NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Guideline

Supply Chain Procurement Language

December 10, 2025

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

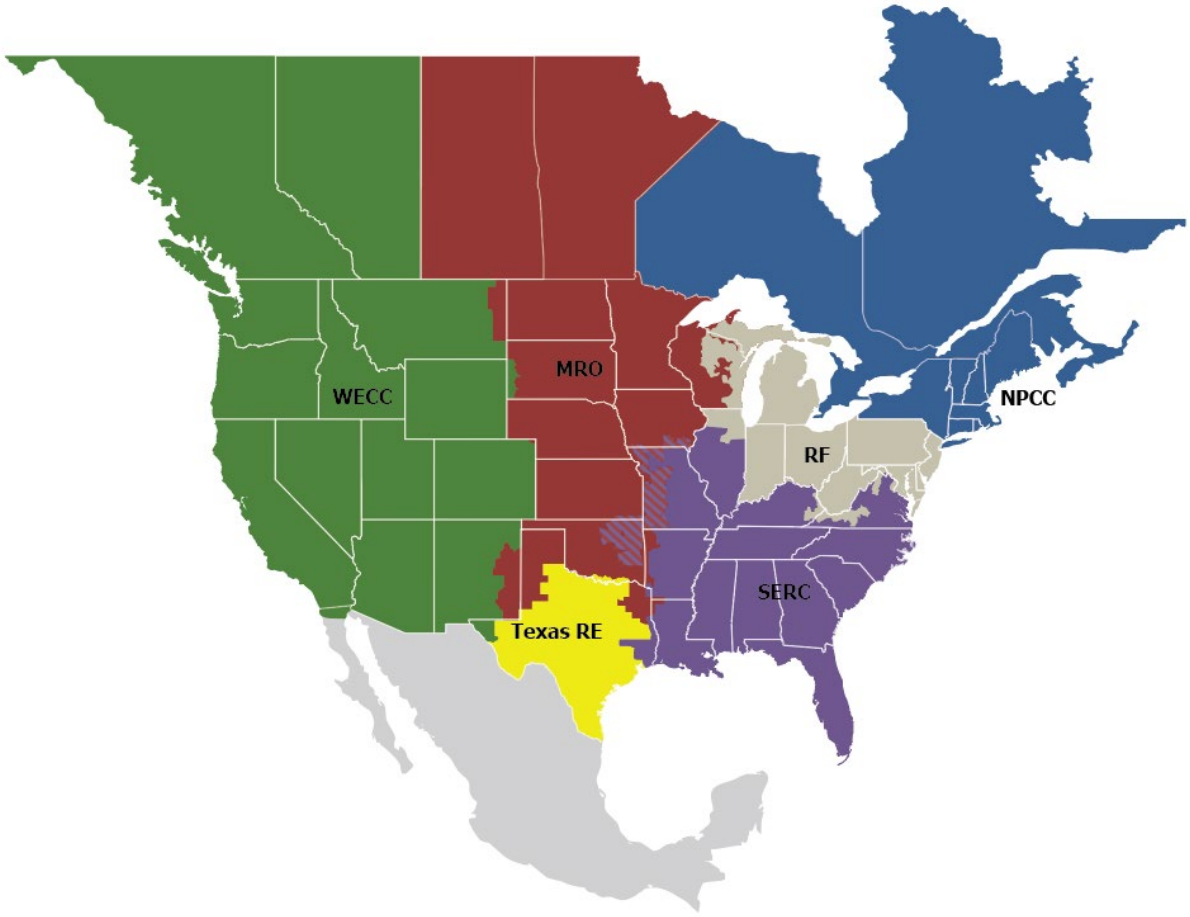
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to ensure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entity boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners /Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Preamble

The NERC Reliability and Security Technical Committee (RSTC), through its subcommittees and working groups, develops and triennially reviews reliability and security guidelines in accordance with the procedures set forth in the RSTC Charter. Reliability and security guidelines include the collective experience, expertise, and judgment of the industry on matters that impact BPS and Bulk Electric System (BES)[1] asset operations, planning, and security. Reliability and security guidelines provide key practices, guidance, and information on specific issues critical to promote and maintain a highly reliable and secure BPS.

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with applicable mandatory Reliability Standards. Reliability and security guidelines are not binding norms or parameters nor are they Reliability Standards; however, NERC encourages entities to review, validate, adjust, and/or develop a program with the practices set forth in this guideline. Entities should review this guideline in detail and in conjunction with evaluations of their internal processes and procedures; these reviews could highlight that appropriate changes are needed, and these changes should be done with consideration of system design, configuration, and business practices.

