NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Guideline

Vendor Risk Management Lifecycle

March 22, 2023

RELIABILITY | RESILIENCE | SECURITY




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

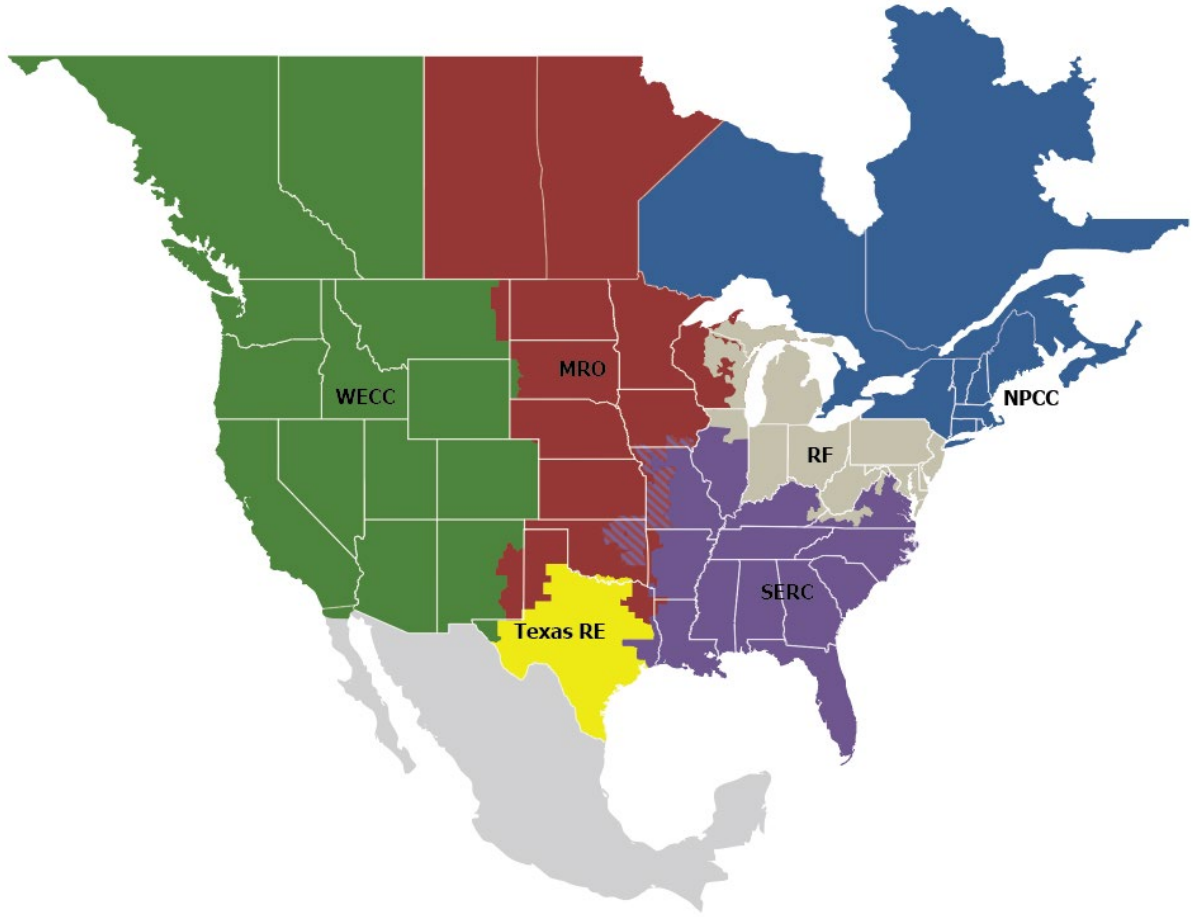
Table of Contents

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, resilience, 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

Most supply chain cyber security risks originate with vendors, so they are the most important component of an entity's Bulk Electric System (BES) supply chain cyber security risk management plan. This security guideline describes how an entity can identify, assess, and mitigate vendor cyber security risks as well as document their vendor risk management program.

Introduction

While some supply chain cyber security risks originate with the organization itself (for example, the risk that the organization will not properly supervise vendor[1] employees while onsite), most originate with vendors. For this reason, vendor risk management should be the most important component of an organization's supply chain cyber security risk management plan. The plan itself is the subject of a separate NERC Supply Chain Working Group (SCWG) guideline, *Supply Chain Cyber Security Risk Management Lifecycle*,[2] which describes the general processes of identification, assessment, and mitigation of supply chain cyber security risks.

