NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Guideline

Supply Chain Provenance

March 22, 2023

RELIABILITY | RESILIENCE | SECURITY




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

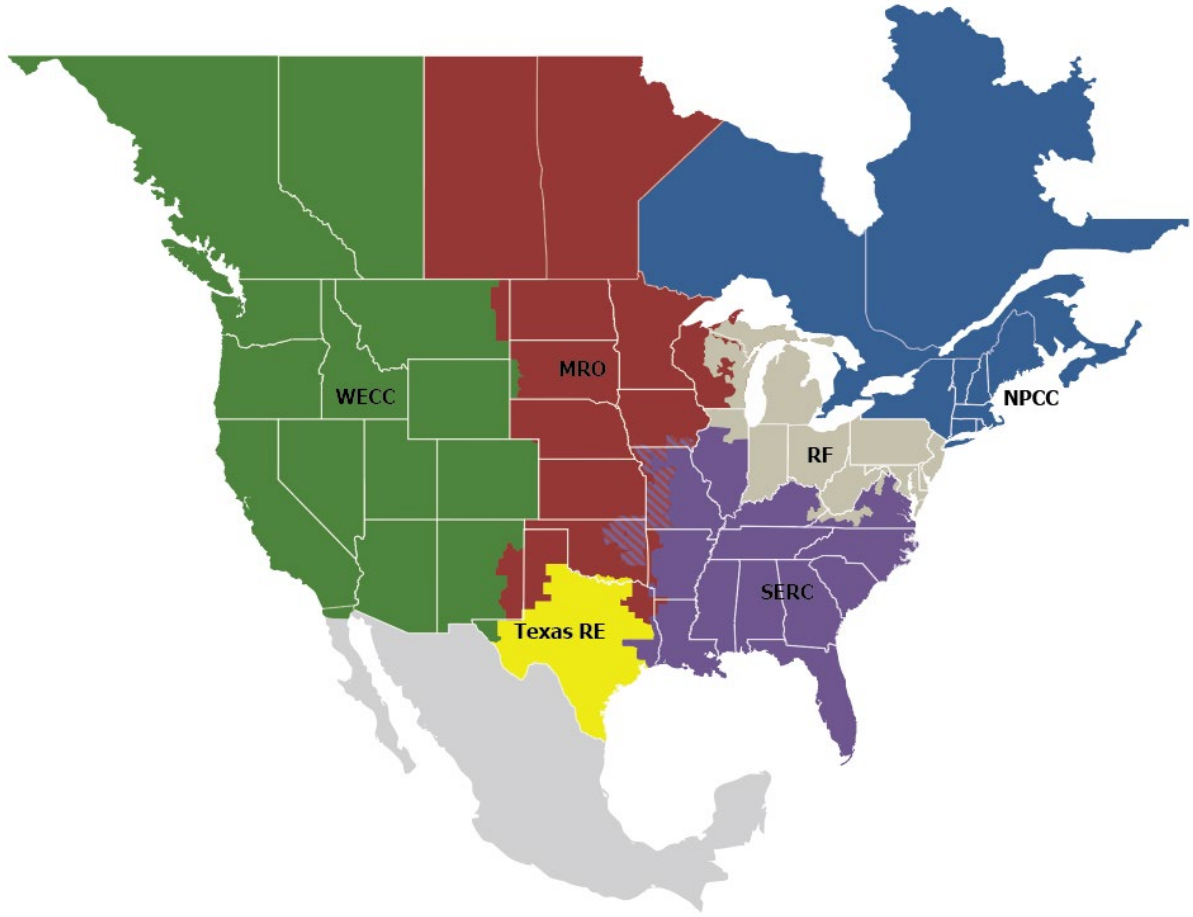
Table of Contents

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 North American Electric Reliability Corporation (NERC) and the six Regional Entities, is a highly reliable 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 comprised 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

In supply chain security, "provenance" refers to knowing about a computer system's "heritage" or that of its components (i.e., information that indicates whether its source is authentic (i.e., genuine or counterfeit)). By knowing a system or component's origin, development, ownership, location, changes to its components, and accompanying data, users are better able to identify and defend against threats to cyber security that could have an adverse impact on the BPS.

