Managing Cyber Supply Chain Risk-Best Practices for Small Entities

April 25, 2018

ACKNOWLEDGMENTS

The American Public Power Association and National Rural Electric Cooperative Association want to acknowledge and thank the firms of Spiegel & McDiarmid and Stinson Leonard Street for their assistance in writing the Supply Chain White Paper. Also, we would like to acknowledge and thank the U.S. Resilience Project for processing the information from the interviews with the sample volunteer utility companies. Finally, we want to express our appreciation for the time and commitment of the sample companies and their contribution to the cyber and supply chain security of their peers.

For questions regarding this paper, please contact:

Jack Cashin
Director of Policy Analysis & Reliability Standards
American Public Power Association
Jcashin@publicpower.org
202-467-2979

Barry Lawson
Senior Director, Regulatory Affairs
Government Relations
National Rural Electric Cooperative Association
Barry.lawson@nreca.coop
703-907-5781

I. EXECUTIVE SUMMARY

In August 2017, the North American Electric Reliability Corporation (NERC) Board of Trustees approved a set of cybersecurity supply chain standards ("supply chain standards") that were developed in response to a directive from the Federal Energy Regulatory Commission (FERC). In conjunction with that action, the NERC Board of Trustees issued a resolution calling on the American Public Power Association (APPA) and the National Rural Electric Cooperative Association (NRECA) (collectively "the Associations") to develop white papers addressing the best and leading cybersecurity supply chain risk management ("supply chain risk management") practices with a focus on small registered entities. APPA and NRECA have collaborated to develop this white paper in response to that resolution.

Supply chain risk management for small registered entities must be understood in the context of the overall risk-based approach of NERC's Critical Infrastructure Protection (CIP) standards, which classify Bulk Electric Systems (BES) Cyber Systems as having low, medium, or high impact on the reliable operation of the BES. NERC's requirements for protecting BES Cyber Systems are commensurate with those systems' risk classification.

Consistent with that risk-based approach, and supported by APPA and NRECA, NERC's supply chain standards appropriately apply to medium and high impact BES Cyber Systems, which is intended to focus industry resources on protecting those systems that pose heightened risk, while not being overly burdensome or diverting resources toward protecting low-impact assets that have less risk to BES reliability. The standards address cybersecurity supply chain risks ("supply chain risks") in a way that sets goals for registered entities, while allowing flexibility in how to achieve those goals. FERC has proposed to approve those standards (with certain directives).

In addition to protecting medium and high impact BES Cyber Systems, NERC's supply chain standards have the potential to indirectly reduce supply chain risk for all BES Cyber Systems. When registered entities implement their processes and procedures to comply with the new supply chain standards for their medium and high impact BES Cyber Systems, they are likely to apply those same or similar processes and procedures more broadly to their procurement and vendor management practices across their organizations. And as larger registered entities with more bargaining power insist that vendors comply with new supply chain risk management practices, those vendors may well adopt those practices across the board benefitting purchasing for all utilities, big and small.

NERC has also undertaken, or is planning to undertake, several activities to support industry's implementation of the supply chain standards, as well as activities beyond the scope of the standards that will further reduce supply chain risk. These activities include the development of implementation guidance, exploring opportunities with product manufacturing standard bodies (e.g., IEEE) to address supply chain risks, and exploring opportunities to assist stakeholders in developing an accreditation model for identifying vendors with strong supply chain risk management practices. If successful, these NERC efforts will help protect all BES Cyber Systems—including low impact—from supply chain risks**.**

This white paper identifies a catalog of practices for supply chain risk management for consideration by small registered entities with low-impact BES Cyber Systems. Each of these

small registered entities with low impact BES Cyber Systems will need to factor in many considerations, such as staffing, resources, and their own unique circumstances in order to determine which of these practices are appropriate and realistic for their use. This catalog of practices reflects the result of extensive interviews of nine APPA and NRECA members. The interviews showed that small registered entities with only low-impact BES Cyber Systems can—and do—implement appropriate supply chain management measures that help mitigate supply chain risk and can be considered best practices commensurate with the low risk that those entities pose to BES reliability. Each of the practices described in Section IV of this white paper are currently being implemented by one or more of the sampled companies, and (except where otherwise noted" each practice is being implemented by one or more of the sample companies that are small registered entities with only low-impact BES Cyber Systems.

