entity's audits on vendors?

The entity dictates what artifacts of evidence best demonstrates compliance with the Standard Requirements. If prescribed by the SCRM plan, entities could provide the results of their audit on vendors to show due diligence in identifying and assessing cyber security risks.

What should registered entitles expect regarding effectiveness and efficiency of third party assessments (Known vs. Unknown)? Overall risk management, Evidence Materials.

It is incumbent on entities to understand the effectiveness and efficiency of third party assessments within their environment. Based on what is documented in the SCRM plan, entities determine if these files are appropriate as evidentiary files.

Addendum May 2021

How much focus do I need to place on my compensating controls for vendor deficiencies?

It is incumbent on the entity to determine the level of risk associated with the utilization of a particular vendor. The identified risks must be either mitigated or accepted in accordance with the SCRM plan.

If I use a single or sole sourced vendor that has a higher risk profile, is that ok?

Entities are to define the level of risk that is appropriate and acceptable within their organization. This information must be documented in the SCRM plan.

If I use a single or sole sourced vendor that has a higher risk profile, does that need to be approved? If yes, by whom?

The entity defined SCRM plan outlines when approvals are necessary and by whom.

Concern with an Audit scope around an emerging security risk. What is the expectation for risk assessments?

As there is no one size fits all, risk assessments should adequately identify and assess risks associated with the entity's high and medium impact BES Cyber Systems.

Is there an expectation that registered entities will be required to provide contracts to auditors?

Both contract language and vendor performance to a contract are explicitly taken out of scope for these Requirements by the Note to Requirement R2. It is recommended that entities do not solely rely on contract language to demonstrate implementation of this Requirement. Instead, it is suggested the implementation of the processes include documentation that you have followed the processes step-by-step.

Contracts will only be considered if entities voluntarily submit them as evidence.

Procurements, including those under existing contracts, performed on or after October 1, 2020 are subject to CIP-013-1 and should be considered applicable to the Supply Chain Risk Management plan(s).

Entities are expected to demonstrate implementation of the SCRM plan on or after the effective date. Dated documentation should demonstrate the process/procedures identified in the SCRM plan were implemented and afforded the required R1 controls to assess and identify cyber security risks (Part 1.1) and mitigating identified risks as applicable (Part 1.2).

Is it going to be acceptable for vendors that provide a service of "contractors" to state in your Supply Chain Cyber Security Plan that contractors hired through a temporary agency will be onboarded through the CIP-004 process and not do a risk assessment on an agency that provides the service of providing temporary employees?

The SCRM Plan can detail how onboarding procedures conducted for CIP-004 compliance are a part of the mitigation strategy for risks associated with utilizing the vendor's services; however, the registered entity is expected to conduct a risk assessment. Risk assessments are not the same as mitigations and as such registered entities should be diligent to ensure risks are identified and appropriate mitigations are implemented or in place to address them.

Should a registered entity identify and assess cyber security risks related to the vendor and/or product or service?

Both should be done to conduct an accurate cybersecurity risk identification and assessment.

Does a registered entity need to mitigate identified and assessed cyber security risks?

As referenced in FERC Order No. 829, the security objective is to ensure entities consider cyber security risks to the BES 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); and options for mitigating these risks when planning for BES Cyber Systems.

Prior to July October 1, 2020, what if a registered entity has Cyber Assets that were purchased in bulk and stored as inventory, then after October 1, 2020, some or all are commissioned as a BCA? Does the registered entity have to implement CIP-013-1 R2?

Any procurement on and after July October 1, 2020, of BES Cyber Systems 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) are subject to CIP-013-1.

How often should a registered entity re-assess a vendor?

Entities are to define the reassessment of vendors. Elements such as cadence, triggers, and use of existing assessments are to be documented within the Registered Entity's SCRM Plan.

Can a registered entity use a third-party service to conduct a vendor cyber security risk identification and assessment?

Third-party services could be used to complement a registered entity's own cyber security identification and risk assessment.

