NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Security Guideline

Cyber Security Risk Management Lifecycle

December 6, 2022

RELIABILITY | RESILIENCE | SECURITY

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

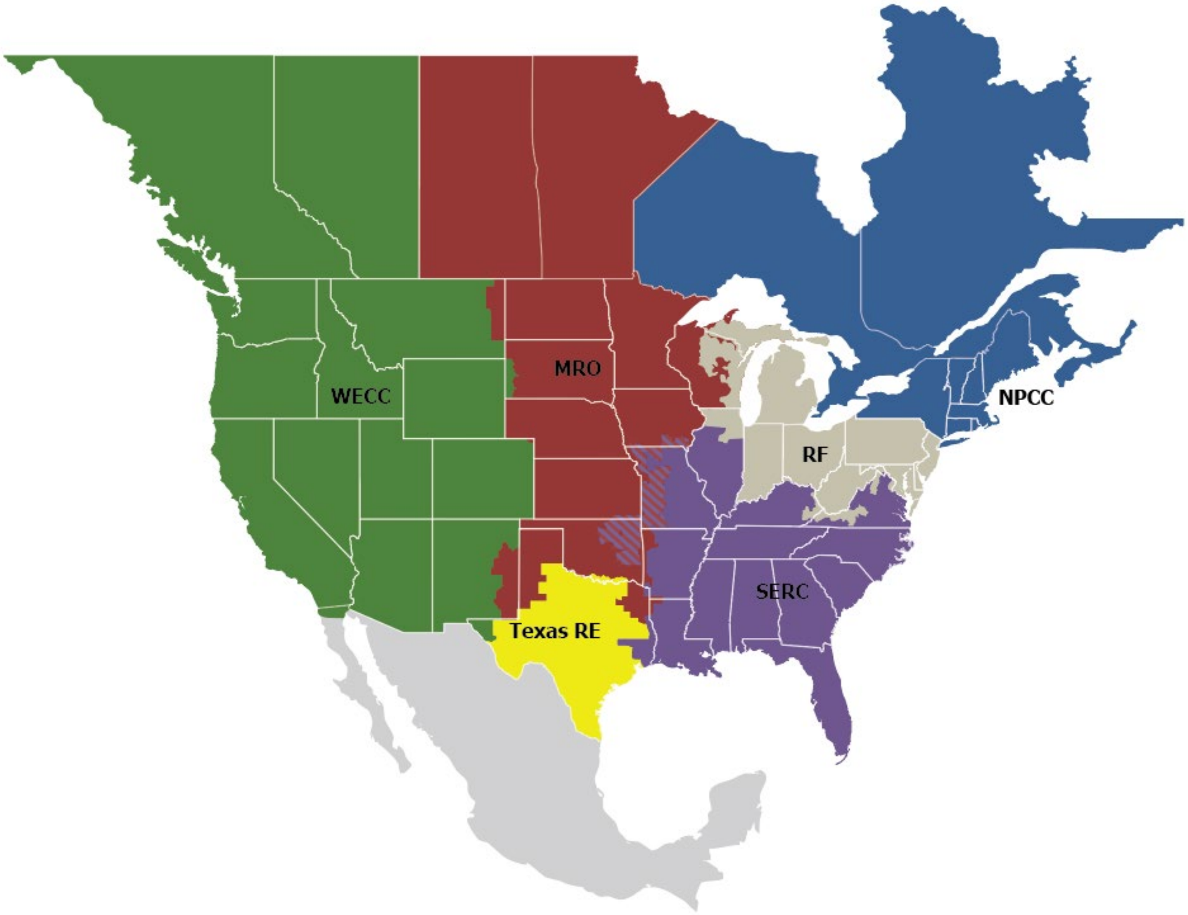
Table of Contents

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 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 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

One of the biggest sources of cyber security risk to the Bulk Electric System (BES) is cyber attacks that originate in the supply chain for operational technology (OT) systems that are used to monitor and control the BES, and for services performed on those systems. One widely documented supply chain cyber security event was the SolarWinds software supply chain attack[1], which was discovered in December 2020. While that attack is not known to have reached the BES, a similar attack in the future might achieve that goal if supply chain security risks are not properly mitigated.

To mitigate supply chain cyber security risks to the BES, the NERC entity should develop a supply chain cyber security risk management plan for risks to OT systems. The plan will describe identification, assessment, and mitigation of those risks. This security guideline describes the different components of that plan and actions the NERC entity should take to create and update the plan.

