North American Transmission FORUM

Community Confidentiality Candor Commitment

Cyber Security Supply Chain Risk Management Guidance

Version 1.0
Approval Date: 06/20/2018

Versioning

Version History

Date	Version	Notes
06/20/2018	1.0	Initial version

Review and Update Requirements

- Review: every 3 years
- Update: as necessary

Contents

About the NATF

The North American Transmission Forum (NATF) promotes excellence in the reliability, resiliency, and security of the electric transmission system. The NATF is built on the principle that the open and candid exchange of information among its members is the key to continuously improving the operation of transmission systems in the U.S. and Canada. NATF members include investor-owned, state-authorized, municipal, cooperative, U.S. federal, and Canadian provincial utilities, and ISOs/RTOs. For more information visit: http://www.natf.net.

Executive Summary

Cyber security supply chain risk management (C-SCRM) is an important aspect of resilient and reliable Bulk Electric System operations. As cyber security supply chain risk evolves, many entities are facing challenges associated with managing this risk. The NATF developed and published this document to describe best and leading practices for establishing and implementing a cyber security supply chain risk management plan, including procurement, specification, vendor requirements, and managing existing equipment activities. The hallmarks of the described approach include:

- **Foundational Practices**: Cyber security supply chain risk management requires coordination between supply chain risk management efforts and cyber security risk management efforts. Existing cyber security and supply chain framework best practices provide a foundation for building an effective cyber security risk management strategy.

- **Organization-Wide Coordination**: Effective cyber security supply chain risk management is supported by all layers of the business, including various business functions, and is implemented throughout the system-development life cycle.

- **Risk Management Processes**: Cyber security supply chain risk management is implemented as part of overall enterprise risk management activities. Execution involves identifying and assessing applicable risks, selecting appropriate mitigating activities, developing a plan to document policies and mitigating activities, and monitoring performance against this plan. Several methods are discussed within this paper; but because cyber security supply chain risk differs across and within entities, the plan should be tailored to individual organizational contexts.

  Define Criteria: Define cyber security supply chain objectives/criteria to assess a supplier's ability to meet and exceed an entity's cyber security objectives.

  Evaluate Risk: Evaluating supplier risks by obtaining an independent assessment or by obtaining responses to an entity-developed questionnaire, describing how the supplier's business operations and controls for providing BES Cyber Systems and/or related services meet an entity's cyber security criteria/objectives.

  Respond to Risk: Residual risks associated with a supplier's BES Cyber System and/or related service should be quantified and addressed. Further, entities should periodically reassess cyber security supply chain risks presented by existing suppliers and BES Cyber Systems and/or related services.

This document describes business practices that are focused on cyber security supply chain risk mitigation generally and go beyond complying with the NERC CIP-013 Reliability Standard[1]. To augment these best practices, the NATF is also providing suggested Implementation Guidance describing how these business practices and associated work product could be used to demonstrate compliance with CIP-013-1 Requirement R1. This Implementation Guidance builds on both Implementation Guidance written by the CIP-013-1 Standard Drafting Team[2] and the "ERO Enterprise Guide for Internal Controls" version 2 (2017).[3]

Lastly, this whitepaper has and will continue to be vetted across the industry and in public forums in order to support the development and sharing of best and leading practices in cyber security supply chain risk management, including procurement, specification, vendor requirements, and managing existing equipment activities.[4]

[1] https://www.ferc.gov/whats-new/comm-meet/2018/011818/E-2.pdf
[2] *See* Implementation Guidance for CIP-013 (2017)
[3] http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Guide_for_Internal_Controls_Final12212016.pdf
[4] *See* NERC Board of Trustees' Resolution (August 2017): https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf

Background: The Need for a Cyber Security Supply Chain Risk Management Plan

Utility companies depend on supplier products and services to support reliable operations. Enterprises have found great advantages in globalization, outsourcing, supply-base rationalization, just-in-time deliveries, and lean inventories. In addition, many utilities consolidate operations both internally and externally to realize economies of scale.

Globalization, extended supply chains, and supplier consolidation offer significant benefits, including lowering operational cost, which also results in customer savings; interoperability; rapid innovation; a variety of product features; and choice among competing vendors. Commercial off-the-shelf products are proprietary or open source and immediately meet the needs of a global group of energy and other sector customers. Unfortunately, the same factors offering significant benefits may increase the risk of a threat event that could directly or indirectly result in adverse impact to BPS reliability. Several recent events have highlighted this risk to energy sector regulators and energy providers.

> *In 2012, an industrial automation company disclosed that attackers installed malicious software and stole project files related to a SCADA offering[5]. In December of 2015, unauthorized code was found in Juniper Networks' firewall solution that could allow remote procedure execution[6]. Most recently, an anti-virus company was implicated for an alleged foreign entity backdoor built into their security products[7]. Once these products are in place and engaged in the transfer of sensitive reliability information, it is difficult to protect against live threats.*

Regulators and practitioners agree effective supply chain risk management is essential to the reliability of the Bulk Electric System. As technology threats continue to evolve with innovation, both the definition of cyber security supply chain risk and the business practices to address this risk need to evolve. Said simply: cyber security supply chain risk management (C-SCRM is an evolving field.