The following are the stages of the vendor risk management lifecycle:

1. Vendor identification through a Request for Proposal (RFP) or otherwise
2. Procurement(s) from the vendor
3. Installation and use of the product or service (including vendor support and patching)
4. Termination of the vendor relationship

Vendor risks need to be addressed at each stage of the lifecycle and documented in the organization's supply chain cyber security risk management plan. Any organization, should identify, assess, and mitigate vendor risks. This security guideline provides examples of vendor risks and suggested mitigations that organizations should consider as they develop their overall supply chain cyber security risk management plans.

As discussed in the guideline, *Supply Chain Cyber Security Risk Management Lifecycle,*[3] a critical infrastructure organization, such as an electric utility, oil refinery, or natural gas pipeline, should develop and maintain two supply chain cyber security risk management plans. One plan should address the supply chain for systems and devices purchased for installation in the IT environment; the other plan should address the supply chain for systems and devices purchased for installation in the Operational Technology (OT) environment (it should be noted that some of the same systems and vendors are utilized in both environments).

This security guideline and other publications developed by the NERC Supply Chain Working Group address systems that operate the BES, but many of the recommendations can be applied to any OT system and vendors—whether the systems control gas pipelines, mining operations, electric power generation, transmission or distribution, container handling at seaports, or other critical processes.

[1] The term "vendor" in this document refers to an organization that sells a product or provides a service and "supplier" as an organization that manufactures or develops the product (hardware or software). In most cases, the vendor and supplier are the same. However, in the case of larger organizations that utilize a separate dealer channel, the vendor may be different from the supplier.
In most cases, "vendor" is used to indicate a combination vendor/supplier or a separate vendor like a dealer organization. When "supplier" is used, it refers either to a supplier that uses dealers to sell and distribute their products (e.g. Cisco™) or to the "supplier" side of a combination vendor/supplier that makes the products that the combined organization sells.
[2] NERC Guidelines Page: https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx
[3] Ibid

Chapter 1: Mitigating Risks Before Procurement

Mitigating Risks during Vendor Identification

In some cases, identifying a new vendor might be a process that is separate from actual procurements from that vendor; in other cases, the vendor identification and procurement steps will be combined. In the former case, the organization will usually put out an RFP to multiple vendors. An RFP can be open to all bidders or limited to pre-qualified vendors. While deciding which vendors should be invited to participate in the RFP, the organization could consider the factors of an approved entity lists, intelligence sources, and publicly available information (e.g., history of vulnerability handling, web site hygiene).

The RFP provides many opportunities for mitigating supply chain security risks, including the following:

- The proposal can require a mutual non-disclosure agreement (MNDA) to be signed so that any confidential information provided during the RFP process will be protected
- The RFP can include a questionnaire designed to gather information about the vendor's mitigations for the risks documented in the organization's OT supply chain cyber security risk management plan. If a standardized questionnaire is used, questions that do not relate to the set of risks that the entity has decided to mitigate in their supply chain cyber security risk management plan should be omitted; both the organization and the vendor time can be more efficient this way instead of by answering questions that the organization has already decided do not address risks that are important enough to mitigate.
- The RFP can include sample contract language, including cyber security terms and conditions; the vendor might be asked to agree to this language or to suggest modifications.
- As an alternative to including cyber security terms and conditions in contract language, the organization can make them deliverables in the RFP itself (e.g., one of the deliverables could be that the winning vendor will implement multifactor authentication for their remote access system).
- The RFP could state that, if the vendor wishes to cite particular security certifications as risk mitigation measures, they may be required to provide supporting evidence, such as an audit report by a qualified third-party assessor.
- One risk mitigation measure is to request in the RFP that the vendor provide a software bill of materials (SBOM) listing all components of their software and/or firmware that were developed by third parties—whether proprietary or open source. A SBOM allows the entity to identify components and hold the vendor accountable for providing patches for vulnerabilities identified in the components that are exploitable in the product itself. Note that it is reasonable to expect that a supplier will require an NDA to be in place before they will provide SBOMs to a customer.