[1] https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach

Introduction

The supply chain is one of the biggest sources of cyber security risk for all businesses and government agencies in the world today. For the electric power industry in North America, supply chain cyber security is especially important because of the serious – and ongoing – attacks by foreign nation-states against critical infrastructure, as demonstrated by devastating supply chain attacks like SolarWinds[2] and Kaseya.[3]

Purpose

Because no critical infrastructure organization (including NERC entities) has resources that are adequate to mitigate all or even most of the supply chain cyber security risks that it faces, an organization should develop a plan to identify the risks that pose the greatest likelihood and mitigate them. Critical infrastructure organizations need to identify, assess, and mitigate supply chain cyber security risks to their critical operational technology (OT) assets. In the case of NERC entities, these are BES assets.

Note that the supply chain cyber security risk management process described in this security guideline is focused on OT systems. Therefore, it is fundamentally different from the supply chain cyber risk management process for information technology (IT) systems (e.g., systems used for purposes such as financial analysis or employee benefits management). For IT systems, the primary goal of cyber security is protecting data contained in, or processed by, those systems.

Applicability

In critical infrastructure industries like electric power or natural gas pipelines, the primary objective of the organization is to protect the smooth operation of a *critical process*. In electric power, that process is the smooth operation of the power grid, which for NERC entities means the BES. In natural gas transmission, the primary objective is the uninterrupted flow of gas in the pipeline. In manufacturing, it is the uninterrupted operation of the plant.

Background

Because of this difference, it is recommended that a critical infrastructure organization such as an electric utility or a gas pipeline operator have two supply chain cyber security risk management plans: one for their IT assets and one for OT assets. While some of the risks are the same in both domains, their likelihood and/or impact will often be different between IT and OT. By separating the two plans, critical infrastructure organizations can focus their risk management activities and resources on the risks that are important in each of the two domains, rather than just those that are common to both.

Another important difference between supply chain risk management in the IT and OT domains is in the risk mitigation process. For example, in IT systems, newly discovered software vulnerabilities are often patched as soon as the patch is available. However, patching OT systems is often delayed until the organization can verify that the process those systems operate will not be adversely impacted.

[2] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

[3] https://www.reuters.com/technology/kaseya-ransomware-attack-sets-off-race-hack-service-providers-researchers-2021-08-03/

Chapter 1: Identifying Risks

The organization's first objective in the supply chain cyber security risk management process is to identify risks to its critical OT assets that could have a high impact, or a high likelihood of compromise, depending on the supplier. Some risks may be common to many critical infrastructure organizations, while other risks might only affect a small number of organizations. Risks that are very unlikely to be realized in the organization's environment – or that would produce little impact if they were realized - need not be considered further.

There are many sources for information on supply chain cyber security risks and their mitigation. These include:

- American Public Power Association, Cyber Supply Chain Risk Management[4]
- NATF CIP-013 Implementation Guidance-Supply Chain Risk Management Plans[5]
- The NATF Criteria v2.0[6]
- NIST 800-161 r1[7]
- NERC CIP-013-2 R1.2.1 – R1.2.6[8]

The above documents describe mitigations for supply chain cyber security risks, not the risks themselves. However, it is easy to reword these mitigations as risks – although it is important to remember that a statement of a risk must include the impact on the critical process (which for NERC entities is the BES) that would result from the realization of the risk. An example of a good risk statement is "A vendor system that has been granted system-to-system access to an organization's OT systems might be compromised by a malicious third party or a rogue insider and used to exploit one of the organization's OT assets, resulting in damage to the BES or to another critical process." This is a restatement of one of the two risks behind the mitigations in NERC CIP-013 R1.2.6.

Identifying risks and their impact on the system is a process called Threat Modeling. For more information on threat modeling, see Open Web Application Security Project (OWASP) Threat Modeling.[9]

The result of the risk identification step is a list of supply chain cyber security risks that the organization deems worthy of consideration. Because the organization will not be able to mitigate all risks, it must determine which are most likely to occur in their environment (or in their suppliers' environments), and which risks might have a significant impact were they to be realized. Only risks that have some likelihood of occurring in the organization or the vendor's environment, or that could have a serious impact if realized, need to be identified in the entity's supply chain cyber security risk management plan ("plan").

For example, one organization might decide there is some likelihood that a vendor employee that performs onsite service on its OT systems would deliberately compromise them, and that this could cause a high impact if it occurred. The organization would want to identify this as one of the risks in the plan. On the other hand, another organization may never allow vendor employees to have onsite access to OT systems, meaning the likelihood of this happening is very low. Given that, this organization might not include the risk in its plan.

