NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Guideline

Product Security Sourcing Guide

December 7, 2023

RELIABILITY | RESILIENCE | SECURITY




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

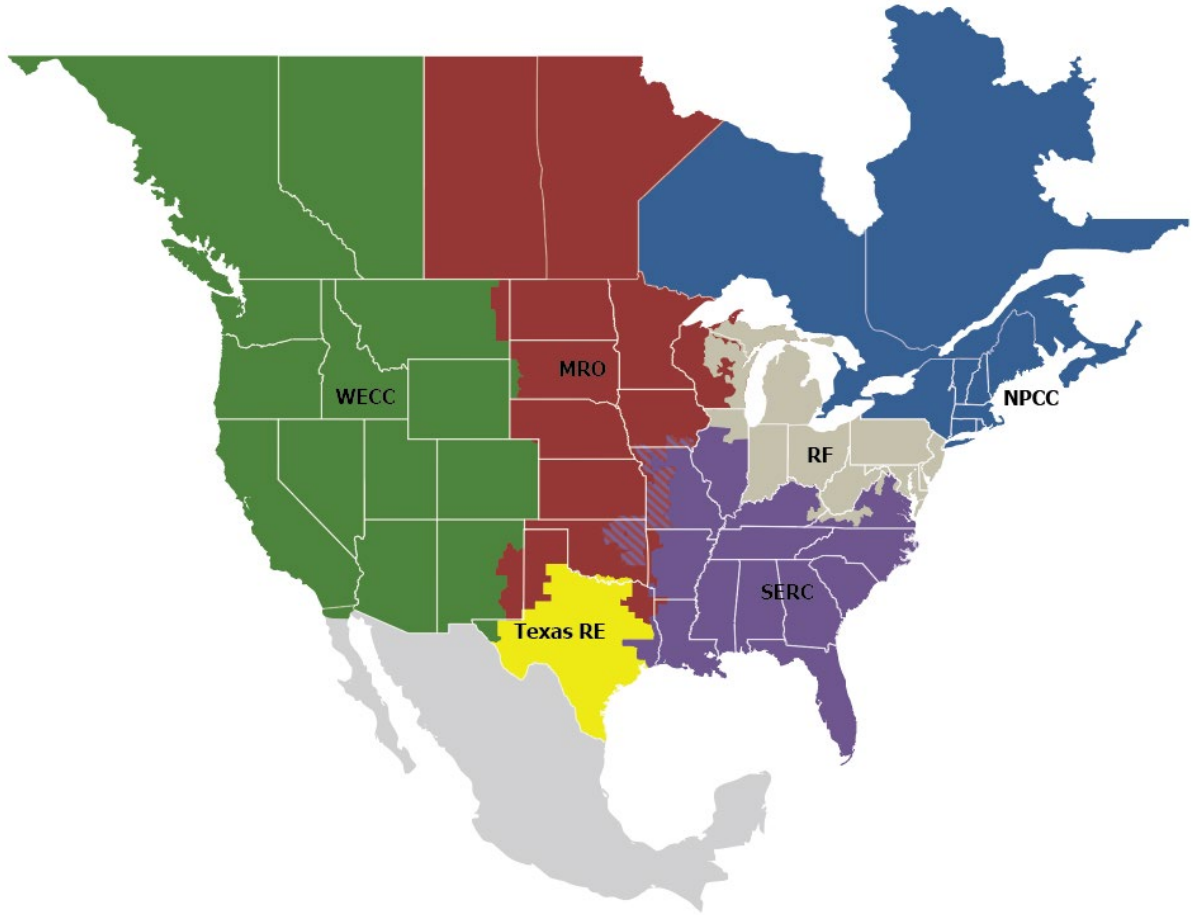
Table of Contents

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 assure 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 Entities as shown on the map and in the 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 guidelines in accordance with the procedures set forth in the RSTC Charter. Reliability guidelines include the collective experience, expertise, and judgment of the industry on matters that impact BPS operations, planning, and security. Reliability 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.