[1] BES assets are a subset of the BPS.

Introduction

Supply chain cybersecurity risks are a continuously evolving threat for most industries, and a priority for mitigation within critical infrastructure. Electric utilities across North America leverage a complex mix of assets to bring power to our communities. A key method for reducing risk to these assets is to implement a robust supply chain security program. Mitigating risk in the procurement of hardware, software, and even the supporting services for these assets is a first line of defense in supply chain risk management programs.

This Security Guideline provides insights and industry helpful information for procurement terms and conditions or procurement language for integration into the contracts and other procurement instruments (e.g., master agreements, service level agreements, work orders) used within Supply Chain Risk Management (SCRM) Programs. Procurement language includes negotiated agreements that formalize the division of responsibilities, performance requirements, and expectations for compliance monitoring. Procurement language, beginning at the planning stage and at each step of an acquisition, is a critical element of an entity SCRM program. This language is expressed in the form of contract clauses developed during the procurement of hardware, software, and computing and networking services associated with BES operations. This Procurement Language Guideline provides basic insights and helpful resources to support the efforts of organizations looking to design, implement, and enhance their supply chain risk mitigation within the procurement process. This Security Guideline is narrowly focused on the procurement language element of a supply chain risk mitigation program. There are other supply chain Security Guidelines and other related resources available to entities looking for additional procurement program insights.[2] Please note, however, that nothing herein should be construed as providing legal advice as the considerations are only recommended considerations depending on facts and circumstances faced by entities. There is no legal advice or counsel provided in this document and it should be considered solely as sharing useful factors for consideration.

Applicability (Target Audience)

This Security Guideline highlights considerations for developing and maintaining risk-based procurement language for electric subsector supply chain purposes. While the standard Applicability is for assets within NERC BES scope, the guidance and concepts can be applied more broadly to any assets within the organization. Where an asset is a BES asset, the associated risks may be defined as higher priority for risk mitigation, but that would not necessarily preclude the application of the program and this Security Guideline to other assets. Aligning the approach to BES and non-BES assets for many cybersecurity controls is leading practice, more efficient, and often easier for personnel with accountability for implementation.

Background

Procurement terms are one component or aspect of implementing controls within an organization's broader Supply Chain Risk Management Program. This Security Guideline focuses on procurement terms and conditions used within contracts and other procurement instruments (e.g., work orders, statements of work). Other NERC Security Guidelines developed by the Supply Chain Subcommittee support entity approaches to supply chain risk mitigation and should also be consulted to ensure a rounded approach for each of the entity's program elements.

[2] Additional resources are provided in Chapter 2: Procurement Language and Information Resources. There are also several NERC supply chain Security Guidelines that provide helpful information to entities looking to improve and mature SCRM programs. Refer also to the NERC Security Guidelines Page for additional resources: https://www.nerc.com/comm/pages/reliability-and-security-guidelines.aspx

Chapter 1: Procurement Language Key Considerations

Procurement language within contracts is one of several mechanisms an entity may use to formalize risk mitigation associated with the relationship between an entity and its vendor(s). Acceptance of the transfer of risk may carry specific liability for each participant. Responsibilities for risk mitigating requirements and controls should be defined in the entity's vendor and procurement processes and/or authorized by an appropriate senior manager or executive with a solid understanding of the risk being transferred or accepted.

Procurement contracts for third-party products and services should be reviewed and updated to ensure that an entity is identifying, assessing, and mitigating supply chain security risks that may be posed by vendors. Entity supply chain risk management controls for vendors should monitor contracts, master agreements, service level agreements and other documents associated with vendor procurements for opportunities to align agreement terms and risk transfer to current state objectives. Examples of triggering events that may warrant review and update include:

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

Supply Chain Risk Management Program

As with all of the other SCRM program implementing controls, the procurement language should consider the full context of the entity's program, the enterprise, security , supply chain risks of the specific entity, and the entity's desired supply chain risk mitigation objectives. The language should be developed with an understanding of each of these factors and how to further the risk mitigation objectives through the requirements set forth in the agreement that defines the relationship with a supplier. Additionally, a periodic review of any lessons learned from historical supply chain risk mitigation programs and efforts is helpful to ensure the language does not exacerbate challenges for entity personnel responsible for the day-to-day implementation of the program and any business and operations issues that may have been cured or improved with other controls.