Could a registered entity provide a redacted (due to confidentiality issues relating to the contract and associated communications) executed contract, attestation(s) from vendor and internal supply chain personnel, and internal processes/procedures as evidence of implementation for CIP-013-1 R2?

An executed contract demonstrating Part 1.2 was addressed could be sufficient to demonstrate compliance if the registered entity also provides additional supporting evidence such as processes/procedures, email communications, and attestations. The registered entity should not reveal any sensitive or proprietary information that would cause a breach of contract.

Is open-source software in scope for CIP-013-1 and CIP-010-3?

A registered entity should implement its cyber security risk identification and assessment for all procurements of open-source software on all applicable systems.

A registered entity should implement a method to verify the identity of the source and the integrity of the open-source software on all applicable systems.

Document controls implemented that minimize the risks associated with open-source software.

How can a Registered Entity assess manufacturers that may not have enough public information and do not respond to questions.

As one size does not fit all, it is incumbent on the Responsible Entity to perform a risk assessment on any vendors with which the Responsible Entity is considering to supply BES Cyber Systems and related services; which includes resellers and manufactures, based on risk. Any identified risks, including those associated with the manufacturer not responding to a questionnaire should be addressed according to what is documented in the SCRM plan.

If an entity uses a third-party assessment or certification (including evaluations conducted by a solution provider) as part of its supply chain risk assessment, is this acceptable to the ERO to give the ERO confidence?

Third-party services can be an acceptable input into the overall cyber security risk(s) assessment implemented by the entity.

Are there third-party assessors/certifiers/solution providers that the ERO will not accept as capable or recognize as providing an acceptable verification? How does the ERO determine whether the ERO will determine that the third-party assessor/certifier/solution provider is capable?

It is incumbent on the entity to demonstrate the effectiveness of their risk assessment, including the utilization of third-party assessor/certifiers/solution providers.

Can an entity utilize a certification program (i.e., ISO 27001 or IEC 62443, UL, etc.) in place of doing an assessment using a questionnaire, on site audit of the vendor, or having a third-party assessment performed? This could cut out all the different surveys going to suppliers and maybe push more suppliers to gain certifications like ISO 27001.

The Standard Requirement affords an entity the flexibility to utilize frameworks as an input in their overall SCRM Plan.

What type of third-party assessment or certification (framework – e.g., SOC2, ISO 27001, IEC 62443, etc. or individual solution provider's methodology) does the ERO perceive is sufficient to be used as a consideration in an entity's supply chain risk assessment?

The utilization of frameworks in an entity's supply chain risk management program can be implemented. It is the responsibility of the entity to demonstrate the effectiveness of the framework within the overall supply change risk management strategy being implemented.

Is the ERO supportive of the ability to take advantage of other federal processes (FedRamp,. CMMC, etc.) as potential frameworks to leverage as well as certifications?

The utilization of frameworks in an entity's supply chain risk management program can be implemented. It is the responsibility of the entity to demonstrate the effectiveness of the framework within the overall supply change risk management strategy being implemented.

If the entity uses a third-party assessment or certification to assess supply chain risk, does the ERO believe further actions are necessary?

Third-party assessments or certifications can be an acceptable input into the overall cyber security risk(s) assessment implemented by the entity. However, entities should ensure the identification and assessment of cyber security risk(s) to the Bulk Electric System specifically address the entities applicable Cyber Assets

from vendor products or services. Entities are expected to mitigate all identified risks as dictated by their SCRM plan. Mitigation of all identified risks may include adding new controls or leveraging existing controls.

If an entity uses a third-party assessment or certification to assess supply chain risk, does the ERO require the output to be submitted as evidentiary material?

The entity determines which evidentiary artifacts are appropriate to demonstrate adherence to the Standard Requirements. These elements should be documented within the SCRM Plan and/or presented during an audit engagement. These artifacts individually or collectively should be able to demonstrate reasonable assurance of adherence to the applicable Standard Requirements.