Mitigating Risk in Procurement Transactions

- Every procurement should begin with an assessment of the risks that apply to procuring and installing/implementing a product or service; most of these risks apply to the vendor of the product or service being procured. In the case of a procurement in which multiple vendors were considered, this assessment is performed after the vendor has been selected. This is a procurement risk assessment (PRA). For a description of the PRA, see the section titled "Assessing Risks" in the NERC SCWG guideline, *Supply Chain Cyber Security Risk Management Lifecycle*[4].
- The organization should take steps to mitigate every high risk identified in the PRA. Some of these risks can be mitigated during procurement or installation (e.g., through a term in the contract or by installing a risky

[4] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Cyber_Security_Risk_Management_Lifecycle.pdf

device on its own network segment). Other high risks need to be mitigated during use of the product or service (e.g., patching vulnerabilities as they arise, limiting external electronic access to devices, escorting vendor employees when onsite)

- If a software supplier does not quickly patch newly identified vulnerabilities in a product that is too strategic to replace, the organization may need to implement a vulnerability management plan for that software product by taking action to quickly mitigate vulnerabilities. That way, a serious vulnerability will not remain unmitigated until the supplier finally provides a patch.

Chapter 2: Assessing Risks

Assessing Vendor Risks after Procurement

Once a vendor relationship is in place and the organization has begun obtaining products or services from the vendor, the organization needs a process for continually identifying, assessing, and mitigating both residual and new risks posed by the vendor. Following are possible steps that organizations can take to assess vendor risk:

- Questionnaires can be provided regularly (on a schedule determined during procurement, although they should be provided at least annually) to the vendor. Questionnaires should address the set of risks documented in the then-current risk management plan, including whether there have been changes (since the last questionnaire) that would increase or reduce each risk or if the vendor has effectively mitigated the risk. It is important to get the vendor to agree—preferably in contract terms—that they will answer all relevant questions in security questionnaires, and when their answer to a question indicates high risk, implement reasonable mitigation steps required by the organization.

- An important source of vendor risk is the policies governing the remote access system that is used by the vendor's own employees and contractors. The U.S. Department of Homeland Security (DHS) stated in 2018 that Russian state actors had penetrated the remote access systems of at least 200 vendors of the U.S. electric power industry in an attempt to penetrate multiple electric utilities.[5] The organization should ask vendors how they protect remote access; if they have not implemented multi-factor authentication, the organization should require them to verbally set a date to do so and include that provision the next time the contract is revised.

- Before submitting a questionnaire to a vendor, the organization could review documents made available by the vendor (on their public web site or directly to their customers) to determine whether they contain information that satisfactorily answers any questions.

- The organization may also utilize an industry-based questionnaire, such as the one prepared by the North American Transmission Forum.[6] However, the organization should always first prepare their own questionnaire that is based on the risks they have already identified in their supply chain cyber security risk management plan or modify the industry-based questionnaire to include only the questions that are relevant to the organization.[7] The organization could also simply mark any questions that are not applicable to the vendor as "N/A," so the vendor knows they don't need to answer them.

  For example, the organization might identify a risk such as, "A Supplier might not notify XYZ of any vulnerabilities in its products or services in a timely manner that does not increase threat vectors (e.g., a security patch is available, or the vulnerability is publicly known or imminent to be released publicly)." The question based on this risk might be, "Will you notify us of any vulnerabilities in your Products or Services in a timely manner that does not increase threat vectors (e.g. a security patch is available or the vulnerability is publicly known or imminent to be released publicly)?"[8]

- The organization should then review each question in the industry questionnaire and determine whether it addresses a risk that the organization has not already identified in their questionnaire. Questions that do not

[5] https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110

[6] https://www.natf.net/docs/natf/documents/resources/supply-chain/energy-sector-supply-chain-risk-questionnaire---formatted-v3-0.xlsx

[7] It is very possible that the organization will identify questions that they did not consider previously but would be good additions to the organization's questionnaire while reviewing the industry-based questionnaire. The organization should add them to their own questionnaire. However, they should also reframe the new question as a risk and add it to the organization's list of risks identified in their supply chain cyber security risk management plan (for a discussion of that plan, see the separate NERC security guideline with that title). There should never be a question in the questionnaire that does not correspond to a risk in the organization's plan although the converse is not true as there could well be risks in the plan that the organization believes should not be in the questionnaire. One reason this might happen is a case in which the risk is due to the organization itself; for example, the organization's purchasing department will purchase a networking device from an unauthorized vendor and receive a lookalike device that contains a backdoor.

[8] This is criterion 57 in the NATF Criteria v2.

address risks deemed important by the organization should be removed from the questionnaire or otherwise identified as not applicable before it is sent to the vendor. Similarly, any questions on the organization's questionnaire that are not found in the industry questionnaire should be added to it.