In this document, the NATF outlines an approach to C-SCRM. This document provides a framework for collecting, developing, and implementing best practices for C-SCRM. It focuses on:

- procurement processes through framing risk and establishing security objectives;
- setting of specifications for identifying and assessing risk;
- setting of vendor requirements, thereby enabling entities to better control risk and facilitating the monitoring of risk;
- establishing practices to review, and as necessary, adjust security practices, as risk profiles associated with existing equipment change.

The NATF's Cyber Security Supply Chain Risk Management Guidance document is meant to assist bulk power system users, owners, and operators with C-SCRM and related processes. Approaches for identifying, evaluating, controlling, and monitoring cyber security supply chain risk will differ across individual utilities,

[5] https://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/
[6] https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/
[7] https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html

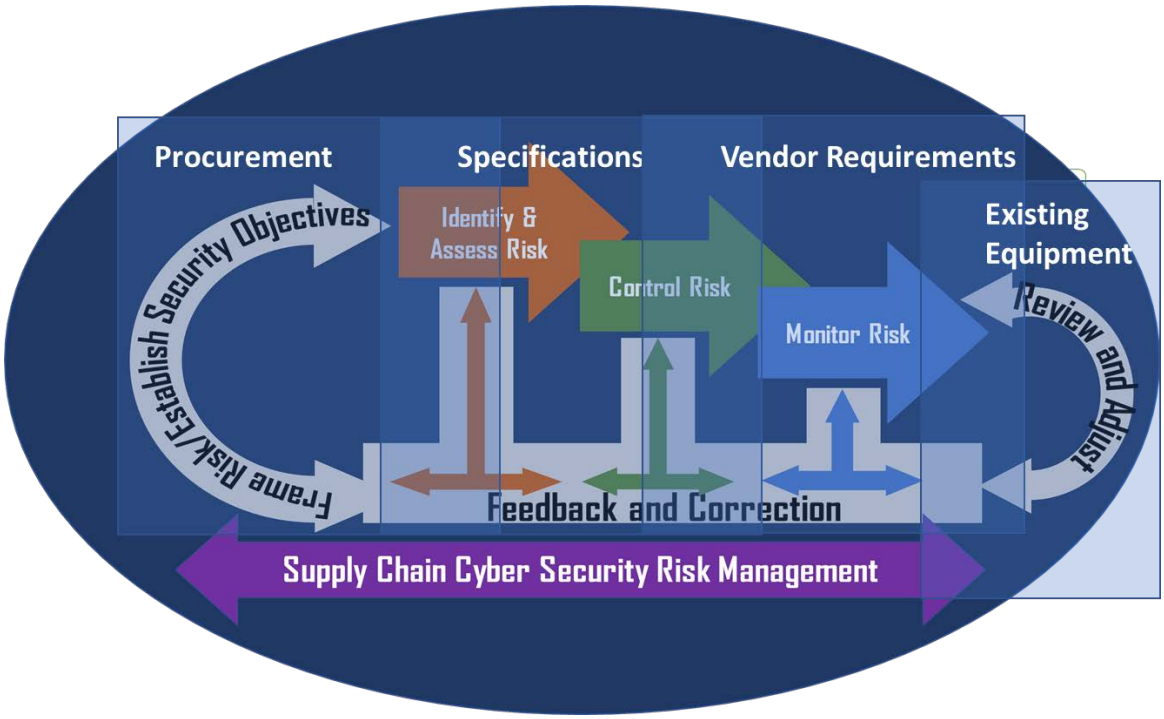
depending on their size, nature of their extended supply chains, and their own risk exposures. Rather than prescribing a specific approach to C-SCRM, this document highlights several possible approaches a utility may consider, including examples of tools used successfully by NATF members. Individual utilities will likely adapt ideas presented in this document to fit their unique characteristics and expand the depth and breadth of processes to meet explicit organizational requirements.

This document seeks to foster the development of best practices related to cyber security supply chain risk management for technical application in utility settings, rather than providing a regulatory framework for implementation. In Order No. 706-A, FERC stated "there is an important distinction between a Reliability Standard and a guidance document. While a Reliability Standard sets forth mandatory and enforceable compliance obligations, a guidance document should provide valuable assistance to responsible entities on how to achieve compliance with the requirements of a Reliability Standard. A guidance document, however, is not binding and cannot be the subject of an enforcement action, unless it is incorporated into a Reliability Standard." With implementation of the NERC CIP-013-1 standard, this document will identify components of these best practices that could be used as part of a C-SCRM strategy.

This is a dynamic and living document. The current content reflects a collection of best-practice inputs from NATF members. The challenges that C-SCRM aims to address will continue to evolve. The NATF intends that this document will help utilities assess and address cyber security supply chain risks and document evolving practices. We invite collaboration to promote supply chain risk management practices that promote Bulk Electric System reliability and resiliency.

NATF C-SCRM Framework

The NATF approach to cyber security supply chain risk management through best and leading practices in procurement, specification, vendor requirements, and managing existing equipment is depicted in the diagram below, and is described in more detail in the narrative that follows.



Frame Risk, Establish Security Objectives

The C-SCRM strategy is often executed as part of an entity's overall cyber security risk plan, which in turn is an element of the organization's enterprise risk management process. An entity may use existing risk management frameworks to consider cyber security supply chain risk. Many guidance documents are available to help entities identify, assess, and control broad organizational risk[8]. In this document, C-SCRM is identified in terms of this broader risk management strategy. An entity decides whether to manage supply chain risk with one C-SCRM plan or many plans. **Based upon the C-SCRM strategy, critical mission and business drivers (e.g., regulatory or reliability constraints), identified during the enterprise risk management process, provide context for cyber security supply chain risk that is managed within the plan(s).** Mission functions are mapped to system architecture to identify systems, components, and processes critical to the effectiveness of the organization.

