NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Guideline

Electricity Sector - Supply Chain
Secure Equipment Delivery

December 6, 2022

RELIABILITY | RESILIENCE | SECURITY




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

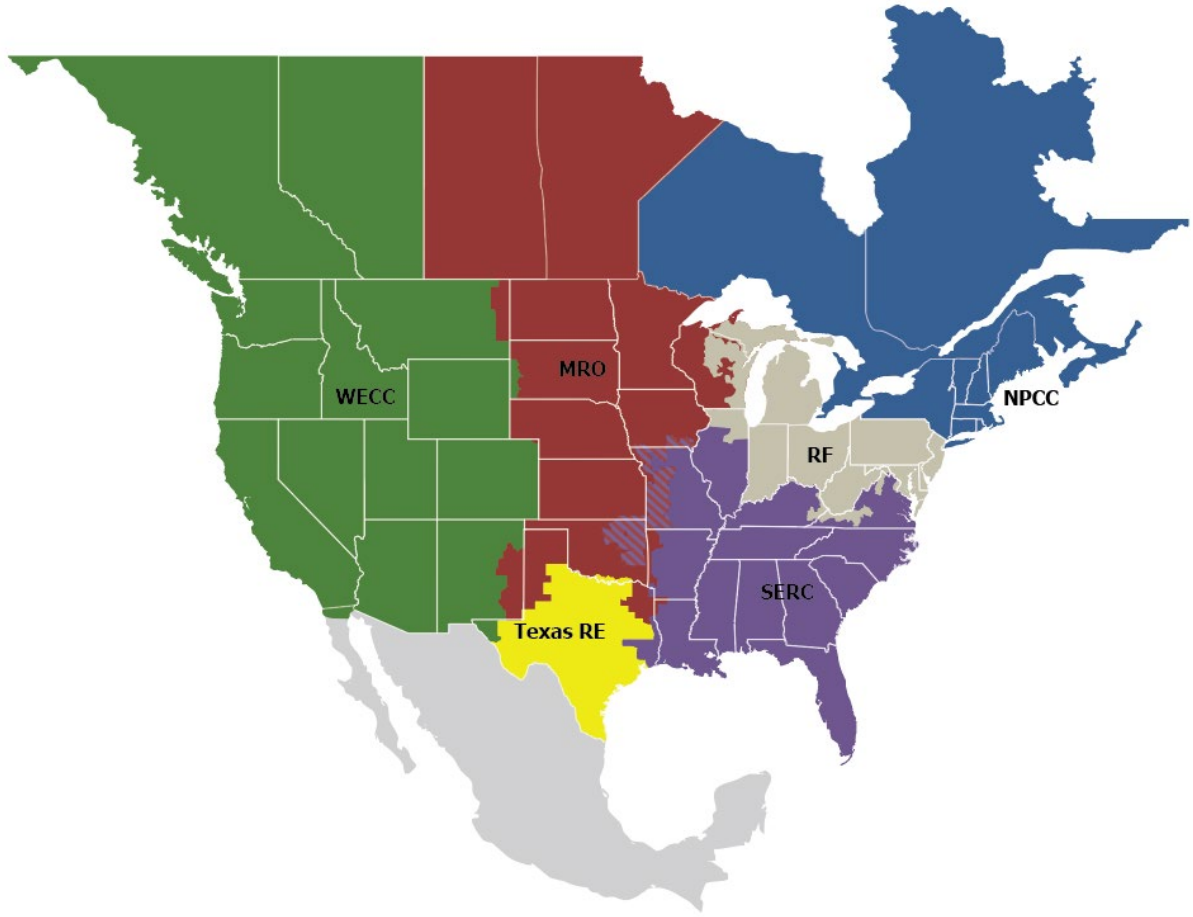
Table of Contents

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 North American Electric Reliability Corporation (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 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 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.

Executive Summary

Cargo theft, lost or damaged equipment, and malicious tampering are unfortunate realities in today's world. This guideline summarizes best practices for entities to address supply chain risks that could occur to equipment during its shipment, handling, delivery, and storage.