[4] https://www.publicpower.org/resource/cyber-supply-chain-risk-management

[5] https://www.natf.net/docs/natf/documents/resources/supply-chain/natf-cip-013-implementation-guidance-supply-chain-risk-management-plans.pdf

[6] https://www.natf.net/docs/natf/documents/resources/supply-chain/natf-supply-chain-security-criteria.xlsx

[7] https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

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

[9] https://owasp.org/www-community/Threat_Modeling

Chapter 2: Assessing Risks

Once the organization has identified risks, it needs to assess its vendors to determine the degree of risk they pose with respect to each risk that was identified; in most cases, the vendor assessment will be conducted via a questionnaire. Because risk is a combination of likelihood and impact, the organization should score the vendor for the likelihood and impact[10] of each risk, based on its answers to the questionnaire or on other evidence available to the organization.

Because there is no way to reliably assign even rough numerical values to the likelihood or impact of a cyber event in the OT domain, it is recommended that the organization assign a value of either high ("unmitigated") or low ("mitigated") to both likelihood and impact of each risk. If *either* likelihood or impact of a particular risk is low, the risk itself will have a low value. If *both* likelihood and impact are high, the risk will have a high value.

For example, consider the risk that the software build process of a widely used software product will be compromised and used to insert a backdoor[11] into the OT environment of an electric utility or other critical infrastructure organization. The backdoor could be exploited to cause a serious impact to the BES or another critical process. If the utility's assessment of the software vendor determines that it lacks adequate controls to prevent a compromise of its build process, the utility would probably assign it a high likelihood value for this risk. In addition, if the utility determines that the impact of this attack on the BES could be high, it will assign the attack a high impact value as well[12]. Because both the likelihood and impact values are high, the value for *this risk* for this supplier would be high.

[10] The organization might decide to assign a single impact value – high or low – to each risk, if they think the impact (on the critical process such as the BES) of the risk being realized will not vary by supplier.

[11] A backdoor exploit was the source of the SolarWinds attacks that were revealed in December 2020.

[12] The organization might determine that the impact of this attack on the BES or critical process would be low, in which case they would assign a low impact value. This might occur if the software in question is installed outside of the Electronic Security Perimeter(s) around the OT networks. Therefore, even if the backdoor were activated by an attacker, the attacker would very likely be prevented from reaching the systems that run the BES. Therefore, the value for this risk would be low.

Chapter 3: Mitigating Risks

If the supplier's value for any risk has been assessed as high, the risk needs to be mitigated. Some high risks should be mitigated as soon as possible, such as the risk to the software build process just described. (See **Assessing Risks**) Some other risks need to be mitigated either during, or after procurement. An example of the latter is the risk that a supplier will not properly monitor the behavior of its employees who are involved with supporting the customer organization. This may allow a supplier's rogue employee to seek to damage systems critical to the BES or another critical process. The mitigation might be to have an organization employee escort the supplier's personnel whenever they are onsite, and to require supervised remote access.

Some risks can be mitigated through contract language, although there should always be verification by the organization to confirm that the language is followed; there should also be consequences if the language is not followed. Some risks can only be mitigated when there is a procurement transaction – e.g., requiring the supplier to take particular steps like documenting reasons for open logical ports on a cyber system.

The goal of mitigation for a risk is to bring its value from high to low; in other words, to reduce either likelihood or impact of the risk (or both) from high to low. In the earlier example, the organization might require a software supplier to follow the Google Supply-chain Levels for Software Artifacts (SLSA) framework[13] in securing its software build environment. When a supplier has documented that they are following this framework, the organization might lower the risk likelihood value for this supplier from high to low. Thus, the value for the risk itself would move to low, meaning no further mitigation is required.

Note that fully mitigating a particular risk will often involve applying multiple controls. Using the example above, an organization might decide that, in addition to requiring its suppliers to implement SLSA, it should monitor what seem to be "normal" communications between a software product installed on its network and its "mother ship"; i.e., information sent from the organization to the supplier. This would also reduce the likelihood of the risk being realized, since it could prevent the attackers from being able to exploit the backdoor, even though the backdoor had been inserted into the build process and had been distributed with the latest software update.[14]

Whenever the proposed mitigation requires a commitment from a supplier to perform particular actions or implement specific controls, the commitment should be documented in some form. It might be documented in a request for proposal or contract language, but it can also be documented with a letter or email from the supplier, or even with a memo that describes a phone conversation in which the supplier made a verbal commitment to take certain actions.