Risk Identification and Mitigation Objectives

An 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 Security Guideline "*Vendor Risk Management Lifecycle*"[3]. A thorough understanding of the risks associated with vendor relationships to critical cyber systems and particularly critical Operational Technology (OT) systems determines the type and quantity of conditions and stipulations appropriate to include in the procurement language to achieve cybersecurity and reliability goals. The legal risk assessment and associated procurement language should consider any analysis of the likelihood of an occurrence and the severity of impact or harm in the event of an occurrence (leveraging a typical enterprise risk analysis formula). This analysis typically considers threats, vulnerabilities, and impact to organizational operations and assets, individuals, and the BES and will inform the proper approach to legal risk as well.

[3] RSTC Security Guideline - Vendor Risk Management Lifecycle March 2023
https://www.nerc.com/comm/CIPC_Security_Guidelines_DL/Security_Guideline-Vendor_Risk_Management_Lifecycle.pdf

Risk Assessment Methodology

The SCRM program risk assessment methodology is used to assess risk and score vendors in determining whether to approve products and/or services. The methodology should: (a) be considered in the development of the procurement language, to prevent any conflicts; and (b) be updated to ensure alignment to any baseline or minimum requirements that are included in the procurement language.

Many entities leverage standardized risk assessment questionnaires and may use risk assessment vendors to support the assessment and analysis of the risk in accordance with the methodology. Where the assessment uses form scripted questionnaires and/or automated tools, the entity may identify unique challenges the first time the assessment is applied to a vendor and with any vendors with less mature cyber programs or unique characteristics (refer also to the discussion below of small business and independent contractors). These same challenges often create unique challenges in the drafting and negotiation of the associated supply agreements. Procurement teams developing contract terms for vendors may want to consider monitoring and internal discussion of any such issues as both the risk assessment process and procurement agreement efforts proceed.

Procurement Terms & Conditions Baselines

The spectrum of vendors that any organization utilizes can be very broad. Procurement terms and conditions should be developed with a baseline of requirements in mind but entities that allow for flexibility as needed to support different risks, needs, capabilities, and other factors will likely have a smoother implementation process. Many organizations may have significant challenges meeting the program objectives during the early implementation phases of their program if the contractual obligations are too inflexible to allow for needed responses or updates addressing specific circumstances.

Defining some minimum requirements and providing guidance in the context of the broader supply chain risk management objectives to procurement and other teams that may be negotiating the agreements, will help improve performance and prevent significant delays in securing needed products and services.[4]

Non-Contractual Purchases

Non-contractual purchases should be avoided where possible. If the entity allows for non-contractual purchases, the entity specific program should clearly define what types of purchases would be classified as non-contractual, when these are and are not permitted, how these should be documented, assessed for risk, and include steps that must be taken to mitigate identified risks.[5] 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 the formally developed procurement language.

The registered entity should also 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 be required to develop after-the-fact, including formal contract and any additional documentation to justify and approve the emergency exception, and how risks mitigation associated with the procurement will be addressed. ***(See: NERC Frequently Asked Questions Supply Chain[6])***.

[4] Organizations are beginning to consider including terms or requirements for SBOM (Software Bill of Materials) and HBOM (Hardware Bill of Materials). However, the ability to develop credible inputs and standardized approaches for SBOM and HBOM requirements remains a challenge for most vendors. If considering these terms, the language should be informed by the immaturity of these tools and impact to the purchase risk and legal reality of enforceability.

[5] This Guideline did not address any applicable requirements for use of open-source or free software and whether it may qualify as a "non-contractual purchase" since that is typically more appropriately managed through the risk assessment and broader program rather than the procurement language and "non-contractual" purchases more directly.

[6] NERC Supply Chain FAQ Small Group Advisory Sessions May 05 2021

Legacy Vendors vs. New Procurement

Procurement language will often need to be developed to account for different approaches with legacy activities and relationships, where the terms may not be able to be modified in the near-term, unlike with new procurement agreements where they can be better defined to the current state and risk objectives. Additionally, the risk to the business operations of both a cyber threat, and of a potential disruption more broadly, may be different if there is an existing relationship. Negotiation may be required for renewal agreements, subsequent contracts, addendums, and/or purchase orders or releases, to ensure the integration of updated terms needed to mitigate current-state cyber risk and meet the cybersecurity risk mitigation requirements. This may slow the procurement process with existing vendors. Since many of these products and services are ongoing, a lag or delay could impact day-to-day operations, this should be accounted for in the approach to development and implementation of the procurement processes for managing transition of legacy vendors and agreements.