Executive Summary

This product security sourcing guide includes recommended processes for safeguarding grid technologies in various operating environments. The document provides both asset owners with a structured approach to vetting vendors and ensuring alignment with regulatory, standard and compliance requirements. Recommended approaches are provided for vendor management and governance, allocation of critical security controls across operating environments, implementation of product vulnerability disclosure programs, understanding and identifying geo-political risks to those operating environments, mitigations to combat product scarcity, and the use of secure cloud services.

Introduction

Continuously evolving power grid designs, including dispersed power producing resources and cloud-based operations, have created new attack vectors for attackers to exploit, particularly in the controllers that manage energy systems. As the networking of embedded systems within energy grids continues to expand, the attack surfaces will only grow larger. Asset owners must understand the unique risks associated with grid operations and enforce stringent requirements on product developers to mitigate potential security vulnerabilities.

The energy grid is a critical part of US infrastructure and can be the target of cyber-attacks intended to disrupt its operation. Some examples of cyber threats to the energy grid include:

- Malware: Malware can be used to infiltrate energy grid systems, steal data, or cause system failures.
- Phishing/Vishing/Smishing: Phishing attacks are commonly used to gain access to energy grid systems. Attackers use phishing emails to trick users into revealing login credentials or downloading malware. Vishing can occur when an actor calls and uses compromised data to earn trust and trick someone to reset credentials or perform an unsecure action. Smishing can occur when an actor uses SMS text messages to try and trick users into those same actions.
- Ransomware attacks: Ransomware attacks are a growing concern for energy grid operators. Attackers use ransomware to encrypt data and demand payment for its release.
- Insider threats: Insider threats are also a significant concern for the energy grid. Disgruntled employees or contractors with access to sensitive systems can cause grave damage.
- Overreliance on overseas or foreign manufacturing of critical infrastructure could be disrupted in times of international conflict or other emergency conditions.

While the NERC Supply Chain Standards focus primarily on the security controls of the supplier, the Product Security Sourcing Guide presented here serves as an industry-standard guide for identifying key security and risk considerations to support procurement of **grid technologies and products.** Asset owners must maintain situational awareness of the risks associated with grid operations in an often-uncertain geo-political environment. This is often hindered by unverified trust in **supplier controls and the presence of unknown product vulnerabilities**. Therefore, asset owners can use this guide to define and enforce supplier controls that ensure minimum cybersecurity requirements have been implemented **within grid products.**

The cybersecurity controls documented in this **Product Security Sourcing Guide** and the accompanying **Product Security Reference Guide** can be leveraged by asset owners to coordinate purchase activities between cybersecurity professionals and their procurement organizations, while complying with NERC requirements to confirm these steps have been successfully executed. These controls also provide consistent guidance to the supplier community.

Vendor-Level Risk Management

Once an asset owner has set out to determine whether a new grid technology is needed, the first step is to begin vetting vendors through various internal and third-party risk assessment procedures. The industry has developed several tools, initiated by the NERC CIP Supply Chain Risk Management Standards, that, over time, have been expanded in terms of guidelines and plans.

NATF guidelines

- Supply Chain Security Assessment Model[1]
- NATF CIP-013 Implementation Guidance-Independent Assessments of Vendors (ERO Endorsed)[2]
- NATF CIP-013 Implementation Guidance-Supply Chain Risk Management Plans (ERO Endorsed)[3]

EEI Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk[4]

NERC SCWG guidelines

- Security Guideline: Vendor Risk Management Lifecycle[5]
- Security Guideline: Supply Chain Provenance[6]

While the NERC CIP Supply Chain Risk Management Standards focus primarily on the procurement of grid technologies and products, entities should consider similar practices for a broader range of technology acquisitions as a best practice.

Managing critical vendors

Effective vendor management enables organizations to proactively mitigate risks throughout the vendor engagement lifecycle. It is essential to establish governance and processes for continuous risk monitoring of your most critical vendors. Cyber risk is constantly changing and evolving at an increasingly rapid rate. Point-in-time security assessment questionnaires, although effective in establishing a baseline security assessment, should be augmented with routine assessments throughout a vendor's engagement. The frequency of subsequent assessments should be based on the initial assessment and the dependence and criticality of the vendor and adjusted as necessary when novel or notorious threats emerge. For instance, if a supplier is impacted by a popular open-source software vulnerability, such as Log4j, it would be reasonable to request from the vendor updated assessment impacts and any changes to the supplier's control environment.

