NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

~~DRAFT~~

# Cyber Security Supply Chain Risks

## Staff Report and Recommended Actions

~~March 28~~May ~~8~~17, 2019

RELIABILITY | ACCOUNTABILITY




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

# Table of Contents

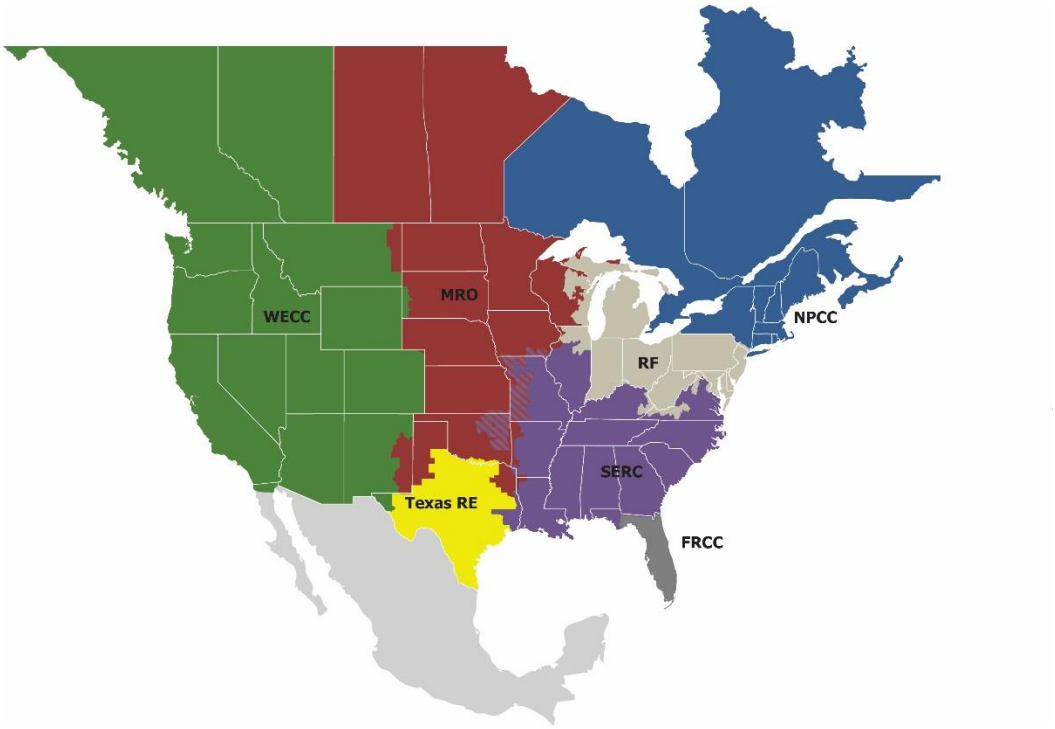
# Acknowledgements

Apart from the efforts of NERC staff, the success of any report depends largely on the guidance and input of many others. NERC wishes to take this opportunity to express a special thanks to Dr. Joseph Baugh of the Western Electricity Coordinating Council and Ray Sefchik of Reliability First for their exceptional contributions in helping to improve the content of this report. NERC also wishes to take this opportunity to express a special thanks to the Critical Infrastructure Protection Committee Supply Chain Working Group for their valuable contribution to this report. The authors also acknowledge and appreciate the significant contributions from individuals, working groups, subject matter experts, and organizations whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this report.

# Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven Regional Entities (REs), 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.

The North American BPS is divided into seven RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.




| | |
|---|---|
| **FRCC** | Florida Reliability Coordinating Council |
| **MRO** | Midwest Reliability Organization |
| **NPCC** | Northeast Power Coordinating Council |
| **RF** | ReliabilityFirst |
| **SERC** | SERC Reliability Corporation |
| **Texas RE** | Texas Reliability Entity |
| **WECC** | Western Electricity Coordinating Council |

# Executive Summary

The supply chains for information and communications technology and industrial control systems may provide various opportunities for adversaries to initiate cyber attacks, thereby presenting risks to Bulk Electric System (BES)[1] security. NERC is committed to using its many reliability tools to support industry's efforts to mitigate supply chain risks.

In 2017, NERC developed new and revised critical infrastructure protection (CIP) Reliability Standards to help mitigate cyber security risks associated with the supply chain for high and medium impact BES Cyber Systems. These standards, collectively referred to as Supply Chain Standards, consist of new Reliability Standard CIP-013-1 and revised Reliability Standards CIP-010-3 and CIP-005-6. Consistent with the risk-based framework of the NERC CIP Reliability Standards, the Supply Chain Standards will be applicable to the highest-risk systems that have the greatest impact to the grid. The Supply Chain Standards will require entities that possess high and medium impact BES Cyber Systems to develop processes to ensure responsible entities manage supply chain risks to those systems through the procurement process, thereby reducing the risk that supply chain compromise will negatively impact the BPS.

When adopting the Supply Chain Standards in August 2017, the NERC Board of Trustees (Board) directed NERC to undertake further action on supply chain issues. Among other things, the NERC Board directed NERC to study the nature and complexity of cyber security supply chain risks, including those associated with low impact assets not currently subject to the Supply Chain Standards and develop recommendations for follow-up actions that will best address identified risks.

In this report, NERC documents the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommends actions to address those risks.

Upon evaluation of the potential supply chain risks presented by Electronic Access Control or Monitoring Systems (EACMSs), and in response to the directive of FERC in Order No. 850 to include such systems within the scope of the Supply Chain Standards,[2] NERC staff recommends revising the Supply Chain Standards to address EACMSs that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.

Additionally, based on the supply chain risks presented by such assets, NERC staff recommends revising the Supply Chain Standards to address Physical Access Control Systems (PACSs) that provide physical access control (excluding alarming and logging) to high- and medium-impact BES Cyber Systems.

At this time and based on the available information, NERC staff does not recommend modification of the Supply Chain Standards to include all low impact BES Cyber Systems. NERC staff recommends further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with External Routable Connectivity as follows: first, by issuing a Request for Data or Information pursuant to Section 1600 of the NERC Rules of Procedure; and second, by continued monitoring of the application of the criteria in CIP Reliability Standards that differentiate medium impact BES Cyber Systems from low impact through the use of ~~pre-audit~~industry surveys and questionnaires following the implementation of the Supply Chain Standards. To address the potential risks associated with the supply chain for such systems prior to completion of this study, NERC staff will work with the Critical Infrastructure Protection Committee (CIPC) Supply Chain Working Group to develop a guideline to assist entities in voluntarily applying supply chain risk management plans to low impact BES Cyber Systems.

[1] Unless otherwise indicated, capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary"), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

[2] Order No. 850, *Supply Chain Risk Management Reliability Standards*, 165 FERC ¶ 61,020, at P 30 (2018) ("Order No. 850").

Due to varying levels of risk, NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities with evaluating their Protected Cyber Assets (PCAs) on a case-by-case basis to determine what, if any, additional supply chain protections are needed.

NERC staff recommends that entities refer to industry practices and guidelines, such as those developed by the North American Transmission Forum, the American Public Power Association and National Rural Electric Cooperative Association, and the North American Generator Forum, when developing their CIP-013-1 process(es) for the procurement of BES Cyber Systems.

Because supply chain risks are complex and constantly evolving, NERC staff also recommends conducting additional data collection on BES supply chain risk management through the use of ~~pre audit~~industry surveys and questionnaires. Such evaluation may result in additional recommendations for future actions. To encourage full and frank industry participation, NERC Staff recommends that these surveys be completed independently of any mandatory compliance monitoring or enforcement process.

## Next Steps on Recommendations

NERC will work through its existing processes with stakeholders to review NERC staff's recommendations and determine appropriate follow up actions.

# Introduction

## Background

In recent years, the Federal Energy Regulatory Commission (FERC or the Commission), NERC, and the industry have identified risks from the supply chain as a potential threat to BES reliability. Supply chains for information and communications technology and industrial control systems are long and multidimensional, involving numerous parties in a multitude of countries across the globe. In procuring products and services for their operations, BPS owners and operators typically rely on vendors and contractors that may use multiple third-party suppliers for components used in their products or technologies. Malicious actors may target one or more vendors in the supply chain to create or exploit vulnerabilities that could then be used to initiate cyber attacks on BES Cyber Systems and equipment.

On July 21, 2016, FERC issued Order No. 829,[3] directing NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as follows:

> "[FERC directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, discussed in detail [in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."[4]

Following the issuance of Order No. 829, NERC staff initiated Reliability Standards Project 2016-03 Cyber Security Supply Chain Risk Management to address supply chain risk management in the CIP Reliability Standards. The project resulted in the development of the Supply Chain Standards that consist of new Reliability Standard CIP-013-1 and modifications to Reliability Standards CIP-005-6 and CIP-010-3.

The Supply Chain Standards support reliability by requiring responsible entities to implement plans and processes to mitigate supply chain cyber security risks to high and medium impact BES Cyber Systems. Consistent with Order No. 829, the proposed Reliability Standards focus on the following four security objectives: software integrity and authenticity, vendor remote access protections, information system planning, and vendor risk management and procurement controls.

Reliability Standard CIP-013-1 requires responsible entities to develop and implement plans to address supply chain cyber security risks during the planning and procurement of high and medium impact BES Cyber Systems. Modifications in CIP-005-6 and CIP-010-3 bolster the protections in the currently-effective CIP Reliability Standards by addressing specific risks related to vendor remote access and software integrity and authenticity, respectively, in the operational phase of the system life cycle.

The Board adopted the Supply Chain Standards at its August 10, 2017, meeting. FERC approved the Supply Chain Standards with directives for additional modifications to address EACMSs in Order No. 850, issued October 18, 2018.[5]

[3] Order No. 829, *Revised Critical Infrastructure Protection Reliability Standards,* 156 FERC ¶ 61,050 (2016).
[4] *Id.* at P 2 (internal citation omitted); *see also id*. at PP 44-45.
[5] Order No. 850, *supra* note 1.

# August 2017 Board Resolutions

In adopting the Supply Chain Standards, the Board concurrently adopted additional resolutions related to implementation and risk evaluation.[6] The resolutions outline six actions for NERC management and stakeholders to take in assisting with the implementation and evaluation of the Supply Chain Standards as well as other actions to address potential supply chain risks for assets not currently subject to the standards.

The Board's August 2017 resolutions include the following:

- **Support Effective and Efficient Implementation of the Supply Chain Standards:** The Board requested that NERC promptly commence preparations for the implementation of the Supply Chain Standards by using similar methods during the transition to version 5 of the CIP Reliability Standards and report regularly to the Board on those activities.
- **Cyber Security Supply Chain Risk Study:** The Board requested that NERC, in collaboration with others, study the nature and complexity of cyber security supply chain risks, including those associated with low impact assets not currently subject to the Supply Chain Standards, and develop recommendations for follow-up actions that will best address identified risks. The Board requested that NERC submit an interim report within 12 months and a final report within 18 months. NERC presented the interim report to the Board in August 2018.
- **Communicate Supply Chain Risks to Industry:** The Board requested that NERC communicate supply chain risk developments and risks to industry in connection with the Cyber Security Supply Chain Risk Study (i.e. this report).
- **Forum White Papers:** The Board requested that the North American Transmission Forum (NATF) and the North American Generation Forum (NAGF) (collectively, the "Forums") develop (and distribute as permissible) white papers to address best and leading practices in supply chain management as described in the resolution.
- **Association White Papers:** The Board requested that the American Public Power Association (APPA) and the National Rural Electric Cooperative Association (NRECA) (collectively, the "Associations") develop (and distribute, as permissible) white papers to address best and leading practices in supply chain management, as described in the resolution, focusing on smaller entities that are not members of the Forums, for the membership of the Associations.
- **Evaluate Supply Chain Standard Effectiveness:** The Board requested that NERC, in collaboration with technical committees and other experts, develop a plan to evaluate the effectiveness of the Supply Chain Standards as described in the resolution and report to the Board.