Choosing the security measures that are most suitable for shipped equipment should be based on the likelihood that it might be compromised, the criticality of its function and placement in the system, and the probability that a compromise would be discovered before the device is placed into service. Enhanced controls should be considered for devices that are both critical to the operation and difficult to inspect, to include storage that protects critical equipment from being tampered with before it is commissioned for use.

A focus on security in-transit presents several options for mitigating the risk of receiving compromised equipment.

Introduction

The objective of this security guideline is to distribute key practices and information on specific issues critical to promote and maintain a highly reliable and secure Bulk Electric System (BES). Security guidelines are not binding norms or parameters to the level that compliance to NERC's Reliability Standards is monitored or enforced. Rather, their incorporation into industry practices is strictly voluntary.

- *What type of equipment is being transported?*
- *What level of operation does it impact?*
- *What is the equipment's function and potential to impact the operation within the total system?*
- *How might the equipment be compromised?*

An important element of an organization's Supply Chain Risk Management Program, according to the National Institute of Standards and Technology (NIST), is safeguarding the transportation of "information systems and components, or applicable system and communications interfaces."[1] Guidance in ISO/IEC 27002:2022 cites the need to help ensure that "the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features."[2] This guideline highlights some of the aspects and potential controls to consider regarding secure transportation and delivery of systems and components from the authorized origin to your loading dock and storage location.

This document summarizes best practices for entities to secure their supply chain concerning equipment deliveries and storage.

- When assessing risk to the supply chain, it is important to weigh the cost of security against the risk of compromise. Equipment that is critical in placement and function deserve more scrutiny and should have equivalent procedures in place. Shipping, handling, and storage should be reflected in these procedures.
- Equipment can be delivered in different ways and with different levels of security, so ensure that important deliveries use the available security options that courier services offer. It is important to keep track of the chain of custody, especially for critical equipment.
- Once equipment is delivered, it is important for storage procedures to properly protect critical equipment to ensure it cannot be stolen or tampered with. Regular inspections and secure facilities reduce the risk to stored equipment.

[1] NIST SP 800-161: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
[2] ISO/IEC 27002:2022: https://www.iso.org/standard/75652.html

Chapter 1: Assessing Risk

Risk management starts with a clear understanding of the BES risks that might be experienced should a product be compromised when received. First evaluate the nature of the equipment, the sensitivity of the operation for which the equipment is intended to take part, and its ability to affect networks and other elements of the system.

Consider possible methods by which the device can be compromised and how easily this might be discovered at incoming inspection. For example, if compromise would require disassembly of the device and reprogramming chips, the security risks will be different from a device that can be reprogrammed through a communications interface. Industry stakeholders that support the reliable operations, planning and security of the BES should include in procurement language that all stakeholders must have processes in place to address supply chain risk, including incident response and secure delivery where appropriate.

The risk presented by the device is a combination of the likelihood that it might be compromised, the criticality of its function and placement in the system, and the probability that a compromise would be discovered before the device is placed into service. Enhanced controls for shipping, handling, and storage should be considered for devices that are both critical to the operation and difficult to inspect. This guideline suggests a few enhanced controls to consider such as tamper evident packaging, tracking versus chain of custody and incoming inspections beginning on page 3.

Cost Benefit

A cost-effective strategy for secure equipment delivery must consider risk and the cost to secure the equipment in question. If the security cost outweighs the potential impact a compromised product would have on the BES, other strategies should be considered.

Chapter 2: Transportation Decisions

Choose the carrier and the services you require to ensure the appropriate level of security. Maintain a list of carriers that meet the requirements for transport of particular components or systems.

Enhanced Packaging

Risk can be further reduced through enhanced security measures, such as tamper evident tape, security inks, truck/trailer serialized steel bands or security seals, Radio Frequency Identification (RFID) tracking, and blister or clamshell packaging. Are there process and procedures in place to address actions and notifications necessary if a seal is broken or the package is damaged? See Chapter 3 for suggestions on performing incoming inspections.