Provenance considerations are important for all stages of a system's life cycle from planning the development or procurement of a system or component to managing its installation, maintaining it while it is in use and disposing of it when it is no longer needed. An entity should have policies and practices that protect BPS systems from the actions of unknown third parties who could maliciously substitute, alter equipment, or make other changes.

Introduction

Purpose

Knowing the source of supply chain threats can help in designing targeted and effective defenses against counterfeiting, unlawful intrusion, industrial espionage, and other cyber security breaches. The risks from not knowing the threat sources occur at all stages of planning, development, installation, maintenance, and disposal.[1] The purpose of this guideline is to provide a set of best practices and recommendations for mitigating those threats; it does not impose requirements or mandates.

Applicability

At a minimum, provenance helps users ascertain whether an item is authentic (i.e., genuine or counterfeit). More fully, it relates to the chain of custody and the lineage of software and hardware; it includes things that are not part of the BPS. It entails traceability—having a "record of element origin along with the history of, the changes to, the record of, and who made those changes."[2] Acquirers, integrators, and suppliers should have best practices in provenance as a part of supply chain cybersecurity. Good provenance requires tools and processes for identity management, access, tagging, tracing, and more.

[1] Additional guidance for Supply Chain Security: https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

[2] National Institute of Standards and Technology (NIST). *NISTIR 7622: Notional Supply Chain Risk Management Practices for Federal Information Systems:* https://nvlpubs.nist.gov/nistpubs/ir/2012/nist.ir.7622.pdf

Chapter 1: Provenance Management Risks

Risks of Poor Provenance Awareness or Management

There are provenance-related risks to consider throughout the life cycle of both hardware and software. Table 1.1 provides examples of those issues.

Table 1.1: Provenance Management Risks and Possible Outcomes

Stage	Origination (Provenance) Risk	Possible Outcome
Planning	• Buyers not aware of adversaries or their actions • Provenance not considered in procurement process	• Adversaries operate undetected within active contracts, under subcontracts, or from outside • New contracts signed with no visibility past the immediate vendor
Development	• Equipment and software of unknown or unverified origin	• Adversaries operate invisibly through subcontracts • Open source software used with no vetting • Inadvertent dealings with denied persons • Remote connections hacked by using stolen credentials or back doors
Installation	• Software installed over insecure connections • Software or patches downloaded from unauthorized or fraudulent locations	• Code is inserted or altered by adversaries before insertion or use
Maintenance	• Equipment sent for repair or replacement without traceability • Weak access privileges • Weak human resource policies on personnel and access • Vendors don't inform customers of vulnerabilities or threats	• Unknown third parties substitute or alter, inserting malware or security weaknesses, intentionally, to cut cost, or negligently • Adversaries make malicious critical configuration changes • Patches do more harm than good • Adversaries penetrate live sites • Vulnerabilities and threats undetected until it's too late
Disposal	• No end-of-life disposal process	• Adversaries repurpose obsolete product or code with security vulnerabilities

Chapter 2: Best Practices

Fortunately, organizations have a number of options for mitigating the risks relevant to the provenance of software and hardware.

Best Practices in Supply Chain Provenance Management

1. **Establish a policy that governs and limits development in adversarial environments**

    a. Establish a corporate data governance policy that limits the flow to riskier development environments. As an example, the United States Bureau of Industry and Security provides information about commerce between the United States and foreign countries; while those policies pertain to exports to a list of Sanctioned Destinations,[3] an entity could develop a similar list for imports.

    b. Monitor compliance against denied persons, disapproved vendors, and related lists and orders.

    c. Establish procedural checks against lists of current and potential adversaries. Executive Order 13873 establishes criteria for prohibiting certain trade,[4] and the United States Department of Commerce maintains a consolidated screening list built from a denied persons list,[5] an entity list, and an unverified list. In addition to screening, make sure procurement decisions take into account the ultimate beneficial owner, not just the party of record.[6] Most companies' procurement departments have approved vendors, and some have a deny list based on these or similar principles and tools.

