North American Transmission FORUM

Community Confidentiality Candor Commitment

NATF Supply Chain Risk Management Guidance

Disclaimer
This document was created by the North American Transmission Forum (NATF) to facilitate industry work to improve reliability and resiliency. The NATF reserves the right to make changes to the information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. "North American Transmission Forum" and its associated logo are trademarks of NATF. Other product and brand names may be trademarks of their respective owners. This legend should not be removed from the document.

Version 2.0
Document ID: 1098
Approval Date: 09/15/2023

Versioning

Version History

Date	Version	Notes
06/20/2018	1.0	Initial version
09/15/2023	2.0	Revised to incorporate updated resources and implementation guidance

Review and Update Requirements

- Review: every 5 years
- Update: as necessary

This document supersedes the *NATF Cyber Security Supply Chain Risk Management Guidance*, developed in response to the NERC Board of Trustees' August 2017 request that the NATF "develop white papers to address best and leading practices in supply chain management, including procurement, specifications, vendor requirements and existing equipment management, that are shared across the membership of each Forum, and to the extent permissible under any applicable confidentiality requirements, distribute such white papers to industry."[1]

This document provides a summary overview of supply chain risk management practices and related resources developed by the NATF and made available to industry and suppliers on the NATF's public website at https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

[1] *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

Contents

About the NATF

The mission of the North American Transmission Forum (NATF) is to promote excellence in the safe, reliable, secure, and resilient operation of the electric transmission system through a set of integrated programs and activities, including peer reviews, assistance, training, practices, surveys, metrics, operating experience, and initiatives. The NATF is built on the principle that the open and candid exchange of information among its members is the key to continuous improvement. NATF members and affiliates include investor-owned, state-authorized, municipal, cooperative, U.S. federal, Canadian provincial utilities, and ISOs/RTOs, representing about 90% of the net peak demand and 85% of the transmission circuit miles (100 kV and above) in the U.S. and Canada.

For more information visit: https://www.natf.net.

Executive Summary

Supply chain risk management (SCRM) is a continuously evolving and expanding facet of the modern bulk power system and represents an increasingly crucial element of its resilient and reliable operation. As risks to the supply chain increase, so do the challenges entities face when working to manage and mitigate them.

To help industry address these risks, the NATF has developed this document to highlight applicable resources and leading practices for establishing and implementing an SCRM plan, assessing supplier risk, leveraging the work of others, and helping to advance entities' own SCRM programs.

Key aspects of this approach include:

- **Core practices:** Effective SCRM programs require the use of well-defined processes and practices that are effectively integrated into all parts of the procurement process. These practices must be understood and internally promulgated to be maximally effective.
- **Industry convergence:** Avoiding duplicative efforts is not only necessary to improve the efficiency of an SCRM program, but also to obtain high-quality data in a consistent format that permits ready analysis and the identification of risks, trends, and other important elements. By converging on leading industry practices and tools, these goals may be obtained.
- **Program maturity:** As an entity continues to improve its SCRM program, additional opportunities exist to further integrate and mature the program into a more holistic, organization-wide approach that seeks to address risk and advance the entity's operations.

It is important to note that this document and NATF-developed resources focus on SCRM topics broadly and go above and beyond compliance with relevant NERC CIP Reliability Standards. Where relevant, the NERC CIP Reliability Standards and NERC-endorsed guidance are referenced for the benefit of bulk power system owners, operators, and suppliers, and understanding how this guidance document may support or enhance regulatory compliance efforts – however, the focus will remain that of promoting superior practices for the benefit of industry.

The field of SCRM continues to grow, and as new guidance, industry approaches, and solutions are created or accepted, this document will continue to evolve to address supply chain risks and core resources available to mitigate them.

Background: The Need for a Supply Chain Risk Management Plan

In order to provide reliable, safe, and effective power, utilities and similar entities depend on a variety of suppliers. As supply chains become increasingly globalized, distributed, and outsourced, entities can realize economies of scale and other efficiencies that would not be otherwise possible. For example, manufacturers can locate production and design centers in areas that best support the work needed, resulting in greater competition and reduced customer costs. Similarly, access to many commercial off-the-shelf products and services allows for greater choice and rapid integration in a variety of operational environments.