The activities undertaken by NERC, the Forums, and the Associations to address the Board's supply chain resolutions are designed to establish a collective understanding of the supply chain risk to the BES and activities to mitigate those risks.

This report addresses the Board's second resolution, which is to prepare a study of cyber security supply chain risks. Building upon the interim report presented to the Board in August 2018 (discussed below), this report addresses the risks associated with low impact BES Cyber Systems, EACMSs, PCAs, and PACSs and the actions that should be taken to address those risks. This report also makes reference to certain white papers and guidance documents prepared by the Forums and Associations in response to the Board's fourth and fifth directives.

[6] The Additional Resolutions for Agenda Item 9.a: Cyber Security – Supply Chain Risk Management – CIP-005-6, CIP-010-3, and CIP-013-1, NERC Board of Trustees Meeting, August 10, 2017, is available at the following: http://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf.

All reports are posted on NERC's website under the Supply Chain Risk Mitigation Program Initiative[7] page. In Appendix A to this report, NERC summarizes the activities taken to address the other Board resolutions.

## EPRI Interim Report (August 2018)

NERC engaged the Electric Power Research Institute (EPRI) to provide an independent assessment of industry supply chain risks to facilitate NERC's supply chain risk study. NERC presented EPRI's report, titled *EPRI Supply Chain Risk Assessment Report*,[8] to the Board in August 2018. In this report, EPRI contributed the following actions:

- Performed an assessment of product/manufacturer types used on the BES for Supervisory Control and Data Acquisition (SCADA), network and telecommunications, and commercial off the shelf operating systems
- Provided an analysis of emerging best practices and standards used in other industries to mitigate supply chain risks, concentrating on practices currently not considered in the scope of the existing CIP Reliability Standards
- Provided a study of the applicability of the CIP Reliability Standards to supply chain risks
- Provided a list of recommendations to reduce residual supply chain risks and facilitate the collection of additional information for future evaluation, so that, prior to any changes in policy, data can be obtained, assessed, and discussed in a transparent manner

## Forum and Association White Papers

In response to the Board's fourth resolution, the NATF and NAGF each prepared White Papers that provide considerations for their member entities on implementing robust cyber security risk management plans and programs.

The NATF White Paper, titled *Cyber Security Supply Chain Risk Management Guidance*,[9] recommends several best and leading practices for members in establishing and implementing their supply chain risk management programs. These practices include considerations for procurement, specification, vendor requirements, and managing existing equipment activities. NATF's White Paper identifies three hallmarks of an effective program, including foundational practices that coordinate supply chain and cyber security risk management efforts; organization-wide communication where supply chain risk management is supported throughout the business and implemented throughout the system-development life cycle; and risk management processes with clearly defined criteria, risk evaluation, and risk response components.

The NAGF White Paper, titled *Cyber Security Supply Chain Management*,[10] identifies examples for generation entities to consider when developing and implementing their cyber security risk management plans. The NAGF White Paper describes a risk-based approach by which entities conduct an initial screen to determine where additional vendor supply chain risk assessments are required, taking into account the entity's cyber assets impact rating criteria, asset connectivity, vendor connectivity, presence of Transient Cyber Assets and Removable Media, support staff considerations, security awareness/training considerations, and considerations related to Personnel Risk

[7] https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx
[8] EPRI, *Supply Chain Risk Assessment Report* (July 2018), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/EPRI_Supply_Chain_Risk_Assessment_Final_Report_public.pdf ("EPRI Interim Report").
[9] NATF, *Cyber Security Supply Chain Risk Management Guidance* (June 20, 2018), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NATF%20Cyber%20Security%20Supply%20Chain%20Risk%20Management%20Guidance.pdf ("NATF White Paper").
[10] NAGF, C*yber Security Supply Chain Management White Paper* (2018), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NAGF%20SC%20White%20Paper%20final.pdf ("NAGF White Paper").

Assessments performed for staff and contractors. If the entity determines that a risk assessment is required, the entity should consider the level of risk posed by the vendor itself and the product or service it provides to determine the appropriate level of supply chain controls required. The NAGF White Paper describes several vendor risk attributes and product/service attributes for the entity to consider in evaluating potential risks.

In response to the Board's fifth resolution, APPA and NRECA prepared a White Paper, titled *Managing Cyber Supply Chain Risk – Best Practices for Small Entities*.[11] The APPA/NRECA White Paper identified several practices for smaller entities with low impact BES Cyber Systems to consider in managing risks from the supply chain. APPA and NRECA identified several best practices for its member entities to consider based on interviews with several smaller entities regarding their supply chain risk management programs. These best practices include, among other things:

- Organizational aspects, such as having senior leadership support for supply chain risk management and conducting enterprise-wide cyber risk assessments;
- Selecting vendors with an eye toward reducing supply chain risk, including using well-known, trusted, and established vendors and considering vendors who have completed third-party accreditation or self-certification of their supply chain practices;
- Placing appropriate limitations surrounding vendor remote access to systems; taking steps to ensure software integrity prior to installation;
- Placing appropriate controls around software updates and patch management.

## Order No. 850 Approving the Supply Chain Standards

FERC approved the Supply Chain Standards in Order No. 850, issued on October 18, 2018. While finding that the standards addressed the Commission's directive in Order No. 829 and constitute "substantial progress" in addressing supply chain cyber security risks, the Commission also issued two directives to NERC.

First, noting the significant role that EACMSs play in the protection scheme for medium and high impact BES Cyber Systems, the Commission found that excluding EACMSs from the scope of the Supply Chain Standards presents risks to the cyber security of the BES. Therefore, the Commission directed NERC to develop modifications to the standards to address EACMSs associated with medium and high impact BES Cyber Systems and to submit those modifications within 24 months of the effective date of the final rule.[12]

Second, while continuing to express its concern that excluding certain categories of assets (PACSs and PCAs) from the standards could pose a reliability risk, the Commission found that NERC is taking "adequate and timely steps" to study whether these items should be included in the standards. The Commission accepted NERC's commitment to evaluate the risks of PACSs and PCAs (in addition to low impact BES Cyber Systems) in its study of cyber security supply chain risks and directed NERC to file the final report with FERC upon its completion. The Commission stated that it would be in a better position to consider what further steps, if any, should be taken to protect reliability after receipt of this final report.[13]

Under the approved implementation plan, the Supply Chain Standards will become effective in the United States on the first day of the first calendar quarter that is 18 months after the effective date of the final rule, which is July 1, 2020.

[11] APPA/NRECA, *Managing Cyber Supply Chain Risk – Best Practices for Small Entities* (Apr. 25, 2018), https://www.cooperative.com/programs-services/government-relations/regulatory-issues/documents/supply%20chain%20white%20paper%204-25%20final.pdf ("APPA/NRECA White Paper").
[12] Order No. 850 at P 30.
[13] Order No. 850 at PP 31, 67.

# Chapter 1: Supply Chain Risks to the Bulk Electric System and Standards and Practices for Addressing those Risks

## Overview

In recognition of the potential risks to BES reliability posed by supply chain vulnerabilities, NERC developed the Supply Chain Standards. These standards will require responsible entities to take additional actions to address cyber security risks associated with the supply chain for BES Cyber Systems.

Consistent with the risk-based approach of the CIP Reliability Standards, and as discussed more fully below, the Supply Chain Standards are applicable only to certain categories of assets. As discussed in subsequent sections of this report, revisions to the Supply Chain Standards may be necessary to help ensure that the standards adequately address supply chain risks related to certain assets that are not within the current scope of the standards.

In addition to the Supply Chain Standards, industry may use other standards and best practices to mitigate potential supply chain risks. Understanding these standards and best practices helps to create a fuller understanding of supply chain risks and the steps that may be taken to help address them in the context of BES reliability.

## Supply Chain Risks

Supply chains for information and communications technology and industrial control systems are long and multidimensional, involving numerous parties in countries across the globe. Multiple entities across the globe may participate in the development, design, manufacturing, and delivery of a single purchased product. Global supply chains can provide the opportunity for substantial benefits to consumers, but at the same time, a vulnerability at any link in the chain could result in risks to the end user.

These risks, like the supply chains themselves, are global, multidimensional, and constantly evolving. As observed by FERC, cyber supply chain risks may stem from insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development processes.[14] Even well-designed products may have malicious components introduced in the supply chain, and it may prove difficult to identify these components before they are deployed.

Over time, NERC and the industry have developed a more sophisticated understanding of the potential impacts these supply chain risks could have on BES reliability:

- In its 2018 Guidance, the NATF highlighted several real-world events that help demonstrate the risk supply chain vulnerabilities could pose to the electric power industry. These events included the installation of malicious software and theft of project files on a SCADA offering, insertion of unauthorized code on a firewall solution that allowed for the execution of remote procedures, and the alleged insertion of a foreign entity "backdoor" into an anti-virus company's security products.[15]
- In its 2018 White Paper, the APPA and NRECA identified the risks posed by the introduction of malicious code in the supply chain and the employees of vendors who have remote access into their systems as two of the most significant supply chain risks facing their member entities.[16]

[14] *Revised Critical Infrastructure Protection Reliability Standards*, 152 FERC ¶ 61,054, at P 62 (2015).
[15] NATF White Paper at 6.
[16] APPA/NRECA White Paper at 2.

- The *EPRI Interim Report*[17] further highlighted that a compromise in a single vendor's supply chain could have widespread impacts where the vendor supplies a substantial portion of a given product market.[18]

A number of standards and best practices have been developed to address supply chain risks in the electric power industry and other industries. These standards and best practices provide a more complete understanding of supply chain risks and the steps entities may take to mitigate them. Additionally, the Supply Chain Standards provide strong protections for certain categories of high-risk BES Cyber Assets. In implementing the Supply Chain Standards, responsible entities should incorporate some of these industry standards and best practices into their Reliability Standard CIP-013 Requirement R1 supply chain risk management plan(s). NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities in selecting which standards and best practices are appropriate.

The Supply Chain Standards, however, do not mandate that entities provide protections for all categories of potentially vulnerable assets. Different categories of assets would present different risks if compromise based on the type of asset and its function. In subsequent sections, this report provides further information on these devices, provides recommendations for the steps entities should take to reduce their exposure to such risks, and, where appropriate, recommends further changes to the Supply Chain Standards to address the risks associated with these specific devices.

## Industry Standards and Best Practices to Address Supply Chain Risks

Supply chain concerns are not unique to the electric power industry. Other industries that are sensitive to such risks have developed standards and best practices to mitigate supply chain risks. These standards and best practices, which are discussed in Chapter 3 of the EPRI Interim Report, may provide considerations for mitigating supply chain risks in the electric power industry context as well.