The sampled companies are well-aware of supply chain risks. One of the largest risks is that of a malware campaign infecting a product with malicious code while the product is still within the control of the vendor (i.e., before the product is received by the utility). Another significant supply chain risk is from employees of vendors that have remote access to BES Cyber Systems. The interviews identified a number of best practices that may be useful for small registered entities with only low-impact BES Cyber Systems to mitigate those risks.

The supply chain risks that have been identified, and the best practices to address those risks, reflect this particular snapshot in time. Supply chain risk assessment is rapidly evolving, so new risks may emerge and existing risks may be diminished. And as NERC's supply chain standards are implemented, larger entities subject to those standards and their vendors will likely evolve as to how they mitigate supply chain risks, which may result in more best practices for small registered entities to consider using to mitigate their lower-impact supply chain risk.

Recognizing that context, the Associations have summarized the following best practices that are currently in use by one or more of their small members that have only low-impact BES Cyber Systems:

A. Organization

1. Leadership from senior management is an important element of mitigating supply chain risks, regardless of the size of an organization.

2. Improving coordination and cooperation between departments within an organization mitigates supply chain risks.

3. Enterprise-wide cyber risk assessments, including supply chain, help identify the most significant threats to each individual organization.

4. Having processes to identify unusual system activity allows utilities to respond rapidly to cyber events, including those arising from supply chain vulnerabilities.

B. Vendor Selection

1. Using well-known, trusted, and established vendors is a good starting point for reducing supply chain risk.

2. Reducing the number of vendors used by a utility can improve expertise in those vendors' systems and allow for better relationships with those vendors, thus reducing supply chain risk.

3. Standard questionnaires can be a useful tool for vetting vendors to reduce supply chain risk.

4. As these issues mature, standard contract language for vendors may become viable tools for all registered entities, large and small, to mitigate supply chain risk.

5. Third-party accreditation and vendor self-certification would improve the ability of all entities, particularly small registered entities, to select reliable vendors.

C. Vendor Remote Access to Systems

1. Limiting the systems that can be accessed remotely reduces supply chain risk.

2. Restricting vendor remote access to specific service requests reduces supply chain risk.

3. Monitoring vendor remote access can be performed in real-time or by reviewing logs after vendor remote access is completed.

4. Monitoring of remote access points reduces supply chain risk.

D. Software Integrity and Authentication

1. Risk assessments should be conducted as part of the decision to upgrade BES Cyber Systems.

2. New software should be thoroughly tested prior to installation.

E. Software Updates and Patch Management

1. Especially for SCADA systems, patch management contracts help to mitigate supply chain risks; however, this can also be managed by the entity without a vendor contract.

2. Testing patches prior to their implementation mitigates supply chain risk.

3. Confirming patch authenticity prevents the insertion of malicious code while the patch is being transmitted.

In addition, smaller registered entities with low-impact BES Cyber systems have other resources they can look to as additional sources of information that may merit consideration in seeking to mitigate their supply chain risk. Specifically, each of the Associations has programs in place to support their members as they work to improve the cyber and physical security of their organizations, including procurement and supply chain issues. Other resources, prepared for entities within and outside the electric industry, are also available to NERC registered entities that are interested in looking at additional perspectives for addressing supply chain risk.

The Associations believe that the catalog of supply chain risk management practices identified in this white paper, along with the additional resources available to Association members, will provide a useful resource for small registered entities with low-impact BES Cyber Systems to further strengthen their existing supply chain risk management practices.

II. INTRODUCTION

In July 2016, FERC directed 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 bulk electric system operations."[1] NERC convened a standard drafting team to address the directive, and in August 2017 the NERC Board of Trustees approved the resulting standards, which were then submitted to FERC for approval. In January 2018, FERC issued a Notice of Proposed Rulemaking proposing to approve NERC's supply chain standards and issue directives for further modification.[2]

In conjunction with approving the supply chain standards, the NERC Board of Trustees issued a resolution calling on the Associations to develop white papers addressing "best and leading practices in supply chain management, including procurement, specifications, vendor requirements and existing equipment management" with a focus on small registered entities.[3]

The Associations have collaborated to develop this white paper in response to the resolution, with an emphasis on best practices for small registered entities with low-impact BES Cyber Systems.[4] Prior to the NERC Board of Trustees' resolution, the Associations and their members had already begun efforts to identify and develop risk mitigation strategies related to supply chain risk management, in recognition of the growing risks posed by global supply chains. The Associations welcomed the NERC Board of Trustees' request, which has prompted the

---

[1] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 81 Fed. Reg. 49,878 (July 29, 2016), 156 FERC ¶ 61,050 (2016).