2. **Use standard contract language about provenance**

    a. Consider standard contract language regarding provenance. The Edison Electric Institute (EEI) provides contract language[7] that includes references to CIP-013 that address the "verification of software integrity and authenticity of all software and patches."[8] In addition, "Cybersecurity Procurement Language for Energy Delivery Systems" provides sample contract language for Account Management, Session Management, Logging and Auditing, and Secure Development.[9]

3. **Require internal and external vendors to validate the authenticity and origins of third-party hardware and software**

    a. Obtain confirmation from integrators and suppliers that outsourced products, components, and services are from where they purport to be, including vendor requirements to identify open source components or libraries at the prequalification stage. EEI's contract template includes contract language on validating origins.

[3] United States Department of Commerce. *Sanctioned Destinations:* https://www.bis.doc.gov/index.php/policy-guidance/country-guidance/sanctioned-destinations

[4] Executive Office of the President. *Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain*. Federal Register Vol. 84, May 17, 2019, pp. 22689-22692.: https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain

[5] United States Department of Commerce. *Lists of Parties of Concern:* https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern

[6] United States Department of the Treasury. *Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions:* https://www.fincen.gov/sites/default/files/2018-04/FinCEN_Guidance_CDD_FAQ_FINAL_508_2.pdf

[7] EEI. *Model procurement contract language addressing cybersecurity supply chain risk (Version 3)*: https://www.eei.org/issues-and-policy/Security

[8] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-2.pdf

[9] United States Department of Energy. *Cybersecurity Procurement Language for Energy Delivery*: https://www.energy.gov/ceser/articles/cybersecurity-procurement-language-energy-delivery-april-2014

b. The Open Trusted Technology Provider Standard (O-TTPS) Certification Program[10] offers language specific to open-source software and requires suppliers to provide assurance of reliable component lineage.[11]

c. North American Transmission Forum best practices recommend that suppliers be able to ensure the integrity and authenticity of all software and patches.[12]

4. Require vendors to provide a bill of materials

a. Every software or firmware supplier and every supplier of intelligent devices to an organization should be able to or have a plan to provide a bill of materials that includes a hardware bill of materials (HBOM), a software bill of materials (SBOM),[13] or both.

b. The HBOM should be generated for every configurable option for that product and hardware revision and it should be re-issued for new hardware profiles or any time a hardware component changes within the manufacturing process. Every HBOM should contain the model and version number for the product and a reference to the associated SBOM if applicable.

c. The SBOM should be re-issued whenever the software changes, including upon application of an update or patch to a product in use at the organization. An SBOM should always contain a unique version number for the product, and every version number should correspond to a unique SBOM. All bills of material should contain a unique time stamp, a means of verifying its authenticity through cryptographic methods, and a unique version number. Further information about SBOMs is available from the National Institute of Standards and Technology (NIST)[14] and the National Telecommunications and Information Administration.[15]

5. Require vendors to use strong authentication

a. Ensure that vendors are using strong multi-factor authentication methods that make it much harder for impostors to make changes to configuration management and other product delivery systems. The Payment Card Industry Data Security Standard recommends a multi-factor user authentication process that consists of something a person knows (e.g., password), something they have (e.g., token device), and something they are (e.g. biometric).[16] The United States Department of Energy recommends assigning multifactor credentials for higher-risk access.[17] ISO 27034 Standard[18] favors using computer-driven security protocols for higher risk access without human intervention.[19]

6. Require vendors to manage credentials stringently, including periodic deprovisioning

---

[10] https://www.opengroup.org/certifications/o-ttps

[11] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). *ISO/IEC 20243-1:2018 Information technology — Open Trusted Technology Provider Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 1: Requirements and recommendations:* https://www.iso.org/standard/74399.html

[12] *NATF CIP-013 Implementation Guidance: Supply Chain Risk Management Plans:* https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-013%20Supply%20Chain%20Risk%20Management%20Plans%20(NATF).pdf

[13] https://www.ntia.doc.gov/files/ntia/publications/sbom_at_a_glance_apr2021.pdf and https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1

[14] Software Security in Supply Chains: SBOM: https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1