If a third-party certification identifies potential gaps for a supplier, meaning either, information provided by a supplier is not substantiated by the assessor or the assessor determines there is a deficiency in performance, will the ERO request evidence for how the entity addressed the gap? Does the ERO perceive not fully addressing the gap, or not addressing the gap to the ERO's satisfaction, is a noncompliance? What evidentiary material would the registered entity need to provide?

Entities are expected to mitigate all identified risks using mitigation strategies as documented within the SCRM Plan. Additionally, mitigation of all identified risks may include adding new controls or leveraging existing controls.

Does the ERO believe that contracts will be considered evidence material in audits?

The entity determines which evidentiary artifacts are appropriate to demonstrate adherence to the Standard Requirements. These elements should be documented within the SCRM Plan and/or presented during an audit engagement. These artifacts individually or collectively should be able to demonstrate reasonable assurance of adherence to the applicable Standard Requirements. However, a contract itself does not show compliance. Evidence should show that controls in the SCRM plan are implemented that meet the requirements of the Standard.

If contracts are considered as evidence, will the ERO be looking for specific clauses and would the absence of any clause be deemed a noncompliance?

The entity determines which evidentiary artifacts are appropriate to demonstrate adherence to the Standard. These elements may be documented within the SCRM Plan and/or presented during an audit engagement. These artifacts individually or collectively should be able to demonstrate reasonable assurance of adherence to the applicable Standard Requirements. The absence of a contractual clause may present more risk and the CEA could test for Standard adherence.

Many contracts contain audit provisions, but registered entities are not resourced to audit the supply chain or the vendor community and suppliers are not resourced to have every customer conduct its own on-site audit. What is the ERO position or perspective about audits of the supply chain or vendor

community? Does the ERO perceive that third-party assessments or certifications by qualified assessors provide the same or greater assurance as on-site audits by the entity?

The utilization third-party assessments or certifications within an entity's supply chain risk management program can be implemented. It is the responsibility of the entity to demonstrate the effectiveness of the third-party assessments or certifications within the overall supply change risk management strategy being implemented. The entity is expected to follow their SCRM plan. If the plan directs the Entity to audit their vendor(s), then it will be incumbent on the Entity to do so accordingly. The Entity needs to be aware of this from a contract standpoint.

Under R1.1, will the ERO be requesting to see the methodology for how an entity compares suppliers' risks and uses that assessment in their procurement determinations if the methodology is not specified in the plan?

The entity determines which evidentiary artifacts are appropriate to demonstrate adherence to the Standard Requirements. These elements should be documented within the SCRM Plan and/or presented during an audit engagement. These artifacts individually or collectively should be able to demonstrate reasonable assurance of adherence to the applicable Standard Requirements.

In instances of sole source suppliers or similar situations that supply unique and "impossible to find elsewhere" products where entities do not have other options. Is there potential for an entity, having performed a risk assessment and accepted risk in accordance with their methodology in R1, to be at a disagreement with an auditor and face a non-compliance over what risk can be accepted and what cannot? Alternatively, how would this be handled?

Entities are expected to mitigate all identified risks using mitigation strategies as documented within the SCRM Plan. The mitigation strategy implemented should be consistent with the entity SCRM Plan. Additionally, any mitigation strategies implemented should be supported by the implemented cyber security risk(s) assessments, business decisions, and the SCRM Plan.

How will the ERO Enterprise address risks with third-party certification vendors that are identified during an audit of a registered entity? Will these risks be brought up during the audit of another registered entity who uses the same vendor?

It is expected that every entity will have a different risk profile, so risks identified for one may be different that those identified for another. Depending on the facts and circumstances, identified risks associated with a particular vendor utilized by other entities may prompt additional internal control discussions.

What is a registered entity supposed to do if they are notified by a vendor of a risk or deficiency, but contractually they cannot share?

Registered Entities should ensure that provisions are included in their contractual agreements, 3rd party assessments, or internal controls are implemented such that if a vulnerability is found or identified by a

vendor, all regulatory compliance requirements can be met (R1.2.4). For example, releasing information to regulatory authorities via evidence submission.