However, no matter how the organization documents the supplier's commitment to implement mitigations, the organization needs to verify that the supplier keeps its promises. See the *Vendor Risk Management Lifecycle* security guideline in this series for further discussion of this topic.[15]

In some cases, a supplier may refuse to cooperate in performing a particular mitigation, yet the relationship with the supplier cannot be terminated for operational or legal reasons (which is often the case for OT systems). In those cases, it is up to the organization to implement appropriate mitigations on its own; for example, a supplier's device deemed to pose a significant risk may be installed on the organization's own network where it can be monitored more closely and to prevent the potential compromise of other devices.

[13] https://slsa.dev/

[14] Monitoring outbound communications from the user's network was an important detection measure for the SUNBURST malware in the SolarWinds attacks.

[15] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Vendor_Risk_Management_Lifecycle.pdf

Chapter 4: Procurements and Installations

Supply chain cyber security risk mitigations need to be considered throughout the lifecycle of a product or service. This starts with procurement of the product or service and ends with retirement of the product or termination of the service. However, the most important opportunities to mitigate supply chain cyber security risks is during procurement and installation of a product, or procurement and use of a service.

The organization should perform a procurement risk assessment at the start of the procurement process, which might be any of the following:

- procurement from a new supplier
- procurement of a new product or service from an existing supplier
- procurement of an existing product or service from an existing supplier
- when the product or service has not been procured for one year or more

The procurement risk assessment will usually be based on the most recent assessment that was performed for that supplier, as long as it is not out of date (which usually means more than one year old). If the assessment is current, the organization should review it to determine if there have been any material changes since it was conducted - for example, if the supplier was recently acquired by a foreign owner and the organization has questions, this may indicate that some risks previously ranked as low might now be ranked high. If there are such material changes, some or all of the assessment may have to be re-executed.

Using the results of the previous assessment and the results of any required re-assessment, the organization will determine whether there are any high risks relevant to the supplier in the procurement. If so, the organization should take steps to mitigate those risks during the procurement process, perhaps by requiring the supplier to commit (in contract language or using non-legal means like an email) to perform particular mitigations as part of the procurement, and also by committing the organization itself to perform particular mitigations, when this is appropriate.

The goal of mitigation is to reduce the level of every risk that was assessed a high value to low by identifying measures that can be applied during the procurement or installation of a product, or the procurement or use of a service. For example, if the organization is concerned that a network device might have been tampered with during shipment, they should discuss with the supplier the tests they can apply to resolve their suspicions.

Chapter 5: Updating the Risk Management Plan

All the steps described above should be included in a supply chain cyber security risk management plan. The plan should be updated at least annually and perhaps more frequently if developments warrant doing so. The update should include:

- Identifying significant new risks that should be addressed in the plan (i.e., risks that *could* have a high likelihood or impact, depending on the supplier);
- Re-assessing any supplier whose assessment is more than one year old, based on the updated set of risks; and
- Reviewing mitigations for each risk, to determine whether they are still appropriate. Considerations include whether any current mitigations have proven insufficient or unnecessary, and whether new mitigations have become available that might provide further risk reduction.

Conclusion

No organization has the resources to mitigate all supply chain cyber security risks. Following an approach such as the one described above is a good way to ensure that the organization mitigates the greatest possible supply chain cyber security risk, given its available resources.

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
James Baldwin	Lower Colorado River Authority
Harvey Collins	Tennessee Valley Authority
Tony Eddleman	Nebraska Public Power District
Markus Epting	S&C Electric Company
Lew Folkerth	ReliabilityFirst
Tom Hofstetter	NERC
Pierre Janse van Rensburg	BBA Inc.
George Masters	Schweitzer Engineering Laboratories, Inc.
Jim McNierney	New York Independent System Operator, Inc.

Guideline Information and Revision History

Guideline Information	
Category/Topic: Supply Chain	**Reliability Guideline/Security Guideline/Hybrid:** Security Guideline
Identification Number: SG-SCH-1222-3	**Subgroup:** Supply Chain Working Group (SCWG)

Revision History

Version	Comments	Approval Date
1	Approved by the Critical Infrastructure Protection Committee	9/17/2019
2	3 year review – placed on new template; reviewed/updated all Approved by the Reliability and Security Technical Committee	12/06/2022

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 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.

- The Supply Chain Working Group (SCWG) will ask users to respond to survey questions that pertain to risk assessment practices that users have adopted and whether this security guideline has provided useful information.
- 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