[15] https://ntia.gov/page/software-bill-materials

[16] PCI Security Standards Council. *PCI DSS Quick Reference Guide, Data Security Standard (Version 3.2.1)*: https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

[17] United States Department of Energy. *Cybersecurity Capability Maturity Model (C2M2) (Version 2.0)*: https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf

[18] https://www.iso.org/standard/44378.html

[19] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). *ISO/IEC 27034-1:2011 Information technology – Security techniques – Application security – Part 1: Overview and concepts*: https://www.iso.org/standard/44378.html

a. Examine vendors' processes for managing their access credentials in order to make it harder for malicious actors to gain access to credentials and access privileges. The United States Department of Energy's Cybersecurity Capability Maturity Model (C2M2)'s Maturity Level Indicator 2, states that IT administrators should regularly ensure that credentials are associated with the correct person or entity and that access should be de-provisioned within defined time thresholds when it is no longer required.

7. Require vendors to deny communications with risky profiles and log denied access incidents

a. Maintain a secure boundary and log all traffic and its attributes; log access denial incidents to maximize forensic investigative potential. The Association of International Certified Professional Accountants has developed the Trust Services Criteria that include provisions to authenticate data subjects' identity as well as to communicate denial of access requests in order to allow better traceability, diagnostics, and forensics that ultimately would support better management of provenance issues.[20]

8. Use intelligence about active and potential threat sources to mitigate active threats

a. Integrate knowledge about current threats to mitigate active supply chain cybersecurity risks. The Software Assurance Forum for Excellence in Code has developed a framework that advises organizations to use a threat library in support of supply chain integrity,[21] and NIST 800-53 recommends similar measures by using "all-source intelligence" to assist in the analysis of risk.[22] Other references include the Sonatype Open Source Software Index database,[23] the NIST National Vulnerability Database,[24] and the United States Cybersecurity and Infrastructure Security Agency lists of cyber threat resources.[25] If any component has an exposed vulnerability that could pose a significant risk if exploited,[26] replace the component with a safer alternative.

b. Share cyber incident and threat information that could impact government networks. Consistent with the spirit of Executive Order 14028 of the United States General Services Administration, the best practice (and law) is to share information that can help government networks avoid malicious activity.[27]

9. Require vendors to establish a notification and patch process with safeguards against malicious actors

a. After an entity has installed a software product or intelligent device on their network, the supplier should provide regular notification to customers of vulnerabilities found in the product whether due to open source components, proprietary third party components, or the code written by the supplier itself.[28]

---

[20] American Institute of CPAs. *TSP Section 100—2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Pp. 47-50: https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

[21] Software Assurance Forum for Excellence in Code (SAFECode). *The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain:* https://safecode.org/wp-content/uploads/2014/06/SAFECode_Supply_Chain0709.pdf

[22] National Institute of Standards and Technology (NIST). *NIST SP 800-53 Rev.5: Security and Privacy Controls for Information Systems and Organizations:* https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[23] Sonatype Inc. *Sonatype OSS Index:* https://ossindex.sonatype.org/

[24] National Institute of Standards and Technology (NIST). *National Vulnerability Database Search Vulnerability Database.* https://nvd.nist.gov/vuln/search

[25] Cybersecurity and Infrastructure Security Agency. *Related Resource:.* https://www.us-cert.gov/related-resources

[26] Exploitability is an important consideration. Over 95% of vulnerabilities found in software components are not exploitable in the product itself, meaning they pose zero-to-minimum risk.

[27] United States General Services Administration. Executive Order 14028: Improving the Nation's Cybersecurity. (issued May 12, 2021): https://www.gsa.gov/technology/technology-products-services/it-security/executive-order-14028-improving-the-nations-cybersecurity

[28] Once low cost or open source tools, or subscription-based services, are available to consume machine-readable SBOMs and VEX documents for software vulnerability management purposes, suppliers should be encouraged to provide vulnerability notifications in a machine-readable format like CSAF: https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/prose/csaf-v2-editor-draft.md), or in the CycloneDX format: https://cyclonedx.org/. A supplier should also be encouraged to provide VEX reports of non-exploitable component vulnerabilities in either the CycloneDX VEX format (https://cyclonedx.org/capabilities/vex/) or using the VEX profile in CSAF: https://docs.oasis-open.org/csaf/csaf/v2.0/csd01/csaf-v2.0-csd01.html#45-profile-5-vex.

b. Review the adequacy of security within vendors' patch processes and consider requiring that suppliers have the capability to ensure the integrity and authenticity of software and patches, such as those stipulated in CIP-013. The vendor's procedures should define the process flow as well as responsibilities, accountabilities, consulted parties and informed parties, and the timeliness of security measures.