[2] *Supply Chain Risk Management Standards*, 162 FERC ¶ 61,044 (2018).

[3] NERC Board of Trustee's August 11, 2017 Resolution. The same resolution called on the North American Transmission Forum and the North American Generation Forum to develop best practices white papers for their members.

[4] A BES Cyber System is a group of programmable electronic devices that perform a reliability task for a functional entity that, if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, adversely impact the reliable operation of the Bulk Electric System. *See* NERC, Glossary of Terms Used in NERC Reliability Standards (Jan. 31, 2018), http://www.nerc.com/files/glossary_of_terms.pdf. The Bulk Electric System is defined, subject to several inclusions and exclusions, as transmission elements operated at 100 kV or higher and generation resources larger than 20 MVA connected at 100 kV or higher. *See North American Electric Reliability Corporation*, Order Approving Revised Definition, 146 FERC ¶ 61,199 (2014).

Associations to further intensify their ongoing efforts and has helped to coalesce efforts of their individual members.

The Associations intend that this white paper will consolidate best practices and provide a useful resource for small registered entities with low-impact BES Cyber Systems that seek to strengthen their existing supply chain risk management practices.

III. BACKGROUND

A. Risk-Based Approach of CIP Standards

NERC's CIP Version 5 standards significantly expanded the scope of assets subject to cybersecurity protections, but also introduced a new approach to classify BES Cyber Systems into those having low, medium, or high impacts "commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the bulk electric system."[5] This classification approach was based on the National Institute of Science and Technology ("NIST") Risk Management Framework for cybersecurity controls.[6]

The bright-line criteria established by CIP Version 5 for classifying BES Cyber Systems are detailed in CIP-002-5.1a. A BES Cyber System is high impact if it is used by and located at, for example, a Control Center that performs the functional obligations of a Reliability Coordinator or Balancing Authority. A BES Cyber System is medium impact if it is associated with, for example, a generating facility exceeding 1500 MW, a transmission facility greater than 500 kV, or a transmission station/substation operating at more than 200 kV that is connected to three or more other transmission stations/substations. Low-impact BES Cyber Systems are those that do not fall within the medium or high impact categories, but are nonetheless associated with Control Centers, transmission facilities, generation resources, system restoration facilities, or applicable protection systems.[7] Thus, the category of low-impact BES Cyber Systems covers a more diverse set of systems than the medium- and high-impact BES Cyber Systems.

While the CIP Version 5 standards included more rigorous requirements for medium- and high-impact BES Cyber Systems, NERC, applying its risk-based approach, determined that the rigor of such requirements was not needed for low-impact BES Cyber Systems. NERC, therefore, proposed that applicable registered entities implement one or more of the documented cybersecurity policies that collectively address cybersecurity awareness, physical security controls, electronic access controls, and incident response for low-impact BES Cyber Systems.[8] NERC explained that an "overriding concern was that by mandating specific controls, the

[5] Order No. 791, P 77.
[6] *Id.*
[7] A registered entity that owns or operates a BES Facility is likely to have at least a low-impact BES Cyber System; but some small registered entities (for example Distribution Providers without any UFLS, UVLS, Cranking Path, or Special Protection Systems) may not have any BES Cyber Systems.
[8] *Id.*, P 93.

Reliability Standards would ultimately stunt the development of the range of controls necessary to protect the diversity of Low Impact assets now subject to the CIP Reliability Standards."[9]

FERC approved the overall risk-based approach embodied in the CIP Version 5 standards, including the low-medium-high impact categorization and the concept that requirements for each category should be commensurate with risk. However, FERC directed NERC to address the lack of objective criteria for the requirements for low-impact BES Cyber Systems. In doing so, FERC emphasized that NERC had flexibility in determining how to address the directive, and that the requirement for low-impact BES Cyber Systems "should be clear, objective, commensurate with their impact on the system, and technically justified."[10] Since then, FERC has issued additional directives requiring changes to standards for low-impact BES Cyber Systems but has continued to uphold the risk-based approach, explaining that requirements for "Low Impact BES Cyber Systems may be less stringent than the provisions that apply to Medium and High Impact Cyber Systems – commensurate with the risk."[11] The currently enforceable cybersecurity requirements for low-impact BES Cyber Systems, which are included in the CIP-003-6 standard,[12] are appropriately tailored to those systems' lesser risk to reliability.