Relevant standards and best practices include the following:

- **Off-premise Supplier Services:** In the government context, where a supplier performs deployments or services for an entity involving federal information systems that are not on government premises, the Federal Risk and Authorization Management Program (FedRAMP) standards apply.
- **Third-Party Accreditation Processes:** Suppliers that follow standards, such as FedRAMP and quality management and information security management standards published by the International Organization for Standardization, use independent third parties to assess their adherence to the standards.
- **Secure Hardware Delivery:** The Energy Sector Control Systems Working Group of the U.S. Department of Energy (DOE) developed Cybersecurity Procurement Language for Energy Delivery Systems that identified controls for hardware delivery to help reduce the risk of compromise during transport.
- **Provenance:** Provenance is the ability to provide traceability in the supply chain processes and supplier relationships. Several standards and guidelines address provenance, including the National Supply Chain Risk Management Practices for Federal Information Systems (NISTIR 7622) published by the National Institute of Standards and Technology (NIST).

[17] EPRI, *Supply Chain Risk Assessment Report* (July 2018), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/EPRI_Supply_Chain_Risk_Assessment_Final_Report_public.pdf ("EPRI Interim Report").

[18] *See generally* EPRI Interim Report at Chapter 2.

- **Threat Modeling:** Threat modeling is a process employed to ensure that all products have a threat model specific to the current development scope of the product as described in International Electrotechnical Commission standard IEC 62443-4-1.
- **Supply Chain Deficiencies Assessment:** Addressing the controls for identifying and mitigating the risk of assessed vulnerabilities or inherent weaknesses in the supply chain process of certain product or service providers is an important risk management approach as described in NIST SP 800-53. The NATF white paper highlights how such an approach may apply to supply chain risk management for BES cyber systems.[19]
- **External Dependencies Recognition:** One aspect considered by the DOE's Cyber Security Capabilities Maturity Model (C2M2) is considering supply chain as a process of identifying and managing external dependencies. Recognizing dependencies and those that are most critical to operations can improve an entity's ability to highlight and mitigate supply chain risks.
- **Policy for Handling Supplied Products or Services that Do Not Adhere to Procurement Processes:** Entities may use controls to mitigate risks when products or services are supplied that do not adhere to their specific supply chain policies. Such an approach is described by the U.S. Nuclear Regulatory Commission in Appendix B to 10 C.F.R. part 50 in the context of quality assurance. Attachment A of the *NATF Cyber Security Supply Chain Risk Management Guidance* document provides examples of controls used when procuring BES Cyber Assets and services.[20]
- **Unsupported or Open-Sourced Technology Components:** Different processes must be considered to effectively mitigate the risk of legacy or unsupported systems while updating systems or system components. *See* NIST SP 800-53. With respect to open source products, the Open Group[21] has created a set of standards and certification processes titled the "Trusted Technology Provider Standard (O-TTPS) Certification Program" to address supply chain controls for purchasers.
- **Supplier Relationships:** An important aspect of managing suppliers is knowing how to terminate relationships with third parties in a manner that limits the operational impact of losing the product or service. Such considerations are addressed in the Utilities Telecom Council white paper, *Supply Chain Risk Management for Utilities – Roadmap for Implementation.*[22]

While each of these industry standards and best practices can be informative, NERC has identified several best practices as particularly pertinent in addressing the supply chain risks faced by the electric power industry. NERC staff therefore recommends that entities adopt the following practices when developing their supply chain risk management programs:

- **Secure Hardware Delivery:** Many Cyber Assets purchased and deployed on the BES are hardware appliances configured to perform very specific real-time functions; these appliances may possess code that can be manipulated to cause them to potentially affect the reliable operation of the BES. Instituting hardware delivery controls like those described by the DOE Energy Sector Control Systems Working Group may help to reduce the risks if those devices are compromised in transport.
- **Third-Party Accreditation Processes:** Entities should include an independent assessment or third-party accreditation process of their vendors as part of their supply chain risk management strategy as identified in the APPA/NRECA and NATF white papers.[23] NERC will work with stakeholders to develop an accreditation

[19] NATF White Paper at 8–9.
[20] *Id*. at 18.
[21] The Open Group describes itself as a "global consortium that enables the achievement of business objectives through technology standards." The Open Group, https://www.opengroup.org/about-us/who-we-are.
[22] Utilities Telecom Council, Cyber Supply Chain Risk Management for Utilities – Roadmap for Implementation (Apr. 2015), available at https://utc.org/wp- content/uploads/2018/02/SupplyChain2015-2.pdf.
[23] *See* APPA/NRECA White Paper at 16; NATF White Paper at 13.

model for identifying vendors with strong supply chain risk management practices. Such identification would not only help entities increase the level of confidence that vendors providing BES-related products and services are effectively implementing supply chain cyber security controls and measures ~~comply with the proposed Reliability Standards~~ but also- aid compliance with the proposed Reliability Standards~~increase the level of confidence that vendors providing BES-related products and services are effectively implementing supply chain cyber security controls and measures~~. The process(es) for third party accreditation or certification should be developed and submitted to NERC for evaluation. Such process(es) should be implemented within 12 months of the effective date of Reliability Standard CIP-013-1.

- **Threat-Informed Procurement Language:** Entities should tailor their security specifications to the specific risks of their environment. This can be accomplished through threat modeling, which is a process to ensure that all products have a threat model specific to the current development scope of the product. This ensures the risk of procurement of any application or systems is appropriately weighed against the risk of compromise to the overall health of the organization or the BES. For example, if an entity is procuring a new remote access system for its medium impact BES Cyber Systems, the threat model should reflect the impact of the remote access system's effect to the BES, and the procurement language for that purchase should be specified according to its specific risk and system-specific vulnerabilities.
- **Processes to Address Unsupported or Open-Sourced Technology Components:** Where patch sources for systems or components are no longer available, entities should develop a plan to mitigate potential risks posed by these unsupported systems. Entities should also implement controls when purchasing open source technology, including responsibility for ongoing support and patching. NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline on appropriate controls.

**Using Supply Chain Controls to Mitigate Common-Mode Vulnerabilities:** The Supply Chain Standards require entities that possess high and medium impact BES Cyber Systems to develop processes to ensure that supply chain risks are being managed through the procurement process. As a best practice, NERC staff expects entities that have medium or high impact BES Cyber Systems will apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems. Risks of common-mode vulnerabilities can be mitigated if supply chain security practices are applied uniformly across cyber asset types and BES Cyber System impact levels. Further study is needed to determine whether there is any reliability benefit to extending the Supply Chain Standards to low impact BES Cyber Systems.

Additional considerations and guidance for developing robust supply chain risk management programs are provided in the white papers and guidance prepared by the Forums and Associations.

# Reliability Standards to Address Supply Chain Risks

As noted above, NERC developed the Supply Chain Standards to address the risks to reliability posed by supply chain concerns. These standards require that responsible entities afford certain supply chain protections to their higher risk assets. This section summarizes the Supply Chain Standards and how the present applicability of those standards fits in the broader risk-based framework of the CIP Reliability Standards.

## The Framework of the NERC CIP Reliability Standards

The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats. This approach requires BES Cyber S~~s~~ystems or Facilities that could have the highest impact to the grid receive the highest level of protections. In other words, the level of controls required for protecting cyber systems is in proportion to the risk each system presents to reliable operation of the BPS. This approach was used to mitigate the risk of malicious actors targeting specific assets or electric power entities because of their potential impact to the grid.

This risk-based construct requires users, owners, and operators of the BES to identify those cyber systems (referred to as BES Cyber Systems) that could have ~~on~~ an adverse effect on BES reliability if lost, compromised, or misused.[24] Using bright-line criteria, responsible entities must then categorize their BES Cyber Systems as high, medium, or low impact based on the risks they present to the grid if lost, compromised, or misused. Once these BES Cyber Systems are identified and categorized, the CIP Reliability Standards require responsible entities to, among other things, establish plans, protocols, and controls to protect those systems against a cyber or physical attack, train personnel on security matters, report security incidents, and recover from security events. The Supply Chain Standards will require responsible entities to take additional actions to address cyber security risks associated with the supply chain for high and medium impact BES Cyber Systems.

## NERC Supply Chain Standards

The Supply Chain Standards consist of new Reliability Standard CIP-013-1 (Supply Chain Risk Management) and revised Reliability Standards CIP-005-6 (Electronic Security Perimeter(s)) and CIP-010-3 (Configuration Change Management and Vulnerability Assessments). The Supply Chain Standards focus on the following four security objectives: software integrity and authenticity, vendor remote access protections, information system planning, and vendor risk management and procurement controls.

Collectively, the Supply Chain Standard requirements do the following:

- Reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System (CIP-010-3 Requirement R1 Part 1.6 and CIP-013-1 Requirement R1 Part 1.2 address this concern)
- Address vendor remote access-related threats, including the threat of stolen vendor credentials used to access a BES Cyber System without the responsible entity's knowledge as well as the threat that a compromise at a trusted vendor could traverse over an unmonitored connection into a responsible entity's BES Cyber System (CIP-005-6 Requirement R2 Parts 2.4 and 2.5 and CIP-013-1 Requirement R1 Part 1.2 address this concern)
- Address the risk that responsible entities could unintentionally plan to procure and install vulnerable equipment or software within their information systems or could unintentionally fail to anticipate security issues that may arise due to their network architecture or during technology and vendor transitions (CIP-013-1 Requirement R1 Part 1.1 addresses this concern)
- Address the risk that responsible entities could enter into contracts with vendors who pose significant risks to their information systems as well as the risk that products procured by a responsible entity fail to meet minimum security criteria (CIP-013-1 Requirement R1 Parts 1.1 and 1.2 addresses this concern)
- Address the risk that a compromised vendor would not provide adequate notice of security events and vulnerabilities and related incident response to responsible entities with whom that vendor is connected (CIP-013-1 Requirement R1 Parts 1.2.1 and 1.2.2 addresses this concern)

Consistent with the general risk-based framework of the CIP Reliability Standards, the Supply Chain Standards are subject only to defined categories of Cyber Assets and BES Cyber Systems. **Table 1.1** summarizes the applicability of the Supply Chain Standards.

[24] BES Cyber Systems consist of one or more BES Cyber Assets, which the NERC Glossary defines as follows:

> "A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems."

| Table 1.1: Supply Chain Standard Applicability | | | |
|---|---|---|---|
| **Requirement** | **CIP-013-1** | **CIP-005-6 R2.4** | **CIP-010-3 R1.6** |
| High Impact BES Cyber Systems | ✓ | ✓ | ✓ |
| Protected Cyber Asset associated with High Impact BES Cyber Systems | | ✓ | |
| Physical Access Control Systems associated with High Impact BES Cyber Systems | | | |
| EACMSs associated with High Impact BES Cyber Systems | | | |
| Medium Impact BES Cyber Systems[25] | ✓ | ✓ | ✓ |
| Protected Cyber Assets associated with Medium Impact BES Cyber Systems | | ✓ | |
| Physical Access Control Systems associated with Medium Impact BES Cyber Systems | | | |
| EACMSs associated with Medium Impact BES Cyber Systems | | | |
| Low Impact BES Cyber Systems | | | |

The Supply Chain Standards will require responsible entities to provide strong protections against the risks posed by supply chain compromise for those BES Cyber Systems and Protected Cyber Assets that are subject to the standards. As discussed in subsequent sections of this report, applying these protections more broadly would help reduce the supply chain risks inherent to categories of assets not currently subject to the standards.