It is important for asset owners to distinguish between vendors (those who produce and directly sell products) and suppliers, which may include third-party distributors or engineering firms. When asset owners do not procure directly from a vendor, they should establish clear agreements with suppliers. These agreements should stipulate that the supplier will provide comprehensive product security information, including vulnerability patch updates and patch availability. Asset owners may include clauses in procurement language to this effect.

[1] https://www.natf.net/docs/natf/documents/resources/supply-chain/supply-chain-security-assessment-model.pdf
[2] https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-013-1 R1 R2 Supply Chain Management (NATF).pdf
[3] https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-013-1 R1 R2 Supply Chain Management (NATF).pdf
[4] https://www.eei.org/-/media/Project/EEI/Documents/Issues-and-Policy/Model--Procurement-Contract.pdf
[5] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Vendor_Risk_Management_Lifecycle.pdf
[6] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Supply Chain Provenance.pdf

Vendor management governance

It is advisable to establish vendor management processes that are the best fit your organization. To ensure the right contract, metrics, and frequency of assessments are in force, segment or categorize vendors based on your initial assessment results and cyber risks. Use this approach to determine which vendors are most critical or strategic to your operations. Identify accountable resources or vendor relationship managers and establish proactive methods, such as scorecards, to proactively assess the performance of your most critical vendors. This will require cross-functional collaboration between Procurement, Information Technology, Cybersecurity, Engineering and Compliance, among others.

Vendor management risk mitigation practices

Establish and maintain a list of your most critical vendors that includes supplier points of contact as well as escalation contacts for issue resolution. Procurement and cybersecurity teams should be collaborating closely by ensuring that their cybersecurity Supply Chain Risk Management plans identify continuous monitoring scenarios during the supplier lifecycle that may trigger a security reassessment. Responsible entities should ensure that their contracts with vendors include obligations for the vendor to report at minimum:

- Material changes in supplier scope-of-engagement. (E.g., original purchase of hardware followed by a subsequent software purchase later in the engagement.)
- Mergers, acquisitions, or changes in ownership.
- A security incident or vulnerability notification.
- A change in the type of physical and logical access required by a supplier or their resources.
- An uncharacteristic change in supplier performance.

Determine comprehensive stakeholder responsibilities for the following roles:

- Cybersecurity
- Engineering
- Procurement
- Information Technology
- Operations

Additionally, the following metrics and conditions should be implemented:

- Risk assessment frequency for critical vendors, ranked by
  - High risk
  - Medium risk
  - Low risk
- Raise supplier accountability
  - Highlight performance or non-compliance
  - Increase strategic alignment
- Risk mitigation upon contract renewal or amendment
  - Demonstrate how risk is mitigated with compliance and enforcement

- Update contract templates and standards accordingly

Vendor artifacts and attestations

Supplier attestations noted herein and in other guidance, such as NIST guidance in response to "Executive Order 14028, Improving the Nation's Cybersecurity," should be requested as part of your supplier selection process.

- Incorporate the appropriate attestations in your Request for Proposal (RFP) or supplier solicitation process. Attestations should be reviewed and evaluated as part of your supplier selection process. This enables entities to evaluate risks early in the supplier selection process and support a faster contracting cycle time when considering supplier attestations.
- For existing suppliers, incorporate the appropriate attestations in subsequent contracting activities, such as contract amendments, contract extensions, renewals, etc. Critical vendors should include the appropriate attestations necessary to mitigate risk for your entity.
- When attestations are requested and supplied, the asset owner should seek to add clauses in the contracts to allow the right to audit or independently verify the attestation.
- Entities should consider centralized repositories for the secured archival of vendor related artifacts in support of your security supply chain risk management plans.