- It is also important to have separate questionnaires for IT and OT vendors; a vendor will need to receive both questionnaires because they sell to both environments in some cases. This is important because risks that apply to IT and OT vendors are sometimes not the same; this means there will be questions in the OT questionnaire that do not appear in the IT questionnaire, and vice versa. For example, an IT questionnaire should include many questions regarding data protection since IT vendors often store or process the organization's data. On the other hand, OT vendors seldom store or process the organization's data. Including many data protection questions in an OT questionnaire is counterproductive since both the OT vendor and the organization have better uses of their time than answering and evaluating questions that are not relevant to OT risks.[9]
- The organization should consider a vendor's certification by a third party to an industry-recognized cyber security standard, such as ISA/IEC 62443, ISO 27001, or SOC2, if available from the vendor. Such standards require annual audits and provide constant oversight of the vendor's ability to meet industry best practices for supply chain security and secure development practices. Such a certification may address many of the questions in the organization's questionnaire although the organization should not hesitate to ask the vendor to identify where specifically in the certification document each of their questions is answered and to still require the vendor to answer any questions not satisfactorily addressed by the certification. The organization should never accept a certification as the equivalent to a satisfactory answer to every question in a questionnaire without verifying that each question is in fact "answered" in the certification.
- The NERC Implementation Guidance for CIP-013-1 states: "Periodic review processes…can be used with critical vendor(s) to review and assess any changes in vendor's security controls, product lifecycle management, supply chain, and roadmap to identify opportunities for continuous improvement."[10] It is up to the organization to decide which of their vendors are "critical". The organization (e.g., a registered entity) can conduct direct assessments or use a third party engaged by the organization. The organization and the vendor should agree during the procurement on the frequency and content of assessments as well as who will bear the costs. These assessments can be expensive, both for the organization and for the vendor; the organization should make sure a direct assessment would be worth the additional cost, compared to using a questionnaire.

[9] Basic data protection questions are relevant in an OT questionnaire. One good example of those is the data protection questions in the NATF Criteria.

[10] NERC, "Cyber Security Supply Chain Risk Management Plans - Implementation Guidance for CIP-013-1," July 2017, p. 3.

Chapter 3: Mitigating Risks During Product/Service Use

Securing the Vendor's Commitment to Mitigating Risks

No matter the means used to assess vendor risks, once the organization has identified risks applicable to a particular vendor (usually, those receiving a high score in a questionnaire) the organization should ask the vendor to mitigate those risks. The vendor's agreement to do this should be documented by using one or more of the following methods:

- **RFP:** Language in an RFP should provide clear criteria that would aid the vendor in identifying security risks and any mitigations the vendor must undertake to address those risks. This will simplify the assessment process by the responsible organization in determining to what degree the vendor has mitigated each of the risks that were included in their proposal.
- **Contract:** Language in a contract should document the vendor's commitment to implement specific security controls, provide for the organization to review the vendor's progress, and identify methods for future communication on these matters. If prewritten contract language is used, it should be reviewed and tailored so that it only includes clauses that correspond to risks identified in the organization's supply chain cyber security risk management plan.
- **Letter or email:** If contract language is infeasible or impractical, a letter or email—preferably from a high-ranking manager at the vendor—can also be used to document the vendor's commitment to implementing particular security controls to mitigate risks the organization considers important.
- **Verbal commitment:** If the commitment from a vendor can only be obtained verbally, either record the conversation with permission or take notes. Document the person's name and title, date and time as well as the key points of the conversation. Document the vendor's exact words as closely as possible. Note that no permission is required to take notes of a conversation.

When evaluating the usefulness of vendor contract language for risk mitigation, it is important to consider the following:

- Contract language governing purchases made from resellers or other intermediaries may not be binding on manufacturers or software developers.
- Contract language may not apply to purchases made from stores or distributors or products or services purchased from online-only vendors, since these transactions typically are not governed by a contract.
- Because negotiating contract language with a vendor can often be expensive and time-consuming, the organization should consider whether it might be better to utilize one of the other methods listed above, especially when the organization trusts the vendor to keep their word.

Chapter 4: Verifying Risk Mitigation

Verifying Vendor Compliance with Risk Mitigation Measures

No matter how the organization has documented that a vendor agreed to comply with its request for risk mitigation(s), the organization always needs to verify that the vendor is complying (for example, implementing a policy to notify the customer when an employee with access to customer systems has been terminated). There are different means to verify the vendor's compliance; these vary according to the degree of trust the organization places in the vendor and the nature of the mitigations agreed to. These means can include a new questionnaire, emails, face-to-face meetings, phone calls, audit by the organization or a third party, and direct evidence, such as documents showing the degree to which a vendor has taken particular mitigation steps.