However, the very elements that provide many of these benefits often come with their own concomitant set of risks and challenges that must also be addressed. Unfortunately, there have been several examples in recent history that demonstrate the ways in which supply chain vulnerabilities can be exploited to cause significant impact to entities and their operations. In 2020, an advanced persistent threat (APT) compromised a software manufacturer and planted malware in its products, affecting thousands of customers. In 2021, attackers used a stolen credential to deploy ransomware to a utility, causing service impacts over several days. More recently, in 2023, a service provider was the victim of a supply chain attack which led to malicious code being deployed to its customers via automated and manual software updates.

As technology threats continue to advance in novel and often unexpected ways, the business practices designed to address these risks must similarly continue to evolve. Both regulators and practitioners agree that effective SCRM is essential to the reliability of the bulk power system. As in many areas of security and risk management, a static approach becomes increasingly untenable in light of the rapidly changing threats that entities face on a daily basis.

In this document, the NATF outlines an approach to SCRM developed in collaboration with industry entities, suppliers, solutions providers, and trade associations that provides a framework for collecting, developing, and implementing leading practices for SCRM. It provides:

- A model for approaching the risk assessment process;
- Resources for various phases of the risk assessment;
- Guidance for leveraging third-party certifications and assessments;
- Considerations for internal business practices

This *NATF Supply Chain Risk Management Guidance* document, along with the *NATF Supply Chain Security Assessment Model* (Model) and associated tools, is intended to assist bulk power system users, owners, and operators with SCRM and related processes. Approaches for identifying, evaluating, controlling, and monitoring supply chain risk differ across individual entities, depending on their size, nature of their extended supply chains, and their own risk exposures. Rather than prescribing a specific approach, this document highlights several possible approaches an entity may consider and adapt to fit their unique characteristics and explicit organizational requirements.

This document will continue to evolve as changes in supply chain risk occur and the practices to address such risks mature. The NATF intends this document to be a resource for entities to aid in managing supply chain risk. To that end, we invite continued collaboration to promote SCRM practices that promote bulk power system reliability and resiliency.

NATF Supply Chain Security Assessment Model

To help address industry needs surrounding supply chain risks, the NATF developed the *Supply Chain Security Assessment Model* (Model) in collaboration with suppliers, entities, solution providers, and other industry participants. The Model outlines a foundational, five-step approach for addressing risk management throughout the supply chain lifecycle that provides a holistic approach in addressing supply chain risks, with clearly defined steps and recommended actions. Understanding that every entity has unique needs based on their size, capabilities, and other drivers, the Model is designed to adapt to the requirements of the entity and anticipates that entities will develop their own in-house processes to accomplish the steps described in the Model.

In the Model, the SCRM lifecycle is divided into five distinct phases, as represented in Figure 1.

Figure 1: The Supply Chain Security Risk Assessment Lifecycle

Each phase of the supply chain lifecycle corresponds to a specific set of actions, or steps, that is further described in the Model and represented in Figure 2.

Figure 2: The Supply Chain Security Assessment Model

Each step is briefly reviewed in the following sections, along with applicable or supplemental resources, to demonstrate how each step relates to the overall goal of SCRM guidance. Further information regarding each step is described in the Model document itself, which is publicly available on NATF's website [1].

Collect Information

The first step of the Model involves obtaining information from current or potential suppliers. Later steps rely on this information to assess, mitigate, and monitor supply chain risks. This information may be acquired multiple ways, including phone calls, face-to-face (or virtual) meetings, custom questionnaires, and verifying references, amongst others. However, relying on numerous ad-hoc processes can result in difficulty when scaling to handle a large volume of potential suppliers or in providing consistent data on which to base a risk decision.

To assist with data collection and increase efficiency and consistency in the assessment process, the NATF has published two key resources, the *NATF Supply Chain Security Criteria* (Criteria) and the *Energy Sector Supply Chain Risk Questionnaire* (Questionnaire). Both resources were developed in collaboration with industry stakeholders and designed to provide a consistent method of obtaining information from suppliers, each with their own unique approach. These resources are described in further detail below.

NATF Supply Chain Security Criteria

The Criteria [2] tool provides a collection of best-practice statements regarding supply chain security that can be used as a foundation to collect information from a supplier or used as a basis to measure a supplier's security posture. These statements are presented in a convenient spreadsheet format, facilitating swift dissemination and review, and are also mapped to several industry frameworks to demonstrate how a supplier's practices may be correlated with the requirements of one or more security standards.