Grid Technologies and Applicable Control Environments

After the initial vendor vetting has been completed, the next step is to understand what types of grid technology are being purchased by the asset owner and what considerations should be addressed given the regulatory, standards, and compliance considerations of the given environment within which the system will be implemented. For products specific to the energy industry, product developers should implement the product, supply chain, and development environment security controls for their technologies and products in a manner consistent with the controls required for the operating environment. Energy companies have complex operating environments that will dictate which regulations and standards are met for a given operating environment. In practice, there are three core operating environments:

1. **Bulk Electric System** (BES) – the official definition of the BES can be found here[7]. The BES can be considered as those systems associated with anything at or above 100KV or 50MVA, and applicable to low, medium or high BES Control Systems categorizations of the NERC CIP standard.
2. **Non-BES/BPS – Encompasses the elements of the electric system that are outside of the BES and non-BPS distribution systems, such as local distribution networks, smaller generation units and microgrids.**
3. **Non-BPS (Distribution, DER and Renewables)** – systems not considered to be under the jurisdiction of FERC or NERC, which are, instead, generally under the jurisdiction of state public utility commissioners. This category of systems is not mandated to be compliant with NERC CIP standards and therefore does not have a uniform set of cybersecurity requirements.
4. **Defense-Critical Electric Infrastructure** – "any electric infrastructure that serves" a Critical Defense Facility, "but is not owned or operated by the owner or operator of such facility."[8]

Table 1 provides a high-level view of the critical security controls for grid products based on the operating environments described above. Critical control categories are allocated to either Asset Owner or Vendor. In cases where a product is being developed by an Asset Owner, the security controls for "Vendor" also apply to that Asset Owner. Detailed control descriptions, including measures of compliance, can be found in the accompanying Product Security Reference Guide.

Table 1: Critical Security Controls

Security Controls	Responsible Party	Description
Vendor- Level Supply Chain Security	Asset Owner	Perform independent penetration tests of all integrated COTS components and validate that vendors have established processes for managing device identity. Perform due diligence of all hardware, software, firmware and service suppliers, and require Software Bill of Materials (SBOMs) and Hardware Bill of Materials (HBOMs) for relevant products.
Geo-political Risk Considerations	Asset Owner	Some organizations have requirements or mandates that dictate which companies and suppliers they may source from for certain grid technologies. Obtaining information about their geographical footprint can help inform the purchasing organization of foreign ownership, control or influence risk.
Secure Development Processes and Practices	Vendor	Validate that suppliers have established cybersecurity training programs for product developers and that each product undergoes a threat modeling and operational impact assessment. Validate the use of secure coding practices and that suppliers have in place vulnerability discovery response plans and published

[7] https://www.nerc.com/pa/Stand/2018%20Bulk%20Electric%20System%20Definition%20Reference/BES_Reference_Doc_08_08_2018_Clean_for_Posting.pdf

[8] https://www.energy.gov/oe/articles/oe-dcei-strategy-eac-101420

Table 1: Critical Security Controls		
Security Controls	**Responsible Party**	**Description**
		methods for submission of independent vulnerability disclosures. This may include SBOMs to aid in the analysis of software risk management.
Device & Product Security Management, Tamper Protections and Physical Security Controls	Vendor	Validate that products require change of default passwords upon first use, establish product lockouts based on failed login attempts, validate digital signatures on all updates, and allow disablement of ports and services. This may include the evaluation of component risk that can be identified through the review of HBOMs. Validate that products implement secure storage for cryptographic primitives and keys, restrict access to audit logs, and support disablement of specific ports and services.
Authentication, Authorization and Access Controls	Asset Owner Vendor	Validate that products require multi-factor authentication (MFA), when supported, for all administrative access, implement role-based access controls to support separation of duties, require minimum password complexity or use private keys, and implement session timeouts.
Monitoring and Logging	Asset Owner Vendor	Validate that the products log actions including login events, privilege escalation, account creation, unauthorized file access, and remote access attempts.
System Segmentation	Asset Owner	Ensure that systems segment systems based on trust, risk profiles or other security-relevant attributes; segment all data acquisition interfaces from management functions and segment all enterprise networks from the Internet.
Information Protection	Vendor	Validate that products encrypt all interfaces, use standards-compliant cryptographic modules/libraries, authenticate all messages, protect integrity of all messages, and secure all wireless interfaces.
Vulnerability Management & Disclosure	Asset Owner	Validate that manufacturers have processes and procedures in place to accept vulnerability disclosure reports from customers and independent security researchers and can track those reports to closure.