Tracking vs. Chain of Custody

Based on the analysis discussed above, the equipment can be tracked by using available tracking options provided by most carriers and courier services or you can require additional chain-of-custody procedures.

While tracking records the movement of a package from facility to facility, the chain of custody provides evidence of the identity of each person or entity who had access to it during its movement. This helps to ensure that equipment remains in the same condition from the moment it was sealed in the container at origin until the moment it was released into the receipted custody of another and provides accountability for discrepancies. A link[3] has been provided at the bottom of this page to the Cybersecurity & Infrastructure Security Agency Insights for Chain of Custody and Critical Infrastructure Systems paper to explore the topic in more detail.

[3] Chain of Custody: https://www.cisa.gov/sites/default/files/publications/cisa-insights_chain-of-custody-and-ci-systems_508.pdf

Chapter 3: Delivery and Storage

Security does not end once the equipment is delivered to its destination; consider incoming inspections and processes, secure storage facilities, and internal chain-of-custody through deployment of the equipment.

- *Facility of origin product and packing list details*
- *Enhanced packaging details*
- *Location, date and time of release*
- *Signatures (released by, received by)*
- *Description of the package (visual inspection)*
- *Receiver comments or observations*

Incoming Inspection

Incoming inspection provides an opportunity to formalize awareness and reduce risk by applying simple checks and recording evidence of findings, including careful documentation of exceptions. The receiving inspection procedure should dictate whom the receiving operator should contact for further scrutiny of the package if any damage or other compromise is detected. For freight deliveries, it is advised to take several photos of the unopened package while the product is still in the truck when any damage or possible compromise is found.

Inspection records should be retained as they may become of interest if the subject item is involved in an incident. The following are some inspection steps to consider:

- Is the carrier the one(s) normally used by the vendor?
- Was there any unexpected delay between shipment by the vendor and receipt of the item?
- Was the packaging and its condition consistent with other shipments from the same vendor?
- Was there any evidence on the packaging or the device indicating it may have been opened?
- Identify features of the product that may help offset the risk that it was tampered with; did you receive what you expected?
- In the case of equipment, is the unit in the expected state when first powered up? Do logs show unexpected events? Do the logs indicate the expected version(s)? The expected state should be noted for a new vendor or product and those expectations be made part of incoming inspection.
- If the shipment includes software media, is it packaged as expected?

Secure Facilities and Staff

Restricted access to receiving and warehouse facilities is among the best controls for maintaining the integrity of the equipment prior to installation to the BES. Based on risk, additional measures may be warranted, such as secure cages and video monitoring.

Another additional measure to consider is assessing and implementing training and awareness required for each warehouse position. Include training on protecting information about the equipment order. Be on the lookout for well-crafted email phishing or social engineering attempts designed to gather information. Open warehouse docks and storage areas make it easy to become a target by allowing a bad actor easy physical access.

Chapter 4: Incident Management

Consider establishing processes to be followed if a shipment is damaged when received, if it appears to be tampered with as may be indicated during your incoming inspection or if a shipment is lost. Procedures for logging incident management activities, handling of evidence, communication, and escalation should be documented and clearly communicated to management and other applicable personnel, and those procedures should be followed when an incident occurs. Where appropriate, post-incident analysis should be conducted in coordination with the vendor and the carrier. Detailed guidance on information security incident management can be found in ISO/IEC 27035-1:2016[4], ISO/IEC 27035-2:2016[5] and NIST SP 800-161.[6]

Working with your Vendor

As part of the overall contract process, during the initial qualification stage and contract updates, establish confidence in each vendor's policies and procedures for supply chain security incident management processes. Be sure to include their transportation service providers. If the transportation service provider delivering or picking up the equipment has changed without notification, contact the vendor to verify it is an authorized change. Know your preferred vendors' processes for handling shipments that appear to have been tampered with or damaged. Provide clear and timely communication regarding enhanced security requirements for any given shipment.