Energy Sector Supply Chain Risk Questionnaire

The Questionnaire [3] tool presents a deeper level of inquiry on the specific security practices, procedures, and operating environment of the supplier. Building upon the best-practice statements of the Criteria, the Questionnaire contains these statements in question format and expands on each of the topics covered by the Criteria. Many questions are presented in a Yes/No format, permitting rapid completion and review of responses, but also provide space for comments for the supplier to provide additional context. An optional scoring methodology is also provided that allows entities to customize the weight of each question and assess the completeness, thoroughness, and suitability of supplier responses.

Other sources

Apart from direct inquiry from the entity to the supplier, entities may use other methods to obtain information about a supplier. One option may be to obtain an audit, security framework report, or other type of report from a qualified, independent third-party. This approach is often referred to as "relying on the work of others," and can be a very efficient and effective use of resources if done properly. Important considerations for utilizing such information are covered in additional detail under the Conduct Risk Assessment section later in this document.

Entities may obtain other information by reviewing the supplier's performance on past contracts, public reporting about the supplier from reputable news, industry, or trade organizations, and discussions with other entities on their experiences with the supplier. See NATF Implementation Guidance for Independent Assessment of Vendors and ERO CMEP Practice Guide: Using the Work of Others sections below.

Importance of Convergence

By converging on the use of the NATF Criteria and Questionnaire, entities may obtain consistent results from suppliers that facilitate quicker review and risk analysis. In addition, suppliers benefit from convergence by reducing the amount of time needed to respond to bespoke requests for items already covered by the Criteria or Questionnaire. Once completed, a supplier can provide a finished Criteria or Questionnaire to any entity that requests it, reducing or potentially eliminating the need for additional, time-consuming requests that often are present in other approaches. Even if the entity has additional questions about specific practices, products, or other concerns, using the Criteria or Questionnaire as a starting point provides a solid foundation on which to build additional conversations and can help reduce the overall effort by both entity and supplier in conducting the risk assessment process.

Evaluate Information/Address Risks

The next step of the Model involves evaluating the information received from the supplier. Evaluating information is a multi-part process that involves analyzing how strongly a supplier adheres to the best practices identified in the Criteria and Questionnaire, evaluating the degree of assurance provided, and evaluating the risks that remain and possible mitigations needed to address the remaining risks. Each of these elements are discussed briefly below.

Does the supplier state adherence to the best practices listed in the NATF Criteria and/or Questionnaire?

Evaluate the responses provided by the supplier to determine how strongly they adhere to the Criteria and/or Questionnaire. Does the supplier fully support each element listed, or only a subset? For any areas that are not fully supported or only supported partially, does this constitute a risk that needs to be addressed by either the entity or supplier?

Does the supplier provide an appropriate level of assurance for its responses?

Consider each response provided by the supplier and evaluate what level of assurance the entity needs for each item. For products or services with a direct impact on the bulk power system, a higher level of assurance may be required from the supplier. Was the supplier able to satisfy the entities' required level of assurance? If not, is there additional information the supplier needs to provide or other actions the supplier can take to provide this level of assurance?

Do significant risks remain, and if so, how might they be addressed?

Given the results of the preceding steps, consider any identified risks, the significance of each risk, and whether additional actions by the entity or suppliers are needed to mitigate the risks, or if the risks may be accepted as-is.

Over time, as industry and suppliers converge on the use of the NATF Criteria and Questionnaire and continue to identify risks, discovery of recurring risks will lead to greater adoption of the best mitigation strategies. Thus, the overall supply chain risk to industry will be reduced. This process of convergence is outlined in Figure 3.