Product Vulnerability Disclosure

Vulnerability disclosure can be managed in two ways: (1) communications from a *customer (or third-party such as the U.S. Cybersecurity and Infrastructure Security Agency known as CISA) to the supplier* (known as Pull) and (2) communications from the *supplier to a customer* (Push). The Pull case is less frequently needed, but a mature supplier organization will be prepared for it and should be willing to share those preparations with their clients and customers.

Disclosure to the supplier

Suppliers should ensure customers know how to report vulnerabilities. Until the asset owner has a vulnerability in hand, the asset owner will not need more than a contact channel and broad outlines of how the process works. Detailed procedural information is normally provided by the vendor upon initiating an actual disclosure. That process should include these steps:

- Contact procedure for reporting a vulnerability.
- Vulnerability disclosure information about how the process will be managed – confirmation, trajectory, and timeline.
- A secure method for confidential transfer of information relating to vulnerability.

Disclosure from the supplier

Disclosure from the supplier can be either current or historical. Current disclosures relate to new vulnerability findings and information as they are identified. Historical disclosures are records for past products and/or versions and are useful when dealing with non-current products.

Current disclosure by the supplier: "Push" or "Pull" Process

When procuring from a supplier, that relationship becomes part of your accepted risk picture. When security vulnerabilities occur in products that are obtained from a supplier, those risks add to the risk posture of the customer's system. Security vulnerability disclosures are how an asset owner learns of vulnerabilities and gains the information necessary to react to them to keep risk at an acceptable level.

As part of vulnerability risk management, vendors should be able to provide a SBOM to assist in managing the risk of security vulnerabilities in products. At the least, this will allow the asset owner to determine whether the security of the asset owner's systems might be affected at the time that a serious vulnerability in a software component is announced, and before a supplier using that component has provided an update.

Information about vulnerabilities can take the form of notifications from the supplier (Push), such as email or a communications channel that provides product release notes and security notices. Push notifications from a supplier or vendor are more likely to be sent in "real time" – i.e., close to the time that the vulnerability is confirmed. Given the possibility that the asset owner may not always immediately pick up these types of Push notifications in a timely way, it is advisable to establish a system of "pulling" updates on vulnerability information. Doing so provides a high degree of assurance (though not 100 percent) that you have all the information currently available.

However, once an asset owner acquires the system, the asset owner will need timely and sufficient information to make an informed decision, usually whether to install an offered update, apply mitigating security controls, or do nothing. Asset owners will need to ask suppliers:

- How will you learn of vulnerabilities?
- Is there more than one legitimate channel?

- Is the channel trustworthy (e.g., https, using TLS protocol as maintained by IETF)? How do you ensure that the information is authentic?
- Are there specific disclosure times, or can disclosures occur at any time?
- Does the supplier have a way to inform customers of a zero-day (product vulnerability not yet patched)?
- Does the supplier treat unsupported/out-of-date components as a security vulnerability?

Vulnerability disclosures must serve your needs. Vulnerability disclosures should:

- Name the affected product(s) and version(s).
- Describe what could happen.
- Describe who could cause it to happen and how.
- Offer means to address vulnerability.

Asking to see examples of past vulnerability disclosures might clarify how these requirements are satisfied, and the audience for whom it was written. After all, someone in the asset owner's organization will have to read and understand the vulnerability disclosures.

Geo-political Risk Considerations

The U.S. Department of Commerce indicates that adversarial nations[9], such as Russia and China, who possess or have access to advanced technological capabilities are a significant risk to the United States and its allies and therefore require stringent export controls. This was acknowledged by the 2022 National Defense Strategy[10], which states:

> "The PRC or Russia could use a wide array of tools in an attempt to hinder U.S. military preparation and response in a conflict, including actions aimed at undermining the will of the United States public, and to target our critical infrastructure and other systems."