Identify Resources

Implementing C-SCRM is most effective when organizations establish a team-based approach to identify, assess, and manage risk. To address all aspects of C-SCRM, it is important to ensure resources from many organizational functions are represented to identify and assess cyber security risk to the entity from its supply

[8] The *NATF Risk Assessment Practices* and *NIST Special Publication 800-30* are two examples of enterprise risk management approaches.

chain. A cross-functional team of subject-matter experts representing the various aspects of the supply chain life cycle will yield the most comprehensive risk assessment, enable effective communication with internal and external stakeholders and partners, and foster organizational consensus regarding appropriate resources for managing cyber security supply chain risk. The entity should engage the following areas:

- Business operations (i.e., transmission operations and planning, field services engineering, system operations)
- Cyber security
- Information technology / operational technology
- Supply chain contracting, acquisition, and procurement
- Risk management and compliance
- Legal

Develop Entity C-SCRM Strategy

There are many different approaches that entities take to develop its C-SCRM strategy (e.g., a C-SCRM plan per supplier, per BES Cyber Asset or BES Cyber System type, or for the enterprise). Examples include the following:

- **Enterprise Strategy** – Entity develops a single C-SCRM plan to identify and assess cyber security risk for all hardware, software, and services (e.g., the entity has one C-SCRM plan that identifies and assesses cyber security risk regardless of asset type, software, service, or supplier).
- **Supplier Strategy** – Entity develops a C-SCRM plan to identify and assess cyber security risk for each supplier or services provider (e.g., entity has a separate C-SCRM plan for each different vendor for workstations, even if used for similar function).
- **Asset Type Strategy** – Entity develops a C-SCRM plan to identify and assess cyber security risk for a type of asset or service being acquired (e.g., entity has a separate C-SCRM plan for energy management system than substation relays).
- **Hybrid Strategy** – Entity develops a template C-SCRM plan to identify and assess cyber security risk and develops a C-SCRM plan for a combination of hardware, software, and services at a point in time (e.g., entity may develop a C-SCRM plan for all types of hardware, software, and services being acquired during a project).

Each entity decides which approach is most effective and efficient for its organization. Whichever approach an entity chooses, the entity considers how changes in risk profile and the cyber security policy will be addressed in the C-SCRM plan(s). Additionally, because C-SCRM involves a variety of stakeholders, organizational change management must be considered with any approach. One approach may be easier initially with respect to organizational change management, while another is more challenging initially but simplified in the longer term.

For instance, while the enterprise approach may appear more daunting initially, it could prove more sustainable long term. Multiple plans may require more tracking as to which C-SCRM plan is associated with which asset, or more document management and organizational change management may be required when the entity risk profile or cyber security policy changes. A supplier approach may provide efficiency and ease in negotiation as

the supplier risks are known; however, this approach could allow risk to remain as cyber security policy is updated and not brought into C-SCRM plan for the specific supplier.

Each entity decides which approach is most effective within its organizational context and whether that approach changes over time. Regardless of whether an entity has one or many C-SCRM plans, each plan addresses the risk to the entity for the specific hardware, software, or services being acquired to perform or support a BES Reliability Operating Service.

Identify and Assess Risk in the Context of C-SCRM Strategy

Using the selected risk assessment approach, **the entity identifies risks associated with the product or service being procured**. The assessment includes an analysis of likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the information system (industrial control system hardware, software, and computing and networking services), or portion thereof, being procured and the information it processes, stores, or transmits. The risk assessment considers threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the BES, based on the operation and use of the third-party product or service.

Measure Entity Risk Exposure and Set Vendor Requirements

The entity considers its individual company's risk exposure when it develops its C-SCRM plan. Whether the entity has one or many C-SCRM plans, the entity considers its own risk exposure which could vary based upon leadership, function, company strategy, security defense-in-depth considerations, and a wide variety of other factors. **The entity considers the following entity-specific inputs, among others, with respect to its own risk exposure when developing its C-SCRM plan**:

- Usage/function of hardware or software
- Physical location of hardware or software
- Quantity of hardware, software, and/or services from one supplier
- Type of access (read or control) provided to supplier
- Type of information provided to or accessible by supplier
- Quantity of information provided to or accessible by supplier
- Service being provided by supplier
- Technology strategy
- Supplier history
- Financial impact to change supplier
- Reliability impact to change supplier
- Entity supply chain process – master services agreement, contract addendums

Regardless of size or specific role in grid reliability or whether an entity has one or many C-SCRM plans, each entity ensures its cyber security policy is considered when identifying and assessing risk for the hardware, software, or services being acquired or used to perform or support a BES Reliability Operating Service (BROS).

Additionally, the C-SCRM plan(s) must be aligned with the entity's overall risk profile. Simply stated, each C-SCRM plan considers the risk to the entity for the specific hardware, software, or services being acquired or used and is aligned to the entity's risk tolerance and cyber security policy. While considering appropriate risk exposure for the hardware, software, or service acquired, **the entity considers specific cyber security criteria** (**see attachment A**) **and known security frameworks (see attachment B) for implementation by the vendor**.

