NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

# Guideline for the Electricity Sector

Supply Chain Procurement Language

The objective of the reliability guidelines is to distribute key practices and information on specific issues critical to promote and maintain a highly reliable and secure bulk power system (BPS). Reliability guidelines are not binding norms or parameters to the level that compliance to NERC's Reliability Standards are monitored or enforced. Rather, their incorporation into industry practices are strictly voluntary.

## Introduction

A core measurement of any supply chain cybersecurity risk management program is proof of its value in risk-reducing terms. Regulators have challenged the levels of rigor regarding risk management practices that organizations claim to have attained. Remedies applied through the inclusion of targeted controls in the procurement of cyber systems, components, maintenance, and related services can assist in the development of a "risk-based" approach to cybersecurity.

## Target Audience

Procurement language, beginning at the planning stage and at each step of an acquisition, is a critical element of a supply chain cybersecurity risk management program. Procurement language includes negotiated agreements that formalize the division of responsibilities, performance requirements, and expectations for compliance monitoring. This language is expressed in the form of contract clauses developed during the procurement of industrial control system hardware, software, and computing and networking services associated with bulk electric system (BES) operations. This paper highlights considerations for developing and maintaining risk based procurement language for electrical sector supply chain purposes.

## Risk Identification

A NERC entity's supply chain cybersecurity risk management program efforts begin by identifying important risks to the cybersecurity of the BES supply chain; this process is described in the guideline "*Vendor Risk Management Lifecycle*"[1]. A thorough understanding of the risks associated with vendor relationships to critical cyber systems and particularly BES cyber systems, determines the type and quantity of conditions and stipulations appropriate to include in the procurement language to achieve cybersecurity and reliability goals. The risk assessment should include an analysis of likelihood and magnitude of harm and consider threats, vulnerabilities, and impact to organizational operations and assets, individuals, and the BES.

Procurement language within contracts is one among several means at an entity's disposal to formalize risk mitigation for the relationship between the entity and vendor. Acceptance or transfer of risk and the mitigating controls afforded or needing to be implemented as it relates to a third party may carry specific

[1] https://www.nerc.com/comm/CIPC_Security_Guidelines_DL/Security_Guideline-Vendor_Risk_Management_Lifecycle.pdf

liability and should be defined in entity's processes; and/or authorized by an appropriate senior manager or executive with a solid understanding of the risk being transferred or accepted.

Procurement language should also enable the audit mechanisms and metrics necessary for an entity to ensure that its vendors are meeting the contractual requirements and changes relevant to industry risks. Procurement contracts should be reviewed and updated as appropriate to ensure that an entity is identifying, assessing, and mitigating risks posed by vendors. Entity risk management controls for vendors should monitor contracts, master agreements, service level agreements and other documents associated with vendor procurements for:

- Change in product(s) or service(s)
- Vendor mergers or acquisitions
- Termination dates
- Renewal dates
- Automatic renewal clause dates
- Other significant contract terms

## Procurement Language Examples

In the "*Letter to the Electric Industry Vendor Community*"[2] from the Critical Infrastructure Protection Committee (CIPC) on 03/06/2019, CIPC encouraged product and service vendors to provide several reasonable controls. The list attached to that letter is not intended to be all-inclusive but should be considered during lifecycles of supply chain vendors along with other sources noted below.

Examples of supply chain cybersecurity risks and procurement language considerations include:

- Energy Sector Control Systems Working Group (ESCSWG), "*Cybersecurity Procurement Language for Energy Delivery Systems*"[3]
- Utilities Technology Council (UTC), "*Cyber Supply Chain Risk management for Utilities – Roadmap for Implementation*"[4]
- *Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk*[5], developed by the Edison Electric Institute (EEI), May 2020
- *SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organization*[6], National Institute of Standards and Technology (NIST)

[2] https://www.nerc.com/pa/comp/Documents/Supply_Chain_Cyber_Security_Practices_20190306.pdf
[3] https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf
[4] https://utc.org/wp-content/uploads/2018/02/SupplyChain2015-2.pdf
[5] https://www.eei.org/issuesandpolicy/Documents/EEI Law - Model Procurement Contract Language.pdf
[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

### Additional information sources

- *Cyber Security Supply Chain Risk Management Guidance*[7], developed by the North American Transmission Forum (NATF), 2018
- *North American Generator Forum Cyber Security Supply Chain Management White Paper*[8], developed by the North American Generator Forum (NAGF)
- CIPC approved guideline / letter to industry – *Supply Chain Cyber Security Practices*[9]
- *NERC Frequently Asked Questions Supply Chain – Small Group Advisory Sessions Version: February 18, 2020 NERC Frequently Asked Questions Supply Chain*[10]

## Non-Contractual Purchases

Non-contractual purchases should be documented, assessed for risk, and include steps taken to mitigate identified risks. Purchases, made without a contract, perhaps in response to an emergency to obtain something quickly, pose risks and lack formal oversight. In some cases, the means of acquisition may affect the support that the entity will receive from the equipment manufacturer, or may impose additional requirements to obtain support, thereby requiring additional steps to mitigate risk. Consider, for instance, the risk of using credit cards without the protections of procurement language.

The registered entity should document the emergency procurement process in a Supply Chain Risk Management (SCRM) procurement plan, along with documentation that registered entity personnel or approved contractors should also address after-the-fact risks and mitigations of the procurement. ***(See: NERC Frequently Asked Questions Supply Chain[11])***.

## Closing

The most effective supply chain cybersecurity risk management program will prioritize a risk-based and tiered approach to mitigating security threats. Clear communication and expectations between vendors and entities will result in procurement language to support entity and industry security controls requirements.

[7] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NATF Cyber Security Supply Chain Risk Management Guidance.pdf

[8] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NAGF SC White Paper final.pdf

[9] https://www.nerc.com/pa/comp/Documents/Supply_Chain_Cyber_Security_Practices_20190306.pdf

[10] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply Chain Small Group Advisory Sessions FAQs %E2%80%93 October 2019.pdf

[11] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Supply Chain Small Group Advisory Sessions FAQs %E2%80%93 October 2019.pdf