Jen Easterly, Director of the US Cybersecurity & Infrastructure Security Agency (CISA), stated that If China were to launch a military takeover of Taiwan, China "might very well" couple that invasion with cyberattacks on United States infrastructure, "with the explosion of multiple gas pipelines, the mass pollution of our water systems, the hijacking of our telecommunication systems, the crippling of our transportation nodes… all designed to incite chaos and panic across our country and deter our ability to marshal military might and citizen will."[11]

In May 2023, China targeted the US through Guam. It has been reported by CISA that the Chinese-sponsored cyber group Volt Typhoon is targeting key United States sectors such as communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education.

By dominating the global critical infrastructure market (batteries, drones, and other technologies), China secures two advantages (1) Economic growth and (2) Exploitation of critical infrastructure to help prevail in wartime, especially by jeopardizing United States public safety and disrupting defense-critical infrastructure. Domestic critical infrastructure owners and operators can expect that US adversaries will continue to target grid technologies and seek to corrupt supply chains supporting United States and allied infrastructure.

Presently, there are no mandatory or enforceable standards to ensure that hardware and software suppliers are measurably secure and have minimal exposures to geo-political risk in grid technology supply chains. For this reason, this section of the guidance document is geared toward providing examples of information that purchasing organizations may request from manufacturers to help obtain visibility into geo-political risk concerns:

1. **Manufacturing, Development or Assembly Location:** Information describing which countries or cities manufactured or developed specific technologies can help the purchasing organization determine the whereabouts of critical components of the product that can be implemented within their environment. Often SBOMs and HBOMs, respectively, can identify key components of the product that then can be mapped to locations. Understanding the component provenance or sourcing is a key step in understanding geo-political risk that can be linked to manufacturing, development, or assembly.
2. **Cyber Presence:** Cyber presence can be described as locations of the supplier's internet-facing infrastructure, such as web servers, DNS servers or IP address ranges where remote support is performed. Remote support services and capability provided by the vendor may often be described in service contracts. This information can provide insight and awareness to the purchasing organization's network or cybersecurity team to manage traffic or incidents originating from identified sources.
3. **Financial Relationships:** Monitoring financial ties and partnerships provides insights into the supplier's business interests or potential sources of influence. By having a geo-locational mapping of each parent, child, or peer organization, the supplier provides insight into financial relationships, which can help inform the

[9] https://www.bis.doc.gov/index.php/policy-guidance/country-guidance
[10] https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF
[11] https://www.cisa.gov/cisa-director-easterly-remarks-carnegie-mellon-university

purchasing organization as to whether those relationships would impact the risk profile of the technology in question.

4. **Emphasizing Domestic Suppliers:** The Department of Energy [12] has established new incentives to ensure that grid technologies are sourced by domestic manufacturers. In addition, the Department of Treasury, and Internal Revenue Service have established programs to incentivize domestic clean energy manufacturing[13]. Purchasing organizations will be looking to determine if their suppliers have domestic manufacturing that fulfills federal incentives. As a result of these policies and federal tax programs, utilities should consider establishing incentives to emphasize domestic sourcing in their procurement processes.

Asset owners should reference the Trade Agreements Act (TAA). The TAA includes a provision that asset owners ensure procurement choices are limited to TAA-complaint countries, for any federally funded contracts. Asset owners working outside of the federal government market should consider these provisions to bolster their supply chain security programs.

[12] https://www.energy.gov/sites/default/files/2023-04/DOE%20DPA%20Roundtables%20and%20RFI%20Executive%20Summary%20FINAL%203-21-23.pdf
[13] https://home.treasury.gov/news/press-releases/jy1477

Product Scarcity Risk Considerations

In August of 2022, Congress passed, and the President signed into Law the Inflation Reduction Act, which included $500M[14] to execute the Defense Production Act. The Defense Production Act (DPA) allows for the federal government to subsidize domestic production to increase the production of a good or a service. The DPA was invoked to increase production of heat pumps and other electric power grid components. The inclusion of electric grid components was in large part in response to the Electricity Subsector Coordinating Council Tiger Team on supply chain. The Tiger Team[15] found that the average delivering time for a distribution transformer is one year from the original purchase.