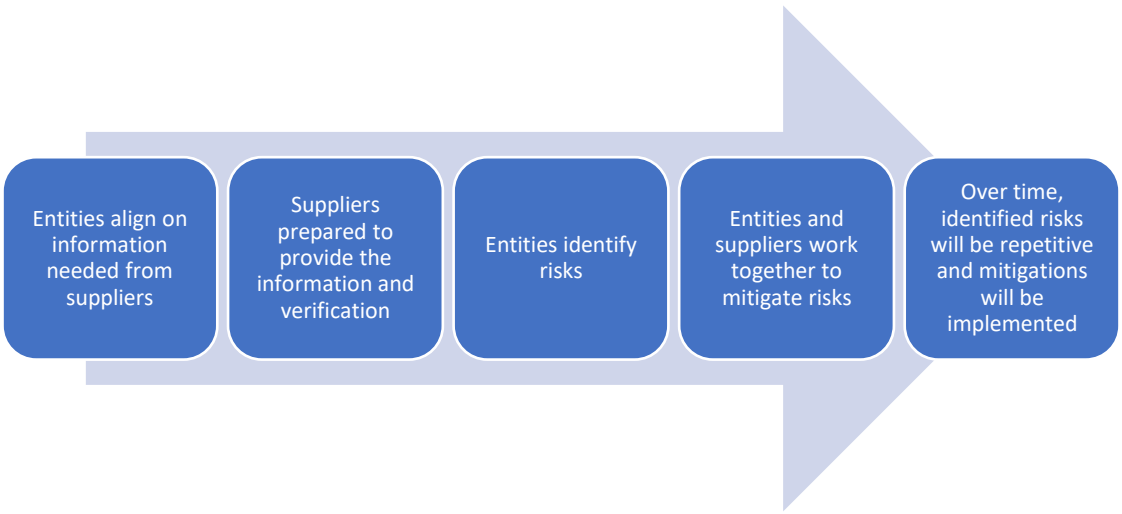

Figure 3: Vision for Convergence

Conduct Risk Assessment

Following or concurrent with the evaluation of the potential supplier's information, the level of assurance provided, and the residual risks, the entity may conduct a formal risk assessment. This step of the Model explores the potential ramifications of the remaining risks more thoroughly. For some entities, this may also be the start of the ranking process, whereby different suppliers are ranked in order of the residual risk that use of the products or services may impart upon the entity.

A variety of approaches exist that may assist with classifying and assessing risk in the supply chain procurement process. One approach may involve the use of a simple ranking system, using pertinent qualitative or quantitative collected information, assurances, and potential mitigations to assess risk or the suitability of particular suppliers in descending order. Another approach could be to institute gates or phases that focus on supplier, product, and/or service information that is deemed critical for the procurement. In this approach each supplier must successfully pass through one gate or phase before advancing to the next gate or phase for further consideration. Still another approach may be some combination of these two.

Ultimately, the best approach for assessing risk may vary between entities, risk appetite, ability to control risk, and even which product or service is procured by entities. Regardless of approach, using a standard and consistent methodology is key to producing accurate and repeatable risk assessments.

NATF Implementation Guidance for Independent Assessment of Vendors

While assessing various suppliers for a potential purchase, the entity can inquire whether the suppliers can provide evidence of conformance to an independent standard, a certification with a relevant organization, or specific reports or assessments that have been performed by a third party and are available for review.

When available, such certifications and assessments can provide an entity with valuable information concerning a given supplier. If trusted and verified, the time and effort spent by the supplier to obtain these qualifications or assessments will provide additional assurances for the entity. Relying on trusted third-party qualifications or assessments as part of a risk assessment is often known as "relying on the work of others" and can be a powerful approach for performing due diligence in an efficient manner.

The NATF has developed specific implementation guidance on the appropriate use of these third-party qualifications and assessments. The *NATF CIP-013 Implementation Guidance: Using Independent Assessments of Vendors* document [4] is endorsed by the ERO Enterprise[2] as an example of leveraging independent assessments in a manner consistent with the CIP-013 reliability standard.[3] Key aspects of this implementation guidance document include:

- Understanding the methodology used to perform the assessment and determining whether the assessment addresses the topics in CIP-013 Requirement R1, part 1.2;
- Evaluating auditor's qualifications and cyber security framework used to perform the assessment;
- Evaluating the scope and results of the assessment, certification, or report;
- Documenting the evaluations of the auditor's qualifications, the methodology, scope of the review, and conclusions regarding appropriate mitigating actions.

For further information, please refer to the implementation guidance document [4].

ERO CMEP Practice Guide: Using the Work of Others

The ERO Enterprise has developed relevant practice guidance for using the work of others. While this document, known as the *ERO Enterprise CMEP Practice Guide* [5], provides guidance for ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) staff, it is prudent for entities to consider this guidance as they develop their own risk assessment processes.

Some important considerations referenced in the guidance include:

- CMEP staff should determine whether materials or evidence provided by an entity are relevant to the current compliance monitoring activity objectives.
- If a registered entity provides CMEP staff with the work of others, CMEP staff should receive and review documentation of others' qualifications, capabilities, and independence and should determine whether the scope, quality, and timing of the work performed can be relied on in the context of the current engagement objectives.

The practice guide also notes that CMEP staff may elect to use work produced by an entity's internal auditing team. Accordingly, entities may wish to take a comprehensive view when designing their supply chain risk assessment process and consider how various business functions such as procurement, auditing, contracting, and others can best work together to identify, assess, and document potential supplier risks.