Subsequent sections of this report address those assets not presently included in the Supply Chain Standards and the risks associated with those assets if compromised in the supply chain. Chapter 2 addresses EACMSs; Chapter 3 addresses PACS; Chapter 4 addresses low impact BES Cyber Systems; and Chapter 5 addresses PCAs. After evaluating each type of asset and the overall risk environment, NERC makes recommendations for further actions to address those risks.

[25] Reliability Standard CIP-005-6 Requirement R2 Part 2.4 and Reliability Standard CIP-010-3 Requirement R1 Part 1.6 are applicable to "Medium Impact BES Cyber Systems with External Routable Connectivity" and their associated PCA.

# Chapter 2: Electronic Access Control or Monitoring Systems

## Overview

This chapter addresses reliability risks associated with the supply chain for EACMSs, which are not currently subject to the Supply Chain Standards.

EACMSs are defined in the *NERC Glossary of Terms* as follows:

> ***Electronic Access Control or Monitoring Systems (EACMSs)***: "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s)[26] or BES Cyber Systems. This includes Intermediate Systems."

The components that make up EACMSs are typically used to control access to, secure, and monitor critical systems on the BES, such as EMS/SCADA and microprocessor-based relays.

Examples of EACMSs include Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, active directory servers, and certificate authorities), security event monitoring systems, and intrusion detection systems.[27] EACMS components include firewalls, routers, layer three switches, intrusion-detection systems, log monitors, and access control systems.

As discussed in this chapter, the CIP Reliability Standards currently contain protections for EACMSs. These protections, however, do not extend to risks specific to the supply chain. Because certain EACMSs components could have a real-time impact on the reliability of the BES if compromised, misused, or rendered unavailable, and consistent with FERC's Order No. 850 directive,[28] NERC staff recommends revising the Supply Chain Standards to address EACMSs. Specifically, NERC staff recommends revising the standard to include those systems that provide electronic access control (excluding monitoring and logging) to high and medium impact BES Cyber Systems.

In the interim, NERC staff expects that entities will identify and assess supply chain vulnerabilities when procuring and configuring various cyber asset types associated with EACMSs that provide electronic access (excluding monitoring and logging) to high and medium impact BES Cyber Systems. That is, an entity should perform a comprehensive CIP-013-1 Requirement 1 Part R1.1 risk identification and assessment process to consider the potential impact of EACMSs within the entity's operating environment.

## Current CIP Reliability Standard Protections for EACMSs

NERC has existing Reliability Standards that are applicable to EACMSs:

- Reliability Standard CIP-003-6 requires responsible entities to have policies that address cyber security for BES Cyber Systems, including EACMSs for high and medium impact BES Cyber Systems and electronic access controls for low impact BES Cyber Systems.
- Reliability Standard CIP-004-6 requires responsible entities to implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities for those individuals that have access to high and medium impact BES Cyber Systems and associated EACMSs. It also requires responsible entities to implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to high and medium impact BES Cyber Systems and associated EACMSs. It further requires entities to implement one or more access management program(s)

[26] The NERC Glossary defines an Electronic Security Perimeter (ESP) as "[t]he logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol."
[27] *See* Background, Reliability Standard CIP-002-5.
[28] Order No. 850 at P 30.

and access revocation program(s) applicable to high and medium impact BES Cyber Systems and associated EACMSs.

- Reliability Standard CIP-006-6 requires responsible entities to implement one or more documented physical security plan(s) and documented visitor control program(s) for high and medium impact BES Cyber Systems and associated EACMSs.
- Reliability Standard CIP-007-6 requires responsible entities to implement one or more documented processes(s) that address enabling and disabling ports and services for high and medium impact BES Cyber Systems and associated EACMSs. It also requires entities to implement one or more documented process(es) that address patch management and malicious code prevention applicable to high and medium impact BES Cyber Systems and associated EACMSs. It further requires entities to implement one or more documented process(es) that address security event monitoring and logging and system access controls applicable to high and medium impact BES Cyber Systems and associated EACMSs.
- Reliability Standard CIP-009-6 requires responsible entities to implement one or more documented recovery plan(s) for high and medium impact BES Cyber Systems and associated EACMSs. It also requires those entities to test and maintain the recovery plan(s).
- Reliability Standard CIP-010-2 requires responsible entities to implement one or more documented processes(s) that address configuration change management and configuration monitoring for high and medium impact BES Cyber Systems and associated EACMSs. It also requires responsible entities to perform vulnerability assessments applicable to high and medium impact BES Cyber Systems and associated EACMSs.
- Reliability Standard CIP-011-2 requires responsible entities to implement one or more documented information protection program(s) and BES Cyber Asset reuse and disposal process(es) for high and medium impact BES Cyber System and associated EACMSs.

These requirements work together to form a cohesive security protection for deployed EACMSs; however, they do not address the concerns specific to the supply chain discussed below.

## Potential BES Risks Associated with EACMSs due to Supply Chain Concerns

EACMSs are potentially vulnerable to risks from the supply chain. If compromised, misused, or rendered unavailable, EACMS components could have a real-time impact on the reliability of the BES. The risks posed by supply chain vulnerabilities depend in large part on the specific configuration of the EACMSs, where the EACMS is deployed (i.e., at low, medium, or high impact BES Cyber System), and the extent to which certain compensating measures are employed.

EACMSs can consist of systems that perform electronic access control and systems that perform monitoring and logging functions. The reliability risks associated with compromise of electronic access control systems are higher than those associated with monitoring and logging functions.

If a component of an electronic access control EACMSs were to be compromised in the supply chain, such as through the introduction of an unauthorized “backdoor,” a malicious actor could access (or bar authorized users from accessing) systems that directly affect the operation of the BES. If the compromised EACMS controls electronic access to a medium or high impact BES Cyber System, this compromise could negatively impact the reliability of the BES.

If a component of a monitoring EACMS was compromised in the supply chain, such as through the introduction of malicious code, it could impact the ability of the owner to quickly detect, alert to, and respond to a cyber attack. It can also result in real-time access alarms being masked from those that are actively assessing reliability. If a component of a logging EACMS was compromised, it could hinder the ability to perform forensic analysis after active or attempted attacks.

Where EACMSs are configured on a single platform, the risk to all services, including access control, monitoring, and logging, share a single higher risk level if the management plane[29] of the single device is compromised or misused. This is because such devices control access to critical systems from a single point. Services required for access, authentication, monitoring, logging, detection, and alerting could be altered or misconfigured, blinding operators and security personnel to potential unauthorized access and introduction of malicious code to BES Cyber Systems within an ESP.

The risks posed by vendor-initiated remote access sessions, whether through interactive remote access or system-to-system remote access, also represent a significant vector for attack into the associated BES Cyber System through the EACMS.

In evaluating the risks posed by supply chain compromise of EACMSs, NERC staff considered that half of the market share of substation networking equipment is held by only two vendors, one of which has a 55 percent world-wide enterprise network market share in the corporate environment of many industries, including the electric power industry.[30] If a major vendor unknowingly supplied compromised networking equipment, and the compromise was then exploited to allow access to EACMSs controlling electronic access to medium or high impact BES Cyber Systems, the compromise could have widespread negative impacts on reliability.

The potential risks of supply chain compromise described above can be mitigated in part by technical controls, some of which are addressed in the CIP Reliability Standards, while others could be addressed in an entity's policies and procedures. For example, strict authorization and authentication, up to and including multi-factor authentication, can be used to limit the risk posed by local or remote access to the management services of an EACMS by owner or vendor personnel. Other technical controls that could be put in place to secure access and communications include the following: implementing strong password policies; implementing role-based access control; using authentication, authorization, and accounting services; implementing access control lists; encrypting remote access sessions; and using separate secured virtual local area networks for data and management traffic. Testing, verification, and validation of the architecture, configuration, and management access of EACMSs can also help ensure that EACMSs are implemented as designed, meet the expected security controls objectives, and protect BES Cyber Systems within a defined ESP.

While the technical controls mentioned above can provide some protections against certain compromises introduced in the supply chain, they do not address all potential risks. Given the potential adverse impacts that could be caused by a compromised EACMS, it is important to identify and assess supply chain vulnerabilities when procuring and configuring these systems.

## Recommended Actions to Address the Risks

Noting that "the vulnerabilities associated with EACMS are well understood and appropriate for mitigation," FERC directed NERC in Order No. 850 to revise the Supply Chain Standards to include EACMSs.[31]

Upon evaluation of the supply chain-related risks associated with EACMSs, particularly those posed by compromise of electronic access functions, NERC staff recommends that the Supply Chain Standards be modified to include EACMSs that perform electronic access control for high and medium BES Cyber Systems.

Consistent with the risk-based framework of the CIP Reliability Standards, any future revision to the Supply Chain Standards should account for the fact that EACMSs present different risks based on the functions that they perform.

[29] "Management plane" refers to the part of the system that configures, monitors, and provides management, monitoring, and configuration services to all layers of the system.
[30] EPRI Interim Report, at Chapter 2.
[31] Order No. 850 at P 30.

As described above, the BES Cyber Systems that perform electronic access control would, if compromised, present a higher risk to reliability than a compromise of monitoring or logging systems. This is because these access control systems serve as "gatekeepers" to critical systems. Work is currently underway on Project 2016-02 Modifications to CIP Standards[32] to develop new defined terms that separate out EACMS functions so that appropriate controls can be placed around appropriate risks.

In the interim, NERC staff expects that entities will identify and assess supply chain vulnerabilities when procuring and configuring various cyber asset types associated with EACMSs. Various risk assessment techniques are provided in the APPA/NRECA and NATF white papers. For example, entities should perform a comprehensive risk identification and assessment process under Reliability Standard CIP-013-1 Requirement R1.1 that would, at a minimum, consider the following EACMS factors within the entity's operating environment:[33]

- Identify the components that comprise the EACMSs (i.e., specific cyber asset types)
- Identify the vendor(s) for each EACMS device type
- Identify the functions each EACMS device type performs to protect reliability (i.e., firewall, router, switch, etc.)
- Identify and prioritize: the risks presented by each EACMS device type if compromised (e.g., a compromised firewall could allow unauthorized or malicious traffic[34]); and informed potential mitigating circumstances (e.g., logging systems are primarily used for after-the-fact analysis rather than real-time protection)
- Assess the identified risks posed by each device type
- Develop potential strategies or recommendations to address and mitigate each identified risk
- Include recommendations to address EACMS risks in the process(es) used to procure BES Cyber Systems that would address identified risks specific to CIP-013-1 Requirement R1 Parts R1.2.1 through R1.2.6, as applicable, and identify existing or planned vendor mitigation strategies or procedures that address each identified risk as follows:
  - Specific to CIP-013-1 Requirement R1 Parts R1.2.3 and R1.2.6, include recommendations relative to coordinated controls between the entity and applicable vendors associated with CIP-005-6 (Parts 2.4 and 2.5) for managing active vendor remote access sessions to and/or through EACMS cyber asset types
  - Specific to CIP-013-1 Requirement R1 Part R1.2.5, include recommendations specific to planned methods associated with CIP-010-3 (Part 1.6) for verifying the identity of software sources and integrity of software obtained from such sources prior to application to EACMS cyber asset types
  - Specific to CIP-013-1 Requirement R1 Part R1.2.6, include recommendations for controls specific to identified risks associated with compromised vendor-initiated remote access sessions

Reliability Standard CIP-013-1 Requirement 1 Part 1.2.5 addresses verifying the integrity and authenticity of software installed on particular assets. This verification helps to ensure that the software installed on high and medium BES Cyber Systems is not modified prior to installation without awareness of the software supplier and is not a counterfeit piece of software.