In addition, many factors, including the Russia-Ukraine conflict, and Regional Transmission Organizations capacity markets, have caused critical shortages of fossil fuels, driving up prices for fossil fuels as the conflict ensues. This has created a surge in demand for wind, solar, and energy storage capacity[16] -- on the order of 50% to 100%. One unforeseen consequence of the surge of renewable technologies is an increased reliance on China to supply key technologies that can support these emerging low-carbon demands on the global energy supply chain.

These supply chain and geo-political risks have created a unique set of complex choices for asset owners and suppliers. To help identify and coordinate efforts to mitigate product scarcity risks, the following recommendations are proposed for consideration during the utilities' procurement process for grid technologies:

- **Product or Component Availability Attestations:** Request product and key component availability or lead-time status of grid technologies as part of procurement activities. This may include requesting HBOMs that identify where key component partners source their technology.
- **Product or Component Change Alerts:** Require that the supplier discloses to the purchasing asset owner when a key product or product sub-component is no longer available or whether the product or subcomponent will be sourced by a different manufacturer or fourth-party supplier.
- **Sourcing Alternatives:** Procurement organizations should identify alternative product manufacturers that coincide with the procurement organization's functionality requirements, ESG practices and security controls.
- **Product Availability Opt-out Clauses:** Ensure procurement contracts with suppliers provide the purchasing organization with a reasonable ability to limit or terminate the contract due to product availability issues, long lead-times, or other delays.

[14] https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/06/memorandum-on-presidential-determination-pursuant-to-section-303-of-the-defense-production-act-of-1950-as-amended-on-transformers-and-electric-power-grid-components/
[15] https://www.electric.coop/tiger-team-electric-co-op-leaders-join-effort-to-ease-supply-chain-problems
[16] https://www.woodmac.com/news/the-edge/how-the-russia-ukraine-war-is-changing-energy-markets/

Cloud Connectivity Product Risks

When certain grid technologies are implemented within an asset owner's environment, they might be implemented with a back-end communications infrastructure that introduces additional security and compliance risks. A specific physical device, appliance, or piece of hardware may incorporate an application or operating system that can interact with or be hosted by the supplier or a cloud service provider (CSP). The diagram below (**Figure 1**), describes various common architectural designs of today's grid technologies.

The traditional environment reflects a typical on-premises installation where cloud connectivity risk is minimal. The virtual and container environment examples reflect how certain grid technologies could be hosted on-premises or in conjunction with a CSP in coordination with the supplier. It is advisable to determine via the procurement process as to whether the grid technology under consideration operates via a virtual or container environment hosted via the supplier or a CSP.

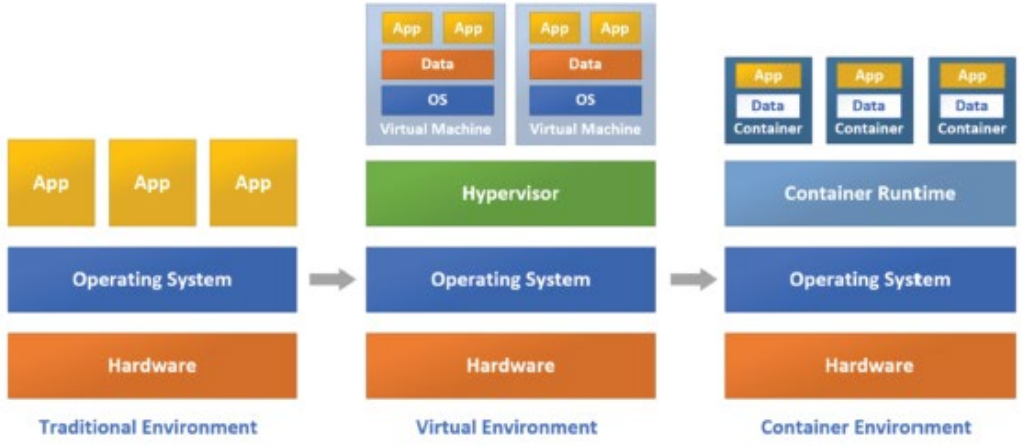


Figure 1: EPRI Research - Cloud Models[17]