Make Purchase Decision

After conducting the risk assessment, the entity will have the information needed to make an informed purchasing decision. Apart from any potential risks identified inherent to the supplier and service or product

[2] The Electric Reliability Organization (ERO) Enterprise consists of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (Midwest Reliability Organization (MRO), Northeast Power Coordinating Council (NPCC), ReliabilityFirst (RF), SERC Reliability Corporation (SERC), Texas Reliability Entity (Texas RE), and Western Electricity Coordinating Council (WECC).

[3] The ERO Enterprise's endorsement of an example means the ERO Enterprise compliance monitoring and enforcement staff will give the method described in the example deference when conducting compliance monitoring activities. See https://www.nerc.com/pa/comp/guidance/Pages/default.aspx.

being procured, the entity may wish to consider what risks it may contribute to the service or product's use case and how this interaction fits into the entity's overall risk appetite. Selected factors that an entity may wish to consider include, but are not limited to, the following:

- Financial
- Operational
- Reputational
- Regulatory requirements

Using a cross-functional approach that incorporates various business units and functions in the determination of risk and purchasing decisions is a best practice that ensures relevant stakeholders are engaged and informed. For example, supply chain lifecycle risk considerations brought forth by an entity's legal department may be considerably different than those envisioned by the information technology (IT) department, the finance department, or other key stakeholders. By incorporating these elements into the purchasing process using a risk-based and cross-functional approach, risks can be identified and mitigated earlier in the lifecycle.

It is important to consider how the risks identified in the preceding steps may be addressed, especially in relation to contractual agreements. The entity should ensure that any agreed-upon mitigations are explicitly stated or referenced in the purchasing agreement or related purchase order terms and conditions to promote accountability and avoid unresolved sources of risk in the future.

Procurement Language

A well-defined purchasing agreement should address several important security areas, such as control of data, incident response, vulnerability disclosure, and others. To assist industry in the development of these crucial business agreements, the Edison Electric Institute (EEI) has developed the *Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk* [6] document ("Model Procurement Language") that can be used by entities as a starting point for negotiating with suppliers. This document was created by a committee of EEI member company representatives and reflects the collective input of many subject matter experts (SMEs).

While the *Model Procurement Language* focuses on security controls and processes required by the CIP-013 reliability standard, it also goes above and beyond these specific requirements to promote cybersecurity practices generally through contractual language. This guidance represents a strong foundation that entities can use to build or enhance their procurement contracts and whose use is not limited to solely CIP-related procurements. Indeed, this guidance can be considered as potentially applicable for all products or service offerings and referenced as part of a holistic approach for ensuring supply chain cybersecurity contractual protections.

Additionally, the NERC Supply Chain Working Group published the *Security Guideline: Supply Chain Procurement Language* [7] document which highlights considerations for developing and maintaining risk-based procurement language.

Implement Controls to Monitor Risks

Once the decision to purchase has been made, the final step of the Model is to implement the controls needed to monitor risks identified and implemented in prior steps. The entity should develop a plan designed to monitor risks throughout the lifecycle of purchased products and services, particularly for those whose offerings or

capabilities may change or adapt throughout the lifetime of its use. For components or services that rely on software or firmware, it is entirely possible that new patches, upgrades, or other changes to the service could have a significant impact on the risk – either positively or negatively – that is presented to the entity.

Accordingly, such reviews of risk and their mitigating controls should be periodically reviewed and re-evaluated to ensure that new sources of risk do not go unaddressed. For example, the entity may wish to refresh and review, on some defined periodicity, the Questionnaire responses of any suppliers for which it has an ongoing product or service relationship. Outside of time-mandated triggers, other factors that should be considered for triggering a new risk review may include:

- Acquisition or merger
- Discontinuation of product/service line
- Data breach or significant security incident
- Change in key supplier(s)
- Relocation to different geographic regions
- Impact of new regulation or law on products/services

Other factors specific to the entity or product/service being procured may be relevant in triggering a risk review. Any risk identified should be reviewed by the entity for mitigation, acceptance, renegotiation, or supplier reselection using the preceding Model steps as appropriate.