The C-SCRM plan(s) identifies what aspects of the entity's cyber security policy are required of the supplier for the hardware, software, or services performing a BROS. Additionally, the entity determines whether the C-SCRM plan covers only hardware, software, or services supporting a BROS or also includes Electronic Access Control or Monitoring Systems (EACMS) Cyber Assets, Physical Access Control Systems (PACS) Cyber Assets, and Protected Cyber Assets. If the entity determines supporting assets and services are not covered by the C-SCRM plan, the entity considers the risk that could be introduced into its environment from vendor products and services and how that risk is mitigated.

Managing Cyber Security Criteria for Supply Chain

The C-SCRM plan(s) **prioritize cyber security criteria**. For entities with multiple C-SCRM plans, it is beneficial if the **cyber security policy criteria are consistent** across the C-SCRM plans. Additionally, **the entity documents in the C-SCRM plan(s) what level of organizational approval is required in the supply chain process**. While most organizations have some type of financial delegation of authority within their supply chain process, the C-SCRM plan(s) should consider if a cyber security risk acceptance delegation of authority needs to be included. An entity may state in the plan what level of individual may approve acquisitions and the conditions under which delegations are permitted.

The **entity can take a variety of approaches to document its cyber security criteria**. The format chosen is intended to encourage usability and adoption by the many C-SCRM stakeholders and the complexity of the organizational model. For example, an entity that has the same requirements and guidelines across all types of hardware, software, and services may develop a more simplified process, whereas an entity that has different requirements for diverse types of hardware/software or few requirements and many guidelines may have a more complex C-SCRM plan.

Assess Risk and Set Vendor Requirements

As the entity develops the processes to identify and assess cyber security risk from vendor products and services used in procuring and installing vendor equipment and software or transitioning from one vendor to another, **the utility also identifies the criteria necessary to manage the risk** associated with acquiring certain vendor services, equipment, and/or software associated with BES Cyber Systems[9].

Entities address supply chain risk in vendor procurement language and include a right to audit a vendor at any time[10].

[9] As defined in the NERC Glossary

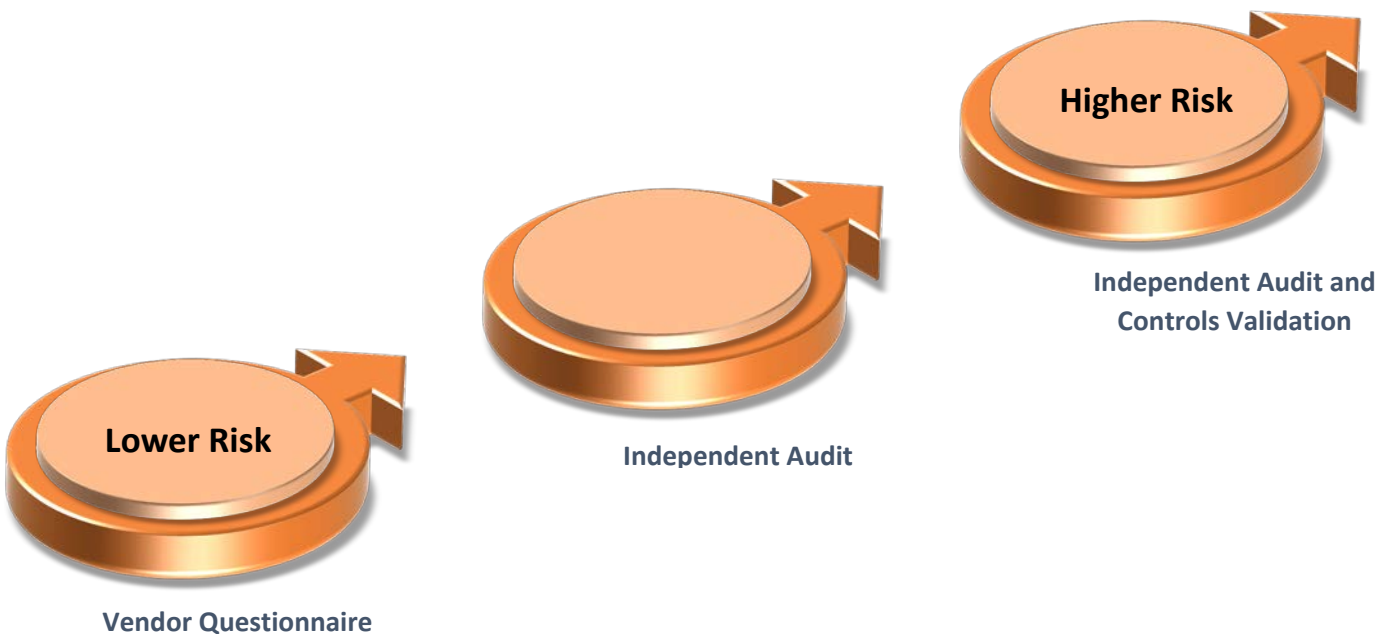
[10] For example, an entity could propose procurement language that gives the entity the right to request documentation of a supplier's cyber security program, including recent assessment results, or the ability to conduct periodic on-site security assessments at the supplier's facilities, and that such assessments could be conducted by an independent third-party, at the discretion of the entity. *See*, for example, Energy Sector Control Systems Working Group "Cybersecurity Procurement

An **entity with defined criteria and/or reliance on known security frameworks (see attachments A and B) to manage risk associated with acquiring the BES Cyber System from the vendor can assess the vendor against these criteria**.