In the EACMS context, this software enables controls and monitoring. This highlights the importance of verification, especially for the "gatekeeping" monitoring assets. When the Supply Chain Standards are modified as recommended,

[32] Project 2016-02 Modifications to CIP Standards, http://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx.

[33] This list is provided as an example of considerations for the CIP-013-1 Requirement R1.1 risk identification and assessment process, but it should not be considered an exhaustive or prescriptive list of all the variables that should be considered by each entity for EACMS within its unique operating environment.

[34] *See, e.g.*, EPRI Interim Report at 4-4.

the integrity and authenticity of the software installed on the particular assets that make up the system for monitoring and controlling would be covered by Reliability Standard CIP-013 Requirement 1 Part 1.2.5. This process would, in turn, support the verification required under Reliability Standard CIP-010-3, Requirement 1 Part 1.6. By verifying the integrity and authenticity of their EACMS software, entities can reduce the risk that software installed on the BES Cyber Systems (not just EACMSs, but all BES Cyber Systems) could be modified prior to installation without awareness of the software supplier or be a counterfeit piece of software.

# Chapter 3: Physical Access Control Systems

## Overview

This chapter addresses reliability risks associated with the supply chain for PACSs, which are not currently subject to the Supply Chain Standards.

PACSs are defined in the NERC *Glossary of Terms* as follows:

> ***Physical Access Control Systems (PACSs)***: "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s),[35] exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers."

The systems that make up PACSs are often used to control and monitor physical access to Facilities and systems on the BES where BES Cyber Systems reside. These include physical intrusion-detection systems, log monitors, and systems to control physical access. Examples of PACSs cyber asset types include authentication servers, card systems, and badge control systems.[36]

As discussed in this chapter, the CIP Reliability Standards currently contain protections for PACSs. These protections, however, do not extend to supply chain risk management issues. To address these risks, NERC staff recommends revising the Supply Chain Standards to address those systems that provide physical access control, excluding alerting and logging. In the interim, NERC staff expects that entities will identify and assess supply chain vulnerabilities when procuring and configuring various cyber asset types associated with PACSs. That is, an entity should perform a comprehensive Reliability Standard CIP-013-1 Requirement 1 Part R1.1 risk identification and assessment process to consider the potential impact of PACSs within the entity's operating environment.

## Current CIP Protections for PACSs

NERC has existing Reliability Standards that are applicable to PACSs listed as follows:

- Reliability Standard CIP-003-6 requires responsible entities to have policies that address physical security for BES Cyber Systems, including PACSs for high and medium impact BES Cyber Assets and physical security controls for low impact BES Cyber Systems.
- Reliability Standard CIP-004-6 requires responsible entities to implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities for those individuals that have access to high and medium impact BES Cyber Systems and associated PACSs. It also requires entities to implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to high and medium impact BES Cyber Systems and associated PACSs. It further requires entities to implement one or more access management program(s) and access revocation program(s) applicable to high and medium impact BES Cyber Systems and associated PACSs.
- Reliability Standard CIP-006-6 requires responsible entities to implement one or more documented physical security plan(s) and documented visitor control program(s) for high and medium impact BES Cyber Systems and associated PACSs.
- Reliability Standard CIP-007-6 requires responsible entities to implement one or more documented processes(s) that address enabling and disabling ports and services for high and medium impact BES Cyber

[35] A PSP is defined in the NERC Glossary as "[t]he physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled."
[36] *See* Background, Reliability Standard CIP-002-5.

Systems and associated PACSs. It also requires entities to implement one or more documented process(es) that address patch management and malicious code prevention applicable to high and medium impact BES Cyber Systems and associated PACSs. It further requires entities to implement one or more documented process(es) that address security event monitoring and logging and system access controls applicable to high and medium impact BES Cyber Systems and associated PACSs.

- Reliability Standard CIP-009-6 requires responsible entities to implement one or more documented recovery plan(s) for high and medium impact BES Cyber Systems and associated PACSs. It also requires those entities to test and maintain the recovery plan(s).
- Reliability Standard CIP-010-2 requires responsible entities to implement one or more documented processes(s) that address configuration change management for high and medium impact BES Cyber Systems and associated PACSs. It also requires entities to perform vulnerability assessments applicable to high and medium impact BES Cyber Systems and associated PACSs.
- Reliability Standard CIP-011-2 requires responsible entities to implement one or more documented information protection program(s) and BES Cyber Asset reuse and disposal process(es) for high and medium impact BES Cyber Systems and associated PACSs.

These requirements work together to form a cohesive security protection for deployed PACSs; however, supply chain concerns still exist and are further discussed in this chapter.

# Potential BES Risks Associated with PACSs Due to Supply Chain Concerns

PACSs are potentially vulnerable to risks from the supply chain. If compromised, misused, or rendered unavailable, PACS components could have a real-time impact on the reliability of the BES. The risks posed by supply chain vulnerabilities depend in large part on the specific configuration of the PACS, where the PACS is deployed (i.e., at low, medium, or high impact BES Cyber System), and the extent to which certain compensating measures are employed.

Depending on specific configurations, PACSs could have a real-time impact on the reliability of the BES if compromised, misused, or rendered unavailable. Given this potential impact, it is important to consider supply chain vulnerabilities when procuring and configuring these systems.

A number of methods and systems may be used to control, monitor, and log physical access to BES Cyber Systems. These methods and systems are typically supplied at least in part by third parties and are thus vulnerable to compromises introduced in the supply chain.

Methods of physical access control include the following:

- **Card Key:** A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- **Special Locks:** These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
- **Security Personnel:** Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- **Other Authentication Devices:** Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter (PSP).

- Methods to monitor physical access include the following:
  - **Alarm Systems:** Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
  - **Video Recording:** Electronic capture of video images of sufficient quality to monitor activity at or near PSPs and/or physical security access points.
  - **Human Observation of Access Points:** Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include the following:

- **Computerized Logging:** Electronic logs produced by the responsible entity's selected access control and alerting method.
- **Video Recording:** Electronic capture of video images of sufficient quality to determine identity.
- **Manual Logging:** A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

Similar to EACMSs, the PACS cyber systems that perform physical access control present a higher risk than monitoring and logging systems. A compromise of PACs could allow access to systems that directly affect the operation of the BES, potentially allowing a threat source to negatively impact the BES reliability. Examples of scenarios applicable to compromised PACS components (such as those described above) include, but are not limited to, the following:

- A combined cyber/physical attack on one or more high impact BES Cyber Systems and their host Facilities, where external control of previously compromised PACS elements could allow external threat actors to obtain undetected physical access to Control Centers and other Facilities that control or operate significant portions of the grid. Once inside the PSP, threat actors could detain, subvert, or eliminate the system operators and take physical control of the BES Cyber Systems.
- Misuse, degradation, or destruction of PACS access control components could also allow internal threat actors to take adverse actions on BES Cyber Systems without detection. Such a scenario may precede a physical attack or support a subsequent cyber attack.

While not a specific supply chain risk, there is also a high potential for insider collusion with external threat actors to ensure PACS supply chain compromises are activated prior to a physical attack.

Compromise of the cyber systems that perform monitoring, while not presenting as high of a risk, could impact the ability to quickly analyze an attack and may mask real-time alarms for access from those that are actively assessing reliability. Compromised PACS monitoring systems may also eliminate the entity's ability to detect illicit access to Facilities and their associated BES Cyber Systems. A physical or cyber attack may be preceded by loss of capability to monitor for unauthorized access and to issue alarms or alerts to monitoring personnel, which may lengthen response times and allow threat actors to succeed in their attacks.

Compromise of logging systems would present a much smaller risk as these systems are used primarily to perform forensic analysis after active and potential attacks. Compromised PACS logging systems, however, could prevent accurate forensic analysis and potentially hamper recovery or restoration efforts.

The potential risks of supply chain compromise described above can be mitigated in part by controls, some of which are addressed in the CIP Reliability Standards while others can be addressed in entity policies and procedures. For example, strict operational or procedural controls can be used to limit the risk posed by unauthorized physical access

to BES Cyber Systems. Other controls that could be put in place to restrict access include implementing a completely enclosed "six-wall" boundary and implementing two or more different and complementary physical access controls. Testing, verification, and validation of the architecture, configuration, and management access of PACSs can also help ensure that PACSs are implemented as designed, meet the expected security controls objectives, and protect BES Cyber Systems within a defined PSP.

In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access.

However, given the potential adverse impacts that could be caused by compromised PACSs, particularly compromised access control systems, it is important to identify and assess supply chain vulnerabilities when procuring and configuring these systems.

## Recommended Actions to Address the Risks

Upon evaluation of the supply chain-related risks associated with PACSs, particularly those that control physical access, NERC staff recommends that the Supply Chain Standards be modified to include PACSs that perform physical access controls for high and medium BES Cyber Systems.

Consistent with the risk-based framework of the CIP Reliability Standards, any future revision(s) to the Supply Chain Standards should account for the fact that PACSs present different risks based on the functions that they perform. As described above, the cyber systems that perform physical access control would, if compromised, present a higher risk to reliability than a compromise of alerting and logging systems.

In the interim, NERC staff expects that entities will identify and assess supply chain vulnerabilities when procuring and configuring various cyber asset types associated with PACSs. Various risk assessment techniques are provided in the APPA/NRECA and NATF White Papers. For example, a comprehensive risk identification and assessment process under Reliability Standard CIP-013-1 Requirement R1.1 would, at a minimum, consider the following PACSs factors within the entity's operating environment:[37]

- Identify the components that comprise the PACSs (i.e., specific cyber asset types), including, but not limited to, the following:
  - Servers
  - Workstations
  - Cameras and other surveillance equipment
  - Access control cyber asset components
  - Monitoring components
  - Logging components
- Identify the vendor(s) for each PACS device type
- Identify the functions each PACS device type performs to protect reliability (e.g., authorizing and granting access, detection, response, monitoring, logging, etc.)

[37] This list is provided as an example of considerations for the CIP-013-1 Requirement R1.1 risk identification and assessment process, but it should not be considered an exhaustive or prescriptive list of all the variables that should be considered by each entity relative to supply chain risk management risks associated with PACS cyber asset types within its unique operating environment.