Internal SCRM Considerations

Although much of SCRM involves the careful consideration of what risks a third-party supplier may introduce to an entity, another vital aspect of SCRM involves which business plans, policies, and procedures the entity has chosen to use for conducting SCRM activities. Indeed, a thorough risk assessment may have little impact if the supplier has no corresponding business processes designed to take advantage of the resulting information. Thus, these internal SCRM considerations are deserving of their own guidance and prioritization. To assist industry in the development of their own SCRM programs, several resources are presented and discussed below.

NATF Supply Chain Risk Management Plans Implementation Guidance

The NATF has developed specific implementation guidance to help entities develop their own SCRM plans through the use of the NATF Model. The *NATF CIP-013 Implementation Guidance: Supply Chain Risk Management Plans* [8] is an ERO Enterprise-endorsed document that describes one method for an entity to develop its own SCRM plans in compliance with CIP-013 requirements R1 and R2.

Apart from compliance considerations, this implementation guidance also incorporates best practices that exceed the requirements of the CIP-013 standard and serve as a solid foundation for any entity wishing to create or further develop its own SCRM plans. Given the wide variability in how different entities structure and conduct their supply chain and procurement activities, the guidance does not provide low-level prescriptive instructions on every individual step or business transaction that may be involved, but rather focuses on the fundamental outputs and critical actions that an entity should seek to achieve in each area. The specifics of how an entity chooses to accomplish these objectives depend largely on the resources, requirements, and capabilities available. By focusing on outcomes, the applicability of this implementation guidance is increased while still meeting CIP requirements and advancing SCRM best practices more broadly.

APPA Cyber Supply Chain Risk Management

Another leading industry organization, the American Public Power Association (APPA), produced its own *Cyber Supply Chain Risk Management* [9] guidance document. Created in conjunction with other energy sector organizations and SMEs, this document discusses a wide variety of topics such as vendor agreements, organizational cybersecurity controls, program maturity assessments, roles and responsibilities, and other areas. This guidance may be particularly useful for entities newly building out their SCRM programs or who may benefit from additional discussion on how best to integrate SCRM into other core business functional areas, such as contracting, compliance, enterprise risk management, and others.

Conclusion

Although the operating environments and risks that entities face vary from one another, the key considerations that underpin effective SCRM often remain the same. This document provides an overview of many SCRM core concepts and identified resources for additional exploration.

Entities are encouraged to take advantage of the many industry resources available to them and benefit from the collective experiences of others. By maintaining a vigilant eye on the ever-changing risks facing modern supply chains and staying up to date on proven methods designed to combat these risks, entities can take a leading role in protecting the bulk power system from attack and ensure its continued safe and reliable operation.

References

[1] North American Transmission Forum, "Supply Chain Security Assessment Model," 4 June 2021. [Online]. Available: https://www.natf.net/docs/natf/documents/resources/supply-chain/supply-chain-security-assessment-model.pdf.

[2] North American Transmission Forum, "NATF Supply Chain Security Criteria," 2 June 2023. [Online]. Available: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

[3] North American Transmission Forum, "Energy Sector Supply Chain Risk Questionnaire," 2 June 2023. [Online]. Available: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

[4] North American Transmission Forum, "NATF CIP-013 Implementation Guidance: Using Independent Assessments of Vendors," 28 January 2022. [Online]. Available: https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-013%20Using%20Independent%20Assessments%20of%20Vendors%20(NATF).pdf.

[5] ERO Enterprise, "ERO Enterprise CMEP Practice Guide - Using the Work of Others," 14 March 2023. [Online]. Available: https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Using%20the%20Work%20of%20Others.pdf.

[6] Edison Electric Institute, "Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk," October 2022. [Online]. Available: https://www.eei.org/-/media/Project/EEI/Documents/Issues-and-Policy/Model--Procurement-Contract.pdf.

[7] North American Electric Reliability Corporation, "Security Guideline: Supply Chain Procurement Language," 15 December 2020. [Online]. Available: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Procurement_Language_FINAL.pdf.

[8] North American Transmission Forum, "NATF CIP-013 Implementation Guidance: Supply Chain Risk Management Plans," 28 January 2022. [Online]. Available: https://www.natf.net/docs/natf/documents/resources/supply-chain/natf-cip-013-implementation-guidance-supply-chain-risk-management-plans.pdf.

[9] American Public Power Association, "Cyber Supply Chain Risk Management," December 2020. [Online]. Available: https://www.publicpower.org/resource/cyber-supply-chain-risk-management.

[10] Federal Energy Regulatory Commission, "Order No. 706-A," 16 May 2008. [Online]. Available: https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order706A_denying_rehearing_CIP_Standards.pdf.