To understand the risk posed by a vendor product or service, the utility obtains adequate detail regarding vendor processes and/or practices to evaluate the adequacy of the vendor meeting the specific risks identified in procuring the BES Cyber System and related services. Approaches that utilities consider taking in assessing cyber security supply chain risk include:

1. Request the **vendor respond to questions** describing the ability of the vendor to meet the technical requirements identified in the entity's risk assessment.
2. Request or obtain an **independent assessment** that the vendor can meet technical requirements identified in the risk assessment.
3. Request vendor provide a third-party, **independent assessment** that the vendor can meet technical requirements identified in the risk assessment, **including evaluation of the overall control environment, and verification/testing of specific controls**.

The selection of approach depends on the level of cyber security supply chain risk associated with the hardware, software, or services being acquired or used, as depicted in the diagram below (the higher the risk, the more comprehensive the assessment):



Language for Energy Delivery Systems" p 24 (April 2014): https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf

Request Vendor Self-Assessment/Vendor Questionnaire

An entity may conduct its own assessment of the vendor to assess risk associated with the identified BES Cyber System and related services. The **criteria identified in attachment A is utilized to tailor the assessment to an entity's procurement objectives**. The entity inquires, at minimum, about the six basic criteria, and adds other criteria pertinent to the product or service being procured. This allows the flexibility to assess vendor risk relative to the risk that the product being procured provides to the entity and may be more effective when procuring resources from smaller vendors. This also allows the utility to consider different mitigating activities based on the results of the risk assessment and residual risks that the product poses.

Request Third-Party, Independent Assessment: Relying on the Work of Others

An entity may determine that obtaining **an independent assessment of the vendor's control design and operating effectiveness** for producing and servicing an identified BES Cyber System is important to effectively understand, assess, and prioritize cyber security supply chain risk.[11] This approach could be considered for acquisition of many different cyber-connected systems, including communication systems, energy management systems (EMS), other enterprise software systems, RTUs/PLCs, meters, sensors, intelligent electronic devices, hard disk drives, cables and wires, integrated circuits, digital storage, and even professional services in any area of the organization.

In such cases, an entity may request that a vendor obtain an independent assessment from an auditor with appropriate audit and/or cyber security certifications[12]. Utilities that adopt this approach consider the following:

1. **Request** that vendors provide a qualified, third-party independent assessment, including evaluation of the vendor's overall controls design and verification/testing of specific control activities in place to meet identified criteria in attachment A and attachment B.
2. **Review** the independent assessment's description of the vendor's system (i.e., the vendor's infrastructure, software, personnel, procedures, and data for developing, maintaining, and delivering the identified BES Cyber System and related services).
3. **Review** the vendor management's assertion regarding the description, the design, and operation of its controls.
4. **Review** how the auditor examined the vendor's controls to achieve the identified criteria. Utilities should expect that an independent assessment would not only describe the vendor's controls, but also explain how the auditor tested the controls in the cyber security areas identified by the entity (**see attachments A** and **B**).

[11] Many vendors have already undergone an independent third-party review of their products or services for other regulatory or operational purposes (e.g., an ISO 27001 certification or had a Standards for Attestation Engagements (SSAE) No. 18 SOC 2 audit report). Using already completed vendor evaluations could reduce overall supply chain overhead. *See* Implementation Guidance for CIP-013-1 at p 4, fn. 3.

[12] Professional standards require an audit team to collectively possess the knowledge, experience, education, and skills that allow the team to competently execute an independent review/audit. The NERC Auditor Handbook describes skill sets that should be part of an audit team reviewing reliability risk. *See* ERO Enterprise Compliance Auditor Manual, at p. 190.

5. **Review** whether the assessment identifies any other organizations relied upon by the vendor to develop, maintain, or deliver the identified BES Cyber System and how the vendor manages risk related to its service organizations.

Obtaining an independent assessment of the vendor's controls can provide value to utilities in many ways:

1. **Leveraging experienced and certified auditor expertise.** Relying on an independent auditor leverages expertise in evaluating/verifying/testing control environments in complex organizational and technical environments and allows the utility to focus on responding to identified risk.
2. **Cost-effective.** An independent assessment report can be supplied to numerous registered entities with similar BES Cyber Systems (such as EMS), thereby eliminating redundant work effort for the vendor.
3. **Beneficial to smaller entities**. By relying on independent auditors' evaluations of the overall controls design and testing the operating effectiveness of internal control activities for areas specified by the industry, companies less experienced in supply chain risk management would use the same reports to identify issues associated with supply chain vendor risk management and procurement controls.
4. **Builds on other industries' experiences requiring security controls.** Other industries have recognized the need for standards and guidelines related to cyber security supply chain risk management. The American Institute of Certified Public Accountants (AICPA), the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), and many other organizations have developed robust cyber security frameworks that vendors already follow. Users of these standards require vendors to undergo an independent review to identify and assess cyber security risk associated with the vendor's products or services.

Control Risk in Accordance with Cyber Security Supply Chain Risk Management Plan

It is important for an entity to assess the results of a third-party assessment, or vendor responses to a supplied questionnaire. An entity's C-SCRM team analyzes:

- The auditor's or vendor's **substantiated** description of how supply chain risk is managed in the context of identified cyber security risks that impact an energy company. Additional clarification regarding the vendor's ability to manage risks may be necessary.
- The need for **additional action to mitigate risks** identified by the auditor or that are apparent from the vendor's response to the questionnaires. When assessing the acceptability of the risk, the entity's cyber security supply chain management team may consider such things as:
    - Other tools or processes already in place that could be applied to the procured BES Cyber System and related service;
    - The availability of installing new controls to accompany the procured BES Cyber System and related service, including employing more frequent or more in-depth vulnerability testing;
    - Limiting the use or functionality of the BES Cyber System.