- Identify and prioritize the risks presented by each PACS device type if compromised (i.e., a compromised access authorization system could allow unauthorized or malicious access)
- Identify potential mitigating circumstances (i.e., logging systems are primarily used for after-the-fact analysis rather than real-time protection)
- Assess the identified risks posed by each device type
- Develop potential strategies and/or recommendations to address and mitigate each identified risk
- Include recommendations to address PACS risks the process(es) used to procure BES Cyber Systems that would address identified risks specific to CIP-013-1 Requirement R1 Parts R1.2.1 through R1.2.6, as applicable, and identify existing or planned vendor mitigation strategies or procedures that address each identified risk:
  - Specific to CIP-013-1 Requirement R1 Parts R1.2.1, R1.2.2, and R1.2.4, entities may include physical security mitigation plans to minimize threats associated with such notifications and disclosures (e.g., increase guard force personnel to provide manual physical access controls at PSP Entry Points until such identified vulnerabilities are addressed)
  - Specific to CIP-013-1 Requirement R1 Parts R1.2.3 and R1.2.6, integrate recommendations relative to coordinated controls between the entity and applicable vendors for managing physical access and active vendor remote access sessions to and/or through PACS cyber asset types
  - Specific to CIP-013-1 Requirement R1 Part R1.2.5, integrate recommendations specific to planned methods associated with CIP-010-3 (Part 1.6) for verifying the identity of software sources and integrity of software obtained from such sources prior to application to PACS cyber asset types
  - Specific to CIP-013-1 Requirement R1 Part R1.2.6, integrate recommendations for controls specific to identified risks associated with compromised vendor-initiated remote access sessions

# Chapter 4: Low Impact BES Cyber Systems

## Overview

Under the CIP-002 standard, responsible entities are required to categorize their BES Cyber Systems as either high, medium, or low impact using the bright-line impact rating criteria (IRC) outlined in Attachment 1 to the standard, as follows:

- Section 1 identifies the IRC for high impact BES Cyber Systems. The IRC is limited to BES Cyber Systems associated with four categories of Control Centers (*see* IRC 1.1–1.4).
- Section 2 identifies medium impact BES Cyber Systems associated with Control Centers, generation and transmission Facilities as well as specified remedial action and load shedding schemes (*see* IRC 2.1–2.13).
- Section 3 identifies BES Cyber Systems located at all other BES assets that were not previously identified under Sections 1 or 2. These low impact BES Cyber Systems are associated with smaller BES Facilities, such as Control Centers, generation and transmission Facilities, systems and Facilities critical to system restoration, specified transmission protection systems, including certain system protection and restoration systems owned by Distribution Providers (*see* IRC 3.1–3.6).

The Supply Chain Standards are applicable only to high and medium impact BES Cyber Systems.

In 2016, registered entities were requested to report the number of BES assets (e.g., Control Center, backup Control Center, substation, generation plant, etc.) identified in CIP-002-5.1 Requirement R1, Attachment 1 with high, medium, and low impact BES Cyber Systems as of July 1, 2016. Based on the results, NERC determined that approximately 21 percent of NERC registered entities own high or medium impact BES Cyber Systems; the remainder own only low impact BES Cyber Systems. It is important to note, however, that these survey results do not represent the percentage of assets containing low impact BES Cyber Systems. Many of the 21 percent of registered entities that own and/or operate high and medium impact BES Cyber Systems also own and operate a significant number of low impact BES Cyber Systems. Thus, additional data is needed to gauge the percentage of assets containing low impact BES Cyber Systems that are owned or operated by registered entities that also own medium and high impact BES Cyber Systems. Further study will help assess the residual risk to BES reliability associated with entities that own only low impact BES Cyber Systems.

NERC staff recommends further study of this issue as discussed below to determine whether the inclusion of low impact BES Cyber Systems with External Routable Connectivity should be considered while taking into account the number and nature of such low impact BES Cyber Systems, the benefits of including such systems in the Supply Chain Standards, and the associated costs of extending CIP-013 to cover these systems. While this work is underway, NERC staff recommends that the CIPC Supply Chain Working Group develop a guideline to assist entities in applying supply chain risk management plans to low impact BES Cyber Systems.

## Supply Chain Risks Associated with Low Impact BES Cyber Systems

Low impact BES Cyber Systems are generally comprised of the same types of cyber assets as those in high and medium impact BES Cyber Systems and are therefore subject to similar supply chain risks, but individually present a lower risk to BES reliability if they are compromised. For example, these supply chain risks would include those posed by the introduction of malicious code in the supply chain and the employees of vendors who have remote access into their systems. These two risks have been cited by NRECA and APPA as two of the most significant supply chain risks facing their member entities.[38]

[38] APPA/NRECA white paper at 2.

The applicability of the Supply Chain Standards is consistent with the overall framework of the CIP Reliability Standards discussed above, which is to focus entity attention and resources on those assets that could pose the greatest risks to reliability if they were to be compromised. Low impact BES Cyber Systems are typically associated with isolated, smaller Facilities that are not currently subject to most[39] of the CIP Reliability Standards. Although compromise of an individual low impact BES Cyber System would, by definition, not pose a risk to reliability, the *EPRI Interim Report*[40] highlighted the potential negative impacts on reliability if numerous low impact BES Cyber Systems were compromised. This could happen if a major vendor with sizeable market share unintentionally supplied a compromised product to a sizeable percentage of the industry, and a malicious actor then exploited the single configuration-based vulnerability across a number of devices. Viruses, worms, and malware programs target "common mode vulnerabilities" in this manner.

To better understand this potential risk, EPRI conducted a market data analysis. This analysis consisted of assessing the product/manufacturer types used on the BES for SCADA/control systems, network and telecommunications, and operating systems. While this analysis does not break out the percentages of vendors supplying only low impact BES Cyber Systems, the information is useful as a general representation of the current state of the market. EPRI's analysis showed that two vendors, when combined, have half of the market share of substation networking equipment. It also showed the dominance of the Windows operating system in deployed systems. A further look at the data showed that a significant number of systems were running outdated (unsupported) operating systems and/or open operating systems. Also, two vendors, when combined, hold 82 percent of the existing deployment of energy management systems. By contrast, EPRI determined that no single vendor in the market for remote terminal units exceeded 20 percent market share.[41]

The risk to reliability posed by the mass exploit of a "common mode vulnerability" introduced in the supply chain for low impact BES Cyber Systems may be mitigated by several factors. First, while many CIP Reliability Standards are not applicable to low impact BES Cyber Systems, applying basic cyber hygiene practices could limit the reach and impact of such an event. Examples of such practices include application whitelisting, patching, minimizing domain or local administrative privileges, and disabling local administrative accounts where they are unnecessary. Second, the Supply Chain Standards are expected to have a positive impact on the overall market for electric industry goods and services, which would ultimately reduce the supply chain risks associated with low impact BES Cyber Systems. As noted in the APPA/NRECA White Paper, smaller entities that own only low impact BES Cyber Systems often purchase from the same, well-established vendors that larger entities with higher risk assets use. As larger entities with medium and high impact BES Cyber Assets demand certain supply chain practices from vendors, vendors may choose to apply those supply chain practices to all of their products sold to the electric power industry.[42] The Supply Chain Standards would therefore provide protections to low impact BES Cyber Assets even though the standards do not specifically cover them.

There is a second potential risk associated with low impact BES Cyber Systems, particularly those owned by an entity that also owns high or medium BES Cyber Systems. The risk is that a malicious actor could target the supply chain for a low impact BES Cyber System and, assuming no other controls were in place, exploit that vulnerability to attack other systems owned by the same entity, including high and medium BES Cyber Systems at larger and more critical BES Facilities including Control Centers, generation plants, and transmission Facilities.

[39] Effective January 1, 2020, Reliability Standard CIP-003-7 will be applicable to low impact BES Cyber Systems; Requirements R1.2 and R2 will require certain programmatic, physical, and electronic access protections.

[40] EPRI, *Supply Chain Risk Assessment Report* (July 2018), https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/EPRI_Supply_Chain_Risk_Assessment_Final_Report_public.pdf ("EPRI Interim Report").

[41] For more information on the specific market assessment, refer to the EPRI Interim Report at Chapter 2.

[42] APPA/NRECA white paper at 9-10.

This risk is thought to be mitigated, in large part, by entity supply chain practices. During the standard development process for the Supply Chain Standards, several procurement professionals stated that, other than for specific projects, they typically order cyber asset types without regard to the final destination. For example, orders may be placed for warehouse stock. A comprehensive Reliability Standard CIP-013-1 Requirement R1 supply chain risk management procurement plan that addresses all cyber asset types used by a registered entity in its high and medium impact BES Cyber Systems would also reduce comparable supply chain cyber security risks for assets deployed in low impact BES Cyber Systems.

## Recommended Actions to Address the Risks

As a best practice, NERC staff expects entities that have medium or high impact BES Cyber Systems will voluntarily apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems. This would help reduce the residual risks arising from the supply chain to those systems. Any cyber asset types identified as exclusive to low impact BES Cyber Systems should be evaluated on a case-by-case basis to determine the impact and extent of any supply chain risk management risks, which, if realized, could present a significant threat to the reliability of the BES. For entities that own both low and medium or high impact BES Cyber Systems, applying such practices to all assets regardless of destination would not only reduce the risks to its low impact BES Cyber Systems, but would also help streamline procurement and deployment processes generally.

NERC staff expects entities that own only low impact BES Cyber Systems to develop supply chain risk management programs tailored to their unique risk profiles and priorities. The APPA/NRECA white paper[43] provides considerations for smaller entities in developing such programs. NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities in voluntarily applying supply chain risk management plans to low impact BES Cyber Systems.

For several reasons, NERC staff does not recommend revising the Supply Chain Standards to require protections for all low impact BES Cyber Systems at this time. The risk-based approach used in the CIP Reliability Standards generally, and the Supply Chain Standards specifically, enables responsible entities to prioritize controls for high and medium impact BES Cyber Assets. High and medium impact BES Cyber Systems as categorized in CIP-002 generally describe assets that are critical to interconnected operations, including transmission operations, reliability coordination, and balancing functions. CIP-013-1 provides responsible entities with flexibility for determining appropriate steps for addressing supply chain cyber security risks for low impact BES Cyber Systems. This approach provides an opportunity for industry to take measured steps to address complex supply chain cyber security risks based on their system needs. The reliability benefit of a measured and prioritized approach is that it is more manageable for responsible entities to focus the development of their plans, processes, and controls on the smaller subset of cyber assets that includes the most significant cyber assets.

As described above, the implementation of the Supply Chain Standards is expected to have broader, positive impacts on both vendor and entity supply chain practices. Practices adopted by vendors to satisfy purchasers of assets deployed in high and medium BES Cyber Systems may ultimately be extended to assets deployed in low impact BES Cyber Systems as well. Following implementation of the Supply Chain Standards, NERC may find that there is no incremental reliability benefit associated with extending the Supply Chain Standards to low impact BES Cyber Systems.

Further, extending the Supply Chain Standards to low impact BES Cyber Systems could have unintended effects that may inadvertently increase the risk of common-mode vulnerabilities due to the reduction in diversity of vendors. For example, some vendors may choose not to provide small entities with the services required by the standards, such

[43] APPA/NRECA, *Managing Cyber Supply Chain Risk – Best Practices for Small Entities* (Apr. 25, 2018), https://www.cooperative.com/programs-services/government-relations/regulatory-issues/documents/supply%20chain%20white%20paper%204-25%20final.pdf ("APPA/NRECA White Paper").

as providing notification of vendor identified incidents that pose a cyber risk to the small entity, and owners of low impact BES Cyber Systems may thus have a smaller pool of potential vendors from which to choose. This smaller vendor pool could result in an increased risk that a common mode vulnerability in any one vendor's products or services could affect a substantial number of low impact BES Cyber Systems. Further study is necessary to determine the costs, reliability benefits, and potential unintended consequences of extending the Supply Chain Standards to low impact BES Cyber Systems.