Aligning as much as possible to a standardized approach is best practice, but when developing procurement language for use within contracts and other terms, there should be some consideration of the possible need for different approaches with legacy and existing vendors. As with many transitions, it is also a good idea to integrate a control that ensures the ability to include the updated procurement language when assessing impact for contracts nearing expiration or renewal.

Small Business and Independent Contractors

Many organizations that have implemented formal Supply Chain Risk Management programs have identified unique challenges in applying the program to smaller vendors and independent contractors whose cybersecurity controls and enterprise architecture infrastructure may look different than the standard model leveraged by larger organizations, around which most of the programs were designed. Current procurement terms and supply chain risk management programs are often modeled with built-in underlying assumptions about the infrastructure and resources used by suppliers to manage security risk. Procurement agreements often consider these distinctions in other contexts, for example the amount of insurance required or types of resources that may be used to complete services. Procurement language developed to address and mitigate supply chain risk should also consider the unique construct and approach to security that may be leveraged by smaller organizations and individuals.

Evolving Technology Considerations

Cloud services, artificial intelligence (AI), managed service and shared technology tools all present unique issues with risk transfer and mitigation. Procurement agreements and terms should be evaluated regularly to address the risks that may not be accounted for in language developed for historical technology. For example, a managed service vendor may be using cloud-based software and tools with the entity data or accessing entity assets from these tools. Shared responsibilities and risks introduced by vendors using cloud based and their own shared technologies should be clearly defined in shared responsibility matrices where appropriate to ensure all parties clearly understand their obligations and the entity risk management objectives are met.[7]

Legal, Insurance, and Other Contractual Risks

Procurement terms should not only consider the introduction of cybersecurity risks within the supply chain but also potential legal and other risks that may be exacerbated by a failure to effectively mitigate cyber supply chain risk. Requirements for product and service vendors are becoming standard practice. Moreover, more stringent requirements are anticipated as more insurance policies, commercial contracts and other legal constructs continue to expand. Many of these terms are copied in from framework template language and could create additional risk if not vetted properly. It is important to assess any procurement language terms being integrated within agreements

[7] Resources discussing shared responsibility models and cloud security for the power sector and within the context of NERC standards were in development or close to publication at the time this Guideline was being published. For example, the Electric Sector: Primer for Cloud and BCSI Protection" and similar papers. Teams interested in additional guidance on this topic should refer to the NERC site for additional support and resources.

to ensure alignment to entity specific requirements, as well as any capability to either implement or enforce terms imposed upon the entity by vendors or other contractual parties.

Measuring Success

A core measurement of any supply chain cybersecurity risk management program is proof of its value in risk-reducing terms. Typical 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.

Like other controls, 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. Defining metrics to measure the value obtained from the procurement language and supply chain risk mitigation program can be challenging but is an important element of a leading practice program.

Chapter 2: Procurement Language and Information Resources

There are a number of resources available with sample language to help any organization get started. The resources provided in this section are some of the more commonly used reference sources within the electric industry and for bulk power system assets. These sources should be reviewed carefully and adapted to the organization's specific needs with advice and guidance from legal counsel.

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

- *Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk,*[8] developed by the Edison Electric Institute (EEI)
- Energy Sector Control Systems Working Group (ESCSWG), "*Cybersecurity Procurement Language for Energy Delivery Systems*"[9]
- Utilities Technology Council (UTC), "*Cyber Supply Chain Risk management for Utilities – Roadmap for Implementation*"[10]
- *SP 800-161 Supply Chain Risk Management Practices for Systems and Organizations (May 2022)*[11], National Institute of Standards and Technology (NIST)

Additional procurement program and language information sources:

- *The North American Transmission Form (NATF)* has developed several industry resources including a full *Supply Chain Security Assessment Model* (NATF), with recommended *Supply Chain Security Criteria*. Resources are available to the public and can be found on the NATF site under Industry Initiatives. [12]
- *American Public Power Association (APPA) Cyber Supply Chain Risk Management Manual*[13]
- *North American Generator Forum Cybersecurity Supply Chain Management White Paper*[14]
- *Idaho National Laboratory Battery Securing Digital Infrastructure: Procurement, Contracting, and Supply Chain Risk Management Guidance (available to the public at the resource page cited)*[15]
- CIPC approved guideline / letter to industry – *Supply Chain Cybersecurity Practices*[16]