An entity's cyber security supply chain risk management team should document its analysis to support management consideration of any residual risk when procuring a BES Cyber System and related services from a vendor.

Lastly, the utility should consider whether it is appropriate to establish policies directing distinct levels of management approval for the procurement of BES Cyber Systems and related services depending on the nature of the risks associated with the BES Cyber System and related service.

Monitor Risk

Continual Monitoring and Review of Risks and Their Controls

For existing equipment: reassess conditions for ongoing vendor relationships

There are many conditions in an ongoing relationship with a vendor that would necessitate reassessment and/or audit of the vendor by the entity or a qualified third party. Among an entity's cyber security risk management cross-functional team, appropriate individuals within the entity should consider steps to monitor conditions that would give rise to reassessment.

Conditions at the entity that trigger reassessment of the vendor or the BES Cyber System and/or related service may include changes to the following:

- Use of the hardware or software (e.g., BES Cyber Asset(s) will support a Nuclear Plant Interface Requirement)
- Impact rating of the hardware or software (e.g., BES Cyber Asset(s) will be used in a High Impact Control Center and was previously only used in Low Impact site)
- Entity cyber security requirements
- Entity risk profile/tolerance
- Threat landscape of entity
- Threat landscape of industry

Conditions at the vendor that trigger reassessment of the vendor or BES Cyber System and/or related service may include:

- Any type of bankruptcy filing by the vendor or parent company
- Change in control—vendor is acquired by a new owner or corporate restructuring
- Security breach—any major breach that affected customer data from the vendor that is similar to the utility's data or services managed by the vendor
- Vendor changes in technology infrastructure—if vendor makes major changes to any of its infrastructure from initial assessment (i.e., change from internally supplied to an outsourced third-party service supplier)
- Manufacturing location change
- Changes to vendor qualification process
- Utility significant changes to the vendor relationship (i.e., change or increase in services provided by vendor or different security levels required by new span of scope)
- Material changes identified in any independent audit finding reports, certifications, or utility administered assessment results

- Significant or recurring defects identified in supplier-provided services or products

The above is not an all-inclusive list for conditions to prompt a reassessment of the vendor. **Entities should consider including contract terms** for the vendor and utility relationship that require vendor to notify the entity in the event any of the above conditions occur, along with timeframe to notify, so entity can take the appropriate action.

Entities may also consider asking vendors to address these issues as deemed appropriate (e.g., once per calendar year, or once every other calendar year) through independent assessments or through updates to self-assessment questionnaires.

Review and Adjust: Entity Cyber Security Supply Chain Risk Management Plan Review

Cyber security risks change with technology advances and as new vulnerabilities and threat vectors are identified. As such, the entity should ensure the C-SCRM plan(s) evolve as the threats evolve. This ensures that any new risks introduced into an environment are within an entity's risk tolerance.

Conclusion

In summary, the focus of this document is cyber security supply chain risk management and assumes each entity has a cyber security policy that already considers the entity's risk profile. Since the C-SCRM plan(s) will be based upon the entity's cyber security policy, the cyber security policy should be comprehensive and consider evolving threats.

NERC CIP-013-1 Implementation Guidance

NERC states that, “Implementation Guidance provides a means for registered entities to develop examples or approaches to illustrate how registered entities could comply with a standard [or requirement within a Standard] that are vetted by industry and endorsed by the ERO Enterprise. The examples provided in the Implementation Guidance are not exclusive, as there are likely other methods for implementing a standard.”

Therefore, NATF has developed a separate implementation guidance document describing one way that a registered entity could comply with CIP-013-1 R1, and subsequently parts of R2. (*See* “NATF CIP-013-1 Implementation Guidance” at http://www.natf.net/documents.)

Attachment A – Cyber Security Criteria

Notification/Recognition of Cyber Security Incidents

Vendors need to be able to identify when an incident occurred to ensure that the vendor can notify the entity in the case of an incident. To meet this requirement, the vendor may have aligned with numerous cyber security frameworks (see table 1 in attachment B).

Coordination of Responses to Cyber Security Incidents

Vendors should coordinate with the entity their responses to incidents related to the products or services provided to the entity that pose cyber security risk to the entity. To meet this requirement, the vendor may have aligned with numerous cyber security frameworks (see table 1 in attachment B).

Notification when Remote or Onsite Access is No Longer Needed or Should No Longer be Available to Vendor Representatives

Vendors should respond accordingly to personnel changes. A vendor should be able to tell the entity when a personnel change occurs that could impact whether or not remote access should still be available to vendor representatives. To meet this requirement, the vendor may have aligned with cyber security frameworks that control use of administrative privileges and/or control access based upon a need to know (see table 1 in attachment B).

Vulnerability Identification

Vendors are to notify an entity when a vulnerability related to a product or service is identified. In order to meet this obligation, a vendor needs to know when a vulnerability exists in their environment. To meet this requirement, the vendor may have aligned with cyber security frameworks that require continuous vulnerability assessment and mitigation (see table 1 in attachment B).