Nevertheless, given the potential risk of a common mode vulnerability affecting numerous low impact BES Cyber Systems, NERC staff recommends further study to determine whether low impact BES Cyber Systems with External Routable Connectivity should be included within the scope of CIP-013. External Routable Connectivity is defined in the NERC Glossary as follows:

> "The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection." Given this connectivity, these low impact BES Cyber Systems may pose a higher risk that could warrant mandatory supply chain protections.

First, NERC staff will propose to the Board a Request for Data or Information under Section 1600 of the NERC Rules of Procedure to obtain more information about the nature and number of BES Cyber Systems currently in use. NERC staff will work with the CIPC Supply Chain Working Group to determine the appropriate scope of the request. NERC staff expects that the request would address, at a minimum, the following considerations:

- The approximate total number of BES Cyber Assets in high/medium impact BES Cyber System(s): Of this number, the approximate number that have External Routable Connectivity
- The approximate total number of BES Cyber Assets in low impact BES Cyber Systems: Of this number, the approximate number that have External Routable Connectivity
- Questions to determine incremental costs and potential benefits to extend CIP-013 to low impact BES Cyber Systems with External Routable Connectivity:
    - The costs and potential benefits for entities that have high/medium impact BES Cyber Systems
    - The costs and potential benefits for entities that have only low impact BES Cyber Systems

Following the collection of the data, NERC staff will provide the results of the data analysis to industry.

Second, NERC staff will monitor the issue through the use of ~~pre-audit~~industry surveys and questionnaires following the implementation of the Supply Chain Standards to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with External Routable Connectivity and to determine if there is consistent application of the criteria in CIP Reliability Standards that differentiate medium impact BES Cyber Systems from low impact. This new information would include actual market and entity practices following implementation of the Supply Chain Standards and the extent to which these practices may help reduce risks to reliability stemming from the supply chains for low impact BES Cyber Systems, including those with External Routable Connectivity. With this information, NERC and its stakeholders may make an informed analysis of whether mandatory requirements for all or a subset of low impact BES Cyber Systems are appropriate while taking into account the costs, expected benefits, and all other relevant considerations. To encourage full and frank industry participation, NERC Staff recommends that these surveys be completed independently of any mandatory compliance monitoring or enforcement process.

# Chapter 5: Protected Cyber Assets

## Overview

This chapter addresses the supply chain risk management risks posed by PCAs, which are currently subject to only a limited subset of the Supply Chain Standards.

PCAs are defined in the NERC Glossary of Terms as follows:

> ***Protected Cyber Assets (PCAs)***: "One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP."

Since there is a wide range of assets that fall under the category of PCAs, it is not possible to clearly define a general risk to the BES in the event they are compromised due to supply chain vulnerabilities. NERC staff recommends that entities, as a best cyber security practice, evaluate each PCA type on a case-by-case basis to identify any specific risks associated with supply chain risk management. This evaluation will allow each entity to determine whether supply chain risk management procurement processes are needed to mitigate the risk to associated BES Cyber Systems. NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities in evaluating their PCAs to determine what, if any, additional supply chain protections are needed. NERC staff will also work with the CIPC Supply Chain Working Group to determine whether additional data should be collected on PCAs, as an extension of the Section 1600 data request to be prepared on low impact BES Cyber Assets.

## Potential BES Risks Associated with PCAs due to Supply Chain Concerns

It is difficult to provide a general assessment of the risks that supply chain-compromised PCAs could present to the BES. By definition, PCAs do not represent an immediate 15-minute adverse impact to the reliability of the BES. PCA types, however, are sometimes identical to those cyber asset types identified as BES Cyber Assets. As a result, supply chain risk management practices should be highly dependent on the specific function of the PCA in question and the exposure risk to the BES Cyber Systems in the same ESP.

Overall PCAs are cyber assets most likely to be typical information technology assets like workstations, servers, printers, scanners, and other peripherals that support the work of operators and staff in the Control Center, data center, or security operations center environment. Based on type and configurations, PCAs could have the same risk profile of BES Cyber Assets associated with a high or medium BES Cyber System. Compounding the risk is that these systems may reside on the same network segments as a BES Cyber System while not being part of the BES Cyber System. Due to the potential interconnectedness of the PCA with the BES Cyber System, a compromise or misuse of the PCA could pivot to the BES Cyber System. The potential risk can be mitigated in part by technical controls, some of which are addressed in the CIP Reliability Standards and others which can be addressed in policies and procedures. For example, implementing access control lists, intrusion prevention systems, and malicious software prevention tools can be used to limit the risk posed by PCAs possibly impacting interconnected BES Cyber Systems.

## Recommended Actions to Address the Risks

As a best practice, NERC staff recommends that entities evaluate each PCA type on a case-by-case basis to identify any specific risks associated with supply chain risk management and to determine whether supply chain risk management procurement processes are needed to mitigate risks to associated BES Cyber Systems. NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities in evaluating their PCAs to determine what, if any, additional supply chain protections are needed. NERC staff will also work with the CIPC Supply Chain Working Group to determine whether additional data should be collected on PCAs, as an extension of the Section 1600 data request to be prepared on low impact BES Cyber Assets.

Entities should seek assurance that hardware or software components for PCAs are authentic and have not been modified prior to provisioning the PCA and when deploying required operational or security updates. Approved configuration management and change management processes should be followed for PCAs. A best practice would be to also include PCAs in a registered entity's baselining program to track and monitor the state of PCAs within their critical infrastructure networks.

Since PCAs are often the same cyber asset type as many common BES Cyber Assets, they may be subject to "common mode vulnerabilities" and represent an attack vector to BES Cyber Systems contained within the same ESP as the PCA. A comprehensive CIP-013-1 Requirement R1 supply chain cyber security risk management plan could be effective to support mitigation of PCA cyber assets obtained under the same supply chain risk management procurement plan as BES Cyber Systems associated with high and medium impact BES Cyber Systems. The specific processes should be made on a case-by-case basis after evaluating the potential risks associated with the supply chain for that device.

NERC staff does not recommend revising the Supply Chain Standards at this time to include PCAs. While PCAs are on the same network as BES Cyber Systems, other controls deployed on the BES Cyber Systems under the CIP-007 and CIP-010 standards would protect the actual assets that could have a 15-minute impact if rendered unavailable, degraded, or misused. Since there is a wide range of assets that fall under the category of PCA, the case-by-case approach described above would provide a flexible and cost effective approach to addressing supply chain risks associated with specific PCAs while avoiding unnecessary regulatory burden.

# Chapter 6: Conclusion

Compromise of certain cyber assets in the supply chain could pose a threat to BES reliability. The Supply Chain Standards require responsible entities that possess high and medium impact BES Cyber Systems develop processes to ensure that supply chain risks are being managed through the procurement process. The Supply Chain Standards will be applied to the higher-risk systems that have the greatest impact to the grid.

NERC staff recommends that the Supply Chain Standards be modified to include certain assets associated with high and medium impact BES Cyber Systems in light of the risks that may be posed by compromise of such devices in the supply chain. In light of the risks posed by compromise of such devices, and to address FERC's Order No. 850 directive, NERC staff recommends revising the Supply Chain Standards to address EACMSs. Specifically, NERC staff recommends revising the standard to include EACMSs that provide electronic access control (excluding monitoring and logging). NERC staff also recommends revising the Supply Chain Standards to include PACSs that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems. In the interim, NERC staff expects that entities will apply supply chain security practices to EACMSs and PACSs to help mitigate supply chain risks associated with these devices.

At this time, NERC staff does not recommend that the Supply Chain Standards be modified to include all low impact BES Cyber Systems. As a best practice, NERC staff expects entities that have medium or high impact BES Cyber Systems will voluntarily apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems to ensure risks are identified and assessed without regard for the ultimate destination of such common cyber assets. Additional consideration may need to be given to processes used by vendors and entities to mitigate supply chain risk to lower impact systems. Risks of common-mode vulnerabilities, as described in Chapter 4, can be mitigated if supply chain security practices are applied uniformly across cyber asset types and BES Cyber System impact levels. Further study is needed, however, to determine whether there is any reliability benefit to extending the Supply Chain Standards to low impact BES Cyber Systems.

NERC staff expects entities that own only low impact BES Cyber Systems will develop supply chain risk management programs tailored to their unique risk profiles and priorities. The APPA/NRECA white paper provides considerations for smaller entities in developing such programs. NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities in voluntarily applying supply chain risk management plans to low impact BES Cyber Systems.

Due to the wide variation in risks associated with PCAs and mitigating controls already in place, NERC staff does not recommend that the Supply Chain Standards be modified to further address PCAs. NERC staff does, however, recommend that entities evaluate the risks on a case-by-case basis and adopt supply chain controls as appropriate to address those risks. NERC staff will work with the CIPC Supply Chain Working Group to develop a guideline to assist entities in evaluating their PCAs to determine what, if any, additional supply chain protections are needed. NERC staff will also work with the CIPC Supply Chain Working Group to determine whether additional data should be collected on PCAs, as an extension of the Section 1600 data request to be prepared on low impact BES Cyber Assets.

## Applying Industry Practices and Guidelines

Chapter 1 identified several noteworthy supply chain risk management techniques that are not required by the CIP Reliability Standards. While these standards address many fundamental elements of effective processes to manage the risk of a supply chain, the following noteworthy approaches, if applied correctly, can reduce residual supply chain risks:

- **Independent Assessment or Third-Party Accreditation Processes:** Entities should verify that standardized processes and measures were achieved to mitigate supplier risks.

- **Secure Hardware Delivery:** Entities should take steps to ensure that hardware and software are protected during physical transport.
- **Threat-Informed Procurement Language:** Entities should tailor their security specifications to the specific risk of their environment.
- **Unsupported or Open-Sourced Technology Component Processes:** Entities should employ processes to mitigate residual risks for unsupported systems and for open source technology.
- **Using Supply Chain Controls to Mitigate Common-Mode Vulnerabilities:** Entities should voluntarily apply similar techniques to manage supply chain risks at lower impact levels.

NERC staff recommends entities include these practices in developing their supply chain risk management programs.

# Going Forward

NERC will work through its existing processes with stakeholders to review NERC staff's recommendations in this report and determine appropriate follow up actions.

The following additional work should be undertaken to evaluate the recommendations included in this report:

- **Section 1600 Data Request:** NERC staff, working with the CIPC Supply Chain Working Group, will develop a Request for Information or Data under Section 1600 of the NERC Rules of Procedure in an expedited manner. The results of this request will inform whether low impact BES Cyber Systems with External Routable Connectivity should be included within the scope of CIP-013.
- **Security Guidelines:** NERC staff, working with the CIPC Supply Chain Working Group, will develop security guidelines to assist entities in managing supply chain risks for EACMSs, PACSs, PCAs and low impact BES Cyber Systems.
- **Practice Guides:** The ERO will develop CMEP practice guides to create clear expectations on the types of questions registered entities may expect regarding their low impact BES Cyber Assets and the supply chain risk management activities afforded to those assets.
- ~~**Pre-Audit**~~**Industry Surveys and Questionnaires to Help Identify and Assess Industry Practices**: Voluntary efforts to obtain risk data ~~in the preliminary stages of Compliance Monitoring and Enforcement Program activities~~ can be used to obtain information about the installed base of systems used on the BES, the procurement language in contracts negotiated with key vendors, and data describing which CIP applicable systems have benefited from procurement language stemming from the Supply Chain Standards. To encourage full and frank industry participation, NERC Staff recommends that these surveys be completed independently of any mandatory compliance monitoring or enforcement process.
- **Targeted Outreach to Vendors that Support the Reliability of the BES:** Various vendors support the secure operations of the BES. Next steps should consider coordinated outreach to vendors that have a high market share of supplied products and services to the BES to ensure that they have awareness to their products' potential impact to reliability and their customers' responsibility to meet the rigor required by the CIP Reliability Standards. It is encouraged that industry work with their vendor points of contacts to ensure that technical and contractual considerations are addressing the standards.
- **Development of Standardized Vendor Data Sheets:** One of the challenges identified during the analysis of information used to prepare this report was the availability of vendor supply chain practices. The CIPC is working to develop a document for vendors about the CIP Reliability Standards. Further consideration should be given to the creation of a standardized method to provide product and supply chain security facts and features regarding vendor capabilities to help mitigate supply chain risks.