However, there is always the possibility that the vendor will fail to perform some or all of what it promised to do. When that happens, the customer organization should always take some action. Possible actions include the following:

- Document and communicate with the vendor the gap in performance, the expected service, and applicable contract terms or documented commitment.
- Engage management or senior leadership of the vendor to impress on them the importance of the control(s) or mitigation(s) and the need to remediate the gap in performance.
- Communicate to the vendor that performance measures will be reflected in future scoring or evaluation of new purchases of products or services.
- Take legal action if needed and possible. However, legal action should always be a last resort, not a first one.
- Evaluate terminating the relationship with the vendor. However, in many cases (especially in OT) a vendor is too valuable to terminate except in the case of gross malfeasance. In such cases, the organization should apply whatever mitigations it can to the risk from the violated term. If the organization has committed to mitigating a particular risk in its risk management plan, it must do that whether or not a vendor cooperates.

Chapter 5: Purchasing, Terminating, and Transitioning

Purchasing through Dealers and Other Third Parties

Very often, a large supplier of software or hardware used on OT networks will require customers to purchase their products through a dealer, systems integrator, value-added reseller, etc. (identified below as vendors). Therefore, the organization will sign a contract with the vendor, not the supplier. The organization will almost always be entitled to support from the supplier, but they will not usually have a contractual relationship with them. The vendor will almost never be willing to make any commitment regarding the products, whether contractual or otherwise, with the customer. In addition, the supplier will not respond to a questionnaire sent directly to them in most cases (although the customer may have some success with asking their vendor to try to obtain answers to at least some of the questions from the supplier).

The problem this very common situation presents is that almost all of the risks in any procurement where the supplier is separate from the vendor are due to the supplier. There may not be an obvious solution to this problem, but entities should still attempt to mitigate it as best they can. The bright side is that literally every other customer faces the same problem. Almost all large OT suppliers provide their customers information on their cyber security practices as well as product security issues, such as software vulnerabilities, on their websites and through webinars and emails. Moreover, the supplier's help desk will usually be very responsive to cyber security questions on specific products.

The organization will usually not be able to assess the supplier using a questionnaire, but they can answer at least some of the questions through reading on the website and talking to the help desk. Of course, there will always be questions for which the organization cannot obtain answers. For those questions, the organization should make their best educated guess that is based on their overall experience with and knowledge of the supplier.

Terminating a Vendor Relationship or Transitioning between Vendors

Whenever an organization terminates an existing vendor relationship or transitions to a new vendor, a process should be in place to identify and mitigate the risks associated with the termination or transition. For example, two risk that might arise from moving from one vendor to another is that the old vendor will continue to hold sensitive information about the organization's network or systems long after the need to do so has passed, and that retained information could fall into the wrong hands if there is a successful breach of the vendor's system.

Since this poses a risk to the organization, possible mitigations include taking an inventory of the sensitive information that the vendor holds about the organization's systems and networks as well as to require the vendor to attest that all information has been deleted.

Another type of transition between vendors is the acquisition of an organization's current vendor by a different vendor; just as in the case where a product that is used by the entity is sold to a different vendor, the organization should do an assessment of the new vendor. Then the organization should try to include in the contract with the new vendor terms that address any important unmitigated risks that apply to the new vendor, whether or not they also were included in the contract with the original vendor. If the organization's assessment identifies any "showstopper" risk considerations for the new vendor, the organization should exercise their right to stop purchasing the product or service. Additional topics and guidance for Supply Chain Security can be found at the web page, Supply Chain Risk Mitigation Program.[11]

[11] 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
Tom Alrich	Tom Alrich LLC
Harsha Banavara	S&C Electric Company
Harvey Collins	Tennessee Valley Authority
Jim McNierney	New York Independent System Operator, Inc.
Markus Epting	S&C Electric Company
Pierre Janse van Rensburg	BBA Inc.
Tom Hofstetter	NERC
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-0323-2	**Subgroup:** Supply Chain Working Group (SCWG)

Revision History		
Version	**Comments**	**Approval Date**
1	Approved by the Reliability And Security Technical Committee	9/17/2019
2	3 year review; placed on new guideline template; added metrics Approved by the Reliability And Security Technical Committee	03/22/2023

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 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 survey
- Industry assessment of the extent to which a reliability 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 ask users to respond to survey questions that pertain to the *Vendor Risk Management Lifecycle* and use those responses to evaluate whether the security guideline has provided useful information and whether the guideline's recommendations 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 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

Errata

N/A