Verification of Software Integrity and Authenticity of all Software and Patches Provided by the Vendor for Use in BES Systems

Vendors are to provide the capability to ensure the integrity and authenticity of all software and patches provided to an entity. In order to meet this obligation, a vendor may have aligned with cyber security frameworks that require application software security (see table 1 in attachment B).

Coordination of Controls for Vendor-Initiated Interactive Remote Access and System-to-System Remote Access with a Vendor

Vendors must coordinate with entities to control vendor-initiated interactive remote access and ensure system-to-system remote access with a vendor is appropriately managed. To meet this requirement, the vendor may have aligned with cyber security frameworks that require account monitoring and control (see table 1 in attachment B).

At a minimum, the vendor should align with the above 6 basic principles of cyber security. The entity may define additional criteria for any vendor, as described below.

As an entity performs a risk assessment and considers risk exposure of products or services to be procured in its environment, additional cyber security controls may be necessary to protect the entity's operating environment. An entity may consider obtaining and evaluating additional information regarding the vendor's capabilities with respect to the following security areas.

Asset, Change, and Configuration Management

Inventory of Authorized and Unauthorized Devices

- Physical devices and systems within the organization are inventoried
- Software platforms and applications within the organization are inventoried
- Organizational communication and data flows are mapped
- External information systems are catalogued

Change Control and Configuration Management Considerations

- Uses a recognized framework for its information technology processes (e.g., ITIL)
- Includes security in its system development life cycle
- Has a mature change-control process
- Maintains separate development and production environments
- Maintains separate environments for different customers
- Has mechanism for software integrity (e.g., PKI with encryption, digital signature)
- Product allows for hardening to minimize attack surface
- Processes to identify, discover, inventory, classify, and manage information assets (hardware and software)
- Processes to detect unauthorized changes to software and configuration parameters
- Able to identify whether hardware, software, or components are U.S. and/or internationally sourced

Governance

Establish and Implement Security Awareness Program

- Documented and implemented security policy and procedures
- All users are informed and trained on cybersecurity policies and procedures
- Third-party stakeholders understand roles and responsibilities and are accountable to same requirements
- Senior executives understand roles and responsibilities
- Physical and information security personnel understand roles and responsibilities
- Ability to provide ongoing support for software and hardware
- Personnel background checks
- Ability to retain data for events such as litigation holds, cyber security incidents

- Presence of trained, knowledgeable, and sufficient cyber security resources
- Supplier has certifications for manufacturing process (e.g., ISO)

Logging and Monitoring Considerations:

- Maintains a program to perform continuous logging, monitoring, and analysis of its systems to identify events of significance
- Has sufficient segregation of duties to ensure logging and monitoring are effective to detect anomalies

Information Protection Considerations

- Uses appropriate controls to manage data at rest (vendor or entity data)
- Ability to provide additional hardware for failures
- Encrypts credentials in transit, internal and externally
- Encrypts credentials at rest
- Uses strongest standard encryption algorithms (e.g., AES or SHA-2)
- Supplier physical access controls to hardware, software, and manufacturing centers
- Physical devices and systems within the organization are inventoried
- Supplier location of data centers (U.S./Canada-based vs international)

Attachment B – Cyber Security Framework Mapping

Entities use appropriate subject matter experts to develop cyber security policy. Various security frameworks that entities may find useful for developing their cyber security policy are mapped in table 1 below. **Table 1 provides example mapping and is not an all-inclusive list.**

Notable cyber security frameworks and best practices include:

- Center for Internet Security (CIS) Critical Controls
- NIST Cyber Security Framework
- PCI DSS
- HIPAA
- COBIT 5
- AICPA SOC 2 and SOC 3 Trust Services Criteria
- NATF Security Principles of Excellence
- NERC Reliability Standards

Table 1: Cyber Security Framework Mapping

NERC CIP-013	Critical Security Control	NIST Cybersecurity Framework	PCI DSS 3.2	HIPAA	COBIT 5	AICPA SOC 2 & SOC3 Trust Services Criteria (TSP Section 100)	NERC CIP v7
1.2.1/1.2.2 Notification by the vendor of, and 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	*Critical Security Control #19: Incident Response and Management*	*PR.IP-9* *PR.IP-10* *DE.AE-2* *DE.AE-4* *DE.AE-5* *DE.CM-1-7* *RS.RP-1* *RS.CO-1-5* *RS.AN-1-4* *RS.MI-1-2* *RS.IM-1-2* *RC.RP-1* *RC.IM-1-2* *RC.CO-1-3*	*12.10*	*164.308(a)(6): Security Incident Procedures - Response and Reporting R*	*APO13: Manage Security DSS05: Manage Security Services DSS02: Manage Service Requests and Incidents*	*CC2.3* *CC7.1-CC7.5* *CC9.2*	*CIP-008-5 R1* *CIP-008-5 R2* *CIP-008-5 R3*
1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives	*Critical Security Control #5: Controlled Use of Administrative Privileges* *Critical Security Control #14: Controlled Access Based on the Need to Know*	*PR.AC-4* *PR.AC-5* *PR.AT-2* *PR.DS-1* *PR.DS-2* *PR.IP-8* *PR.MA-2* *PR.PT-2* *PR.PT-3*	*1.3 - 1.4* *2.1* *4.3* *7.1 - 7.3* *8.1 - 8.3* *8.7*	*164.308(a)(1): Security Management Process - Information System Activity Review R* *164.308(a)(4): Information Access Management - Isolating Health care Clearinghouse Function R* *164.308(a)(4): Information Access Management - Access Authorization A* *164.310(b): Workstation Use - R* *164.310(c): Workstation Security - R* *164.312(a)(1): Access Control - Encryption and Decryption A* *164.312(c)(1): Integrity - Mechanism to Authenticate Electronic Protected Health Information A* *164.312(a)(1): Access Control - Automatic Logoff A* *164.312(d): Person or Entity Authentication - R* *164.312(e)(1): Transmission Security - Integrity Controls A* *164.312(e)(1): Transmission Security - Encryption A*	*APO13: Manage Security DSS05: Manage Security Services*	*CC5.2* *CC6.1-CC6.4* *CC9.2*	*CIP-004-6 R4* *CIP-004-6 R5* *CIP-005-5 R1* *CIP-005-5 R2* *CIP-007-6 R4* *CIP-007-6 R5* *CIP-011-2 R1*