- **Third Party Accreditation/Certification Processes**: Process(es) for third party accreditation or certification should be developed and submitted to NERC for evaluation. NERC will work with stakeholders to develop an accreditation model for identifying vendors with strong supply chain risk management practices. Such identification would not only help entities comply with the proposed Reliability Standards but also increase the level of confidence that vendors providing BES-related products and services are effectively implementing supply chain cyber security controls and measures. Such process(es) should be implemented within 12 months of the effective date of Reliability Standard CIP-013-1.
- **Independent Testing of Legacy Applications and Products**: As discussed in NERC's plan to address supply chain risks, partnerships with independent organizations used to test and communicate product vulnerabilities used on the BES will be a key activity going forward. Understanding known vulnerabilities of the installed base will support the industry's effort to become more effective in negotiating contracts and resolving security issues in the procurement of upgraded systems and implementation of greenfield systems.

# Future Considerations

In developing this report, NERC has identified several issues that, while outside the scope of this report, should be considered as part of future evaluations of supply chain risks and the effectiveness of the Supply Chain Standards.

As technologies and attacks have advanced and become more complex, entities are expressing interest in partnering with outside and government security services. These includes services like NERC's Cyber Security Risk Information Sharing Program (CRISP), Cybersecurity for the Operational Technology Environment, and those of external vendors and internal monitoring centers. It may prove difficult to understand and manage any supply chain risks for these systems. However, these providers have visibility into emerging threats and trends that comes through their extensive collections of information. Analysis of this information can then be shared more broadly, improving the overall cyber security posture of the customers and reliability of the BES through early detection of compromise.

Under the current body of CIP Reliability Standards, using these types of security services (that may also include electronic access or monitoring) may bring all Cyber Assets involved into scope as an EACMS. This may discourage or even preclude entities from using these services based on the associated BES Cyber System level requirements of an EACMS. These limitations affect patching, baselines, and other requirements as outlined in the CIP Reliability Standards, and may also be impacted by the Supply Chain Standards. There is great value in correlating security events seen across those networks that could be expanded to include an entity's other non-BES Cyber Assets. This activity could be precluded or discouraged through the administration of the current CIP Reliability Standards.

# Appendix A: Summary of Actions Taken to Support the NERC Board Resolutions on Supply Chain

## Support Effective and Efficient Implementation

The Board requested NERC to commence preparations for implementation of the Supply Chain Standards by using similar methods during the CIP V5 transition and regularly report to the Board on those activities.

To support this action, NERC engaged in several activities. NERC created a Supply Chain Risk Mitigation Program webpage to provide a single source for resources. The CIPC has established an advisory task force to provide input on activities to support standard implementation (e.g., webinars, workshops, and technical conferences) in coordination with NERC and the Regional Entities. Efforts are also underway to document existing risks and develop security guidelines for use by industry in managing known supply chain risks.

NERC and the Regional Entities hosted several small group advisory sessions with registered entities and NERC standards developers to discuss the preparation for and implementation of the Supply Chain Standards. Each session consisted of closed one-on-one discussions between a registered entity's supply chain security experts and ERO Enterprise staff about concerns pertinent to the entity's implementation of the proposed Supply Chain Standards. These sessions resulted in the development of a Frequently Asked Questions document.[44] The document addresses many of the questions and concerns voiced during those sessions.

In addition, NERC and the Regional Entities presented on the Supply Chain Standards and the security concerns regarding supply chain during regional workshops and outreach engagements. These presentations highlighted some of the costs regarding cyber attacks, risks identified in the EPRI Interim Report, and well-known public supply chain compromises. NERC also presented similar presentations to industry and other independent industry groups.

Going forward, NERC is considering additional small group advisory sessions and providing targeted outreach to entities and stakeholders.

In addition to actions taken to support the Board Resolutions, industry is also using existing NERC structures to improve reliability, security, and compliance. For instance, several prequalified organizations have already submitted compliance implementation guidance to support effective implementation of the Supply Chain Standards.

## Cybersecurity Supply Chain Risk Study

The Board requested NERC to study the nature and complexity of cyber security supply chain risks, including those associated with low impact assets not currently subject to the Supply Chain Standards, and develop recommendations for follow-up actions that will best address identified risks. The interim report would be due 12 months after adoption of the resolutions and a follow-up final report would be due 18 months after adoption.

The following activities have occurred to support this action and are listed as follows:

- **Interim Report**
  - NERC contracted the Electric Power Research Institute to prepare an interim report on supply chain risks. The report focuses on the following areas:
    - An assessment of product/manufacturer types used on the BES
    - An analysis and applicability to BES Cyber Assets

[44] Frequently Asked Questions, Supply Chain – Small Group Advisory Sessions: https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/SGAS%20FAQ%2006252018.pdf. (June 28, 2018).

  - An analysis of best practices and standards in other industries to mitigate supply chain risks
  - An analysis of generalized vendor practices and approaches used to mitigate supply chain risks
- NERC staff presented the interim report at the August 2018 Board meeting and posted the report on the Supply Chain Risk Mitigation Program webpage.

- **Final Report**

  This report, *Supply Chain Risks: Final Report and Recommended Actions*, was presented in draft to the Board in February 2019 and will be presented for acceptance to the Board in May 2019.

## Communicate Supply Chain Risks to Industry

The Board requested NERC to communicate supply chain risk developments and risks to industry in connection with this report.

The following activities have occurred to support this action:

- NERC and E-ISAC have used NERC Alerts to communicate supply chain risks to industry.
- E-ISAC included a supply chain risk topic in NERC's Grid Security Exercise (GridEx IV).
- NERC and Regional Entities have included supply chain topics at workshops in 2018.
- CIPC is in the process of developing supply chain security guidelines.

## Forum White Papers

The Board requested that the Forums (NATF and the NAGF) develop (and distribute, as permissible) white papers to address best and leading practices in supply chain management as described in the resolution.

To support this action, the Forums have developed white papers, which are posted on the Supply Chain Risk Mitigation Program webpage.

## Association White Papers

The Board requested that the Associations (NRECA and APPA) develop (and distribute, as permissible) white papers to address best and leading practices in supply chain management, focusing on smaller entities that are not members of the Forums, for the membership of the Associations.

To support this action, the Associations jointly developed a white paper, which is posted on the Supply Chain Risk Mitigation Program webpage.

## Evaluate Supply Chain Standard Effectiveness

The Board requested that NERC, collaborating with NERC technical committees and other experts, develop a plan to evaluate the effectiveness of the Supply Chain Standards, as described in the resolution, and report to the Board.

The plan to evaluate the effectiveness of the Supply Chain Standards will be developed by NERC staff in 2019, with assistance of the CIPC advisory group and Regional Entities.

## Additional Information

NERC's Supply Chain Risk Mitigation Program webpage[45] provides more information on these and other ongoing efforts to support the implementation of the Supply Chain Standards and address ongoing supply chain considerations.

[45] NERC, Supply Chain Risk Mitigation Program: https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

# Appendix B: CIPC Supply Chain Working Group Members

NERC wishes to take this opportunity thanks the following members of the CIPC Supply Chain Working Group and their organizations for their valuable contribution to this report.

**Table B.1: CIPC Supply Chain Working Group**

| Member Name | Company |
|---|---|
| Amelia Anderson | CenterPoint Energy |
| Andy Bochman | IBM |
| Bob Lockhart | Utilities Technology Council |
| Brenda Davis | CPS Energy |
| Brian Bouyea | New York ISO |
| Brian Millard | Tennessee Valley Authority |
| Brian Tooley | Vectren |
| Celia Sieg | New York ISO |
| Chip Wenz | AES Corporation |
| Christopher Keane | Duke Energy |
| Christopher Plensdorf | DTE Energy |
| Christopher Walcutt | Direct Defense |
| Dalini Khemlani | Amazon Web Services |
| Darrell Klimitchek | South Texas Electric Cooperative |
| Darren Hulskotter | CPS Energy |
| David Godfrey | Garland Power & Light Company |
| David Jacoby | Boston Strategies International |
| David Sampson | DTE Energy |
| Donald Hargrove | Oklahoma Gas and Electric Co. |
| James Brown | California ISO |
| James Howard | Lakeland Electric |
| Jeffrey Kimmelman | Network and Security Technologies |
| Jerrod Montoya | Open Access Technology International |
| Jim McNierney | New York ISO |

| Table B.1: CIPC Supply Chain Working Group | |
|---|---|
| **Member Name** | **Company** |
| John Hochevar | American Transmission Company |
| Jose Flores | North American Transmission Forum |
| Joseph Smith | Public Service Enterprise Group |
| Kaitlin Brennan | Edison Electric Institute |
| Kara White | NRG |
| Karl Perman | EnergySec |
| Keith St. Amand | Midwest ISO |
| Ken Keels | North American Transmission Forum |
| Kevin Weber | Entergy |
| Lee Maurer | Oncor Electric Delivery |
| Marc Child | Great River Energy |
| Marina Rohnow | San Diego Gas and Electric |
| Mark Henry | Texas Reliability Entity |
| Matt Anglin | New York ISO |
| Michael Aukerman | Denton Municipal Electric |
| Michael Meason | Western Farmers Electric Cooperative |
| Mike Mertz | PNM Resources |
| Michele Wright | FoxGuard Solutions |
| Michelle Coon | Open Access Technology International |
| Mike Kraft | Basin Electric Power Cooperative |
| Mike Prescher | Black and Veatch |
| Monika Montez | California ISO |
| Nathan Shults | Kiewit Engineering and Design |
| Patricia Ireland | DTE Electric |
| Patricia Meara | Network and Security Technologies |
| Peter Nelson | Network and Security Technologies |
| Pierre Janse van Rensburg | ENMAX Power Corporation |

| Table B.1: CIPC Supply Chain Working Group | |
|---|---|
| **Member Name** | **Company** |
| Reed Thompson | Public Service Enterprise Group |
| Robert Koziy | Open Systems International |
| Ryan Carlson | Proven Compliance Solutions |
| Sarah Stevens | North American Transmission Forum |
| Scott Webb | Network and Security Technologies |
| Sharla Artz | Utilities Technology Council |
| Sheranee Nedd | Public Service Enterprise Group |
| Steen Fjalstad | Midwest Reliability Organization |
| Steve Brain | Dominion Energy |
| Steven Briggs | Tennessee Valley Authority |
| Tony Eddleman | Nebraska Public Power District |