[4] ISO/IEC 27035-1:2016: https://www.iso.org/standard/60803.html
[5] ISO/IEC 27035-2:2016: https://www.iso.org/standard/62071.html
[6] NIST SP 800-161: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

Chapter 5: Conclusion

An important element of an organization's Supply Chain Risk Management Program is safeguarding the transportation of "information systems and components, or applicable system and communications interfaces."[7]

The following are key points to consider:

- Risk is a combination of the likelihood that the equipment might be compromised, the criticality of its function, and the probability that a compromise would be discovered before the equipment is placed into service.
- Options for secure delivery include choosing a reliable carrier, enhanced packing, and requesting additional chain of custody procedures versus just tracking pickup and delivery points.
- Security does not end once the equipment is delivered; also consider incoming inspections processes, secure storage facilities, and internal chain-of-custody procedures.
- Consider controls for having secure facilities and staff that have ongoing security training.
- Work with your vendor to establish confidence in their policies and procedures.

Cargo theft, lost or damaged equipment, and malicious tampering are unfortunate realities in today's world and can negatively impact the reliable operations, planning and security of the BES; however, an increasing focus on security in-transit presents several options for mitigating the risk of receiving compromised equipment.

Additional topics and guidance for supply chain security can be found on the *Supply Chain Risk Mitigation Program* page.[8]

[7] NIST SP 800-161 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
[8] https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx

Contributors

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

Name	Entity
Walter Magda	WallyDotBiz LLC
Alex Carlson	NERC
Angela Wheat	Southwestern Power Administration
Barry Kuehnle	FERC Office of Electric Reliability
Brenda Davis	CPS Energy
Chris Harvey	MITRE Corporation
Danny Johnson	Southwestern Power Administration
Deryk Yuill	iS5 Communications
Dominick Birolin	Strive Consulting
Frank Kapuscinski	Reliability First.org
George Masters	Schweitzer Engineering Laboratories, Inc.
Harvey Collins	Tennessee Valley Authority/Business Services
Jamie Monette	Minnesota Power
Jim McNierney	New York Independent System Operator
Jimmy Ramirez	ERCOT
John Biasi	Burns & McDonnell
Jon Terrell	Hitachi PowerGrids
Lee Felter	MRO
Lee Maurer	Oncor Electric Delivery
Mayur Manchanda	FERC
Peter Brown	Invenergy
Scotty Barron	Cooperative Energy
Steven Briggs	Tennessee Valley Authority
Terry Campbell	NERC
Tobias Whitney	Fortress Information Security
Tony Eddleman	Nebraska Public Power District

Guideline Information and Revision History

Guideline Information	
Category/Topic: Supply Chain	**Reliability Guideline/Security Guideline/Hybrid:** Security Guideline
Identification Number: SG-SCH-1222-2	**Subgroup:** Supply Chain Working Group (SCWG)

Revision History		
Version	**Comments**	**Approval Date**
1	Original – Approved by the Critical Infrastructure Protection Committee	September 17, 2019
2	3 Year Review, placed on new guideline template Approved by the Reliability and Security Technical Committee	December 6, 2022

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 and security 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 reliability assessments (e.g., Long Term Reliability Assessment and seasonal assessments)
- Use and effectiveness of a reliability and security guideline as reported by industry via survey
- Industry assessment of the extent to which a reliability 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:

- The SCWG will use survey responses to evaluate the extent to which industry is using the recommendations from this security guideline to reduce the risks associated with equipment delivery, analyzing whether the measures that it describes are improving the secure transportation and delivery of critical BPS components.
- SCWG Security Guidelines will be reviewed, updated as needed and sent out for industry comments every three years. Comments will be reviewed and addressed prior to requesting RSTC approval.

Effectiveness Survey

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

- Industry survey on effectiveness of reliability and security guidelines
- Triennial review with a recommendation to NERC on the effectiveness of a reliability or security guideline and/or whether risks warrant additional measures
- 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

Errata

N/A