[8] EEI Model Procurement Language
[9] Cybersecurity Procurement Language for Energy Delivery Systems (ESCSWG)
[10] UTC Cyber Supply Chain Risk management for Utilities – Roadmap for Implementation
[11] NIST Supply Chain Risk Management Practices for Systems and Organizations 800-161
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf
[12] NATF Supply Chain Industry Coordination Resources
[13] Cyber Supply Chain Risk Management | American Public Power Association
[14] NAGF Cybersecurity Supply Chain Management White Paper
[15] Technical Assistance and Training - Center for Securing Digital Energy Technology
[16] CIPC – Supply Chain Cybersecurity Practices

Contributors

NERC gratefully acknowledges the contributions and assistance of the following industry experts in the preparation of this guideline.

Name	Entity
Andrea Koch	Edison Electric Institute
Andrew Ralph	Entergy
Brandon Brown	Cleco
Brian Thiry	Reliability First
Byron Booker	Oncor
Christine Ericson	Illinois Commerce Commission (ICC)
Danny Johnson	Southwestern Power Administration
George Masters	Schweitzer Engineering Laboratories
Gregory Hardin	SERC
Jimmy Ramirez	ERCOT
Johanne Poirier Mouallem	ATCO
Ken Keels	North American Transmission Forum (NATF)
Kelly Crist	Centerpoint Energy
Matt Nicklin	Southern Illinois Power Cooperative (SIPC)
Mayur Manchanda	Federal Energy Regulatory Commission (FERC)
Michael Johnson	Pacific Gas and Electric
Michaelson Buchanan	NERC
Mike Sanders	Southern Company
Morgan King	WECC
Nathan Brown	Georgia Systems Operations Corporation
Pierre Janse Van Rensberg	BBA
Sarah-Lynne Carrara	VELCO
Scott Webb	Network + Security Technologies
Sean Bodkin	Dominion Energy
Shari Gribbin, Esq.	CNK Solutions Group
Simon Slobodnik	Federal Energy Regulatory Commission (FERC)
Steven Briggs	Tennessee Valley Authority
Teri Kelly	WECC
Theresa Greene	Grand River Dam Authority
Tom Alrich	Tom Alrich LLC
Dr. Tom Duffey	Knight Critical Infrastructure Cybersecurity and Compliance
Tom Hoffstetter	North American Electric Reliability Corporation (NERC)
Tony Eddleman	Nebraska Public Power District (NPPD)
Tope Odubanjo	NP Power
Tony Turner	Sentinal 24
Tricia Bynum	FirstEnergy Corporation

Guideline Information and Revision History

Guideline Information	
Category/Topic: Supply Chain	**Reliability Guideline/Security Guideline/Hybrid:** Security Guideline
Identification Number: SG-SCH-1210-2	**Subgroup:** Supply Chain Subcommittee

Revision History		
Version	**Comments**	**Approval Date**
	Original approved by RSTC	8/23/2022
	Reviewed, added metrics	12/10/2025

Metrics

Pursuant to the Commission's Order on January 19, 2021, *North American Electric Reliability Corporation*, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review consistent with the RSTC Charter.

Baseline Metrics

All NERC reliability guidelines include the following baseline metrics:

- Use and effectiveness of a reliability guideline as reported by industry via survey
- Industry assessment of the extent to which a reliability guideline and security guideline is addressing risk as reported via survey

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline in order to measure and evaluate its effectiveness, listed as follows:

- How many entities have utilized one of the procurement terms resources within the Guideline.

Effectiveness Survey

On January 19, 2021, FERC accepted the NERC proposed approach for evaluating Reliability Guidelines. This evaluation process takes place under the leadership of the RSTC and includes:

- industry survey on effectiveness of Reliability Guidelines
- triennial review with a recommendation to NERC on the effectiveness of a Reliability Guideline and/or whether risks warrant additional measures; and
- NERC's determination whether additional action might be appropriate to address potential risks to reliability in light of the RSTC's recommendation and all other data within NERC's possession pertaining to the relevant issue.

NERC is asking entities who are users of Reliability and Security Guidelines to respond to the short survey provided in the link below.

Guideline Effectiveness Survey