To help identify and develop mitigation measures to address the risk of this type of product infrastructure, the asset owner and supplier should coordinate by considering the following practices:

1. Inquire whether the grid technology in question operates in either of the three operating environments (a virtual or container environment hosted via the supplier or a CSP).
2. For technologies that have a virtual or container environment, determine whether any of the architectural functions require off-site support or operations by the supplier or a CSP.
3. For the functions performed off-site, obtain the vendor's security and controls evidence, artifacts and attestations as described on page 1 of this document.

[17] https://www.epri.com/research/products/000000003002017577 - "Cloud concepts and security approaches that are unique to off-premise cloud implementation and provides foundational considerations for reference architectures to manage cloud service provider deployments for grid-edge applications, low-impact BES Cyber Systems located in the cloud and managed security services for low impact BES Cyber Systems."

Contributors

NERC gratefully acknowledges the contributions and assistance of the following industry experts in the preparation of this guideline. Contributions made are the views of the contributors and not necessarily those of the organizations they represent.

Name	Entity
Tobias Whitney	Fortress Information Security
Alan Kloster	Evergy
Andrea Koch	EEI
Andrew Ralph	Entergy
Betsy Soehren Jones	Fortress
Brian Russell	TrustThink
Byron Booker	Oncor
Cassie Crossley	Schneider Electric
Christine Ericson	Illinois Commerce Commission
Christopher Strain	FPL
Cordell Briggs	UTC
David James Earley	NATF
Frank Kapuscinski	RF
George Masters	Schweitzer Engineering Labs
Gregory Hardin	SERC
Jacque Mortenson	OTPCO
Jeffrey Sykes	Utility Services
Jimmy Ramirez	ERCOT
Jonathan Dashner	OSII
Ken Keels	NATF
Krista Koors	Burns & McDonnell
Lee Felter	MRO
Matt Nicklin	SIPC
Mayur Manchanda	FERC
Mike Prescher	Black & Veatch
Olga Oswalt	Sunflower
Seemita Pal	PNNL
Shari Gribbin	CNK Solutions
Teri Kelly	Northwestern
Tom Alrich	Tom AlrichLLC
Tom Duffey	Itegrity
Tom Hofstetter	NERC
Tony Eddleman	NPPD
Tope Odubanjo	NB Power
Tracie Bushman	Idaho Power
Wally Magda	WallyDotBiz LLC

Guideline Information and Revision History

Guideline Information	
Category/Topic: Supply Chain	**Reliability Guideline/Security Guideline/Hybrid:** Security Guideline
Identification Number: SG-SCH-0923-X	**Subgroup:** Supply Chain Working Group (SCWG)

Version History		
Version	**Comments**	**Approval Date**
0.1	Initial Draft submitted for 45-day comment	09/20/2023
0.2	Incorporated feedback from 45-day comment period	
1.0	Approved by the Reliability and Security Technical Committee	12/7/2023

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:

- BPS performance prior to and after a reliability guideline as reflected in NERC's State of Reliability Report and Long-Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments).
- Use and effectiveness of a reliability guideline as reported by industry via surveys.
- Industry assessment of the extent to which a reliability guideline is addressing risks as reported via surveys.

Specific Metrics

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

- The SCWG will use survey responses to evaluate the extent to which industry is using the recommendations from this security guide to address incident response measures in contracts and other documents associated with its vendors and service providers, and whether those measures were effective.
- The SCWG will seek, through meeting announcements and committee member emails, cooperation from industry to identify and interview two to three entities who have used the guide as a reference in modifying their incident response program. The information exchanged will be anonymous and record which aspects and recommendations of the guide have provided improvement for cybersecurity programs.

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.
- NERC's determination whether additional action might be appropriate to address potential risks to reliability considering the RSTC's recommendation and all other data within NERC's possession pertaining to the relevant issue.

NERC is asking entities that are users of Reliability and Security Guidelines to respond to the short survey provided in this link: Guideline Effectiveness Survey

Errata

N/A