10. Verify patch authenticity via cryptography, hashes, certificates, or 2-factor authentication

a. Authentication barriers can be used to ensure the validity of patches and patch processes. EEI provides language for a contractor publishing a hash to verify legitimacy and safety of a patch.[29] NIST IR 7622 suggests performing security assessments of configuration management processes and systems to detect ongoing attacks (Section 4.3).[30] There have also been many other attacks based on creating an illegitimate web site with a URL similar to the legitimate download site for a software product that instead provides malware-tainted software. This means that the supplier should verify that the URL is correct before downloading software in addition to verifying the hash value and digital signature of any downloaded open source component.

11. Prefer vendors that have responsible procedures regarding open source software components

a. Explicitly consider the security of vendors' open source software components in procurement policies and procedures.[31]

[29] Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk, v3: https://www.eei.org/issues-and-policy/Security

[30] NISTIR 7622 Notional Supply Chain Risk Management Practices for Federal Information Systems: https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf

[31] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Risk_Considerations_Open_Source_Software.pdf

Contributors

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

Name	Entity
David Jacoby	Boston Strategies
Alan Kloster	Evergy
Andrew Ralph	Entergy
Brian Irish	SRP Net
Brian Millard	TVA
Byron Booker	Oncor
Cassie Crossley	Schneider Electric
Come Chaput	Hydro Quebec
Dan Goodlett	NERC
Danny Johnson	SWPA
Dave Cates	ACES
David Dillard	Veritas
Deryk Yuill	IS5Com
Dominick Birolin	Rokster
Eric Byres	Adolus
Eric Howell	SERC
Frank Kapuscinski	RF
Frantz Gilbert	AEP
George Masters	SEL
Gregory Hardin	SERC
Harsha Banavara	S & C Electric Co
Jacque Mortenson	OTPCO
Jamie Monette	MN Power
Jimmy Ramirez	ERCOT
Jon Terrell	Hitachi Powergrids
Jonathan Dashner	OSII
Marc Gomez	SWPA
Matt Nicklin	SI Power
Nayab Saeed	OPG
Peter Brown	INV Energy
Pierre Janse van Rensburg	BBA
Sandra Setti	Grid SME
Theresa Reichard	GRDA
Thomas Peterson	Proven Compliance
Tobias Whitney	Fortress
Tom Alrich	Tom Alrich, LLC
Tom Mitchell	Evergy
Tony Eddleman	NPPD
Tony Turner	Fortress

Guideline Information and Revision History

Guideline Information	
Category/Topic: Supply Chain	**Reliability Guideline/Security Guideline/Hybrid:** Security Guideline
Identification Number: SG-SCH-0322-2	**Subgroup:** Supply Chain Working Group (SCWG)

Revision History		
Version	**Comments**	**Approval Date**
1.0	Approved by the Critical Infrastructure Protection Committee (CIPC)	9/17/2019
2.0	3-year review; placed on new guideline template; Approved by the Reliability Security and Technical Committee (RSTC)	03/23/2023

Metrics

Pursuant to the Commission's Order on January 19, 2021, *North American Electric Reliability Corporation*, 174 FERC ¶ 61,030 (2021), reliability and security 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 or security 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 or security guideline as reported by industry via survey
- Industry assessment of the extent to which a reliability or 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 a guideline in order to measure and evaluate its effectiveness, listed as follows:

- The Supply Chain Working Group (SCWG) will ask users to respond to survey questions about this guideline and use those responses to evaluate whether it provides useful information and whether the guideline's recommendations regarding provenance have been implemented.
- SCWG Security Guidelines will be reviewed, updated as needed and sent 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 the following:

- 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