NERC CIP-013	Critical Security Control	NIST Cybersecurity Framework	PCI DSS 3.2	HIPAA	COBIT 5	AICPA SOC 2 & SOC3 Trust Services Criteria (TSP Section 100)	NERC CIP v7
1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity	Critical Security Control #4: Continuous Vulnerability Assessment and Remediation	ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5 ID.RA-6 PR.IP-12 DE.CM-8 RS.MI-3	6.1 6.2 11.2	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	APO13: Manage Security DSS05: Manage Security Services	CC2.3 CC3.2 CC 6.1 CC 7.1-CC7.2 CC9.2	CIP-007-6 R2 CIP-010-3 R3
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	Critical Security Control #18: Application Software Security	PR.DS-6 PR.DS-7 PR.IP-1 PR.IP-2 PR.IP-3 PR.MA-1	6.3 6.5 - 6.7		APO13: Manage Security DSS05: Manage Security Services	CC 6.8	
1.2.6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s)	Critical Security Control #16: Account Monitoring and Control	PR.AC-1 PR.AC-3 PR.AC-4 PR.PT-3	7.1 - 7.3 8.7 - 8.8	164.308(a)(1): Security Management Process - Information System Activity Review R 164.308(a)(4): Information Access Management - Access Authorization A 164.308(a)(4): Information Access Management - Access Establishment and Modification A 164.308(a)(5): Security Awareness and Training - Password Management A 164.312(a)(1): Access Control - Unique User Identification R 164.312(a)(1): Access Control - Automatic Logoff A 164.312(d): Person or Entity Authentication - R 164.312(e)(1): Transmission Security - Integrity Controls A 164.312(e)(1): Transmission Security - Encryption A	APO13: Manage Security DSS05: Manage Security Services	CC5.2 CC 6.1 -CC6.3 CC6.6 CC6.7	CIP-005-5 R1 CIP-005-5 R2 CIP-007-6 R4
Asset, Change, and Configuration Management	Critical Security Control #1: Inventory of Authorized and Unauthorized Devices	DE.AE-1 ID.AM-1 ID.AM-3 ID.AM-4 PR.AC-2 PR.DS-3	2.4	164.310(b): Workstation Use - R 164.310(c): Workstation Security - R	APO13: Manage Security DSS05: Manage Security Services BAI09: Manage Assets	CC6.1 CC6.8 CC7.1 CC8.1	CIP-002-5.1 R1 CIP-002-5.1 R2

NERC CIP-013	Critical Security Control	NIST Cybersecurity Framework	PCI DSS 3.2	HIPAA	COBIT 5	AICPA SOC 2 & SOC3 Trust Services Criteria (TSP Section 100)	NERC CIP v7
Governance	Critical Security Control #17: Security Skills Assessment and Appropriate Training to Fill Gaps	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5 PR.IP-11	12.6	164.308(a)(5): Security Awareness and Training - Security Reminders A 164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A 164.308(a)(5): Security Awareness and Training - Log-in Monitoring A 164.308(a)(5): Security Awareness and Training - Password Management A	APO13: Manage Security DSS05: Manage Security Services	CC1.4, CC2.2, CC6.1 CC9.2	CIP-004-6 R1 CIP-004-6 R2
Information Protection	Critical Security Control #13: Data Protection	PR.DS-1 PR.DS-2 PR.DS-5 PR.IP-4 PR.IP-5 PR.IP-6 PR.IP-7 PR.PT-2 PR.PT-4	1.3 - 1.4 4.3 7.1 - 7.3 8.7	164.308(a)(4): Information Access Management - Isolating Health care Clearinghouse Function R 164.310(d)(1): Device and Media Controls - Accountability A 164.312(a)(1): Access Control - Encryption and Decryption A 164.312(e)(1): Transmission Security - Integrity Controls A 164.312(e)(1): Transmission Security - Encryption A	APO13: Manage Security DSS05: Manage Security Services	CC6.1-CC6.5 CC6.7 CC8.1 CC9.2 C1.1-C1.2	CIP-011-2 R1
Logging and Monitoring	Critical Security Control #3: Secure Configurations for Hardware and Software	DE.AE-3 DE.DP-1 DE.DP-2 DE.DP-3 DE.DP-4 DE.DP-5 PR-PT-1	10.1 - 10.9	164.308(a)(1): Security Management Process - Information System Activity Review R 164.308(a)(5): Security Awareness and Training - Log-in Monitoring A	APO13: Manage Security DSS05: Manage Security Services	CC7.1 - CC7.3	CIP-007-6 R4