B. History of NERC's Supply Chain Standards

On July 16, 2015, FERC issued a Notice of Proposed Rulemaking proposing to direct NERC to develop requirements addressing supply chain risk management for industrial control system hardware, software, and services.[13] After reviewing comments and convening a technical conference, FERC concluded that supply chain management risks pose a threat to bulk electric system reliability.[14] On July 21, 2016, FERC issued a final rule directing NERC "to develop a new or modified Reliability Standard(s) that address supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations."[15] It directed NERC to address four security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.[16] FERC emphasized that it was not directing NERC to develop "one-size-

[9] *See* Comments of NERC on the Notice of Proposed Rulemaking for Version 5 Critical Infrastructure Protection Reliability Standards at 21, *Version 5 Critical Infrastructure Protection Reliability Standards*, Docket No. RM13-5-000 (June 24, 2013), eLibrary No. 20130624-5173.
[10] Order No. 791, P 110.
[11] Order No. 822, P 35.
[12] In response to FERC's further directives approving the CIP-003-6 standard, NERC has submitted CIP-003-7, which clarifies the electronic access control requirements applicable to low-impact systems and adds requirements related to the protection of transient electronic devices used for low-impact systems. FERC has issued a NOPR proposing to approve CIP-003-7 with some directives. *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7*, 161 FERC ¶ 61,047 (2017).
[13] *Revised Critical Infrastructure Protection Reliability Standards*, Notice of Proposed Rulemaking, 80 Fed. Reg. 43,354 (Jul. 22, 2015), 152 FERC ¶ 61,054, P 66 (2015). The same NOPR also proposed to approve, with directives, NERC's CIP Version 6 Reliability Standards.
[14] Order 829, P 32.
[15] *Id.*, P 10.
[16] *Id.*, P 45.

fits-all" requirements, and explained that the new reliability standard should set goals for utilities to achieve, while allowing flexibility in how to achieve those goals.[17]

NERC initiated a reliability standard development project to address FERC's directive. The standard drafting team proposed one new standard (CIP-013-1) and modifications to two existing standards (CIP-005-6 and CIP-010-3)—all of which apply only to medium- and high-impact BES Cyber Systems—that collectively satisfy FERC's directive to address supply chain risks in a way that sets goals, while allowing flexibility in achieving those goals. The supply chain standards were approved by NERC's registered ballot body on July 20, 2017, with more than 80 percent of stakeholders voting affirmatively. The NERC Board of Trustees, when approving the supply chain standards, adopted resolutions—in addition to requesting white papers such as this one—asking NERC management, in collaboration with stakeholders, to further study supply chain risks, including the risks associated with low-impact BES Cyber Systems. The interim study must be complete by August 2018, with a final study due February 2019.

In September 2017, NERC filed the supply chain standards at FERC, and on January 18, 2018, FERC issued a Notice of Proposed Rulemaking proposing to approve them (with certain directives), finding that they make "substantial progress" in addressing supply chain risks.[18]

C. Overview of NERC's New Supply Chain Standards

NERC's supply chain standards, which are pending approval by FERC, are intended to supplement the other CIP standards by expressly addressing BES supply chain risks.[19]

The new CIP-013-1 standard requires applicable registered entities to develop and implement plans to address supply chain risk during the planning and procurement of BES Cyber Systems. Those supply chain risk management plans must include at least six specified security concepts: (i) vendor security event notification processes, (ii) coordinated incident response activities, (iii) vendor personnel termination notification for employees with access to remote and onsite systems, (iv) vulnerability disclosures, (v) software integrity and authenticity, and (vi) coordination of controls for vendor remote access. NERC's revised CIP-005-6 standard addresses specific risks related to vendor remote access. NERC's modifications to CIP-010-3 require applicable registered entities to verify the identity and integrity of software prior to installation, when methods are available to do so.

Consistent with NERC's risk-based approach to CIP standards, NERC's supply chain standards apply only to medium- and high-impact BES Cyber Systems. NERC explained that the decision to exclude low-impact BES Cyber Systems will help focus industry resources on protecting those systems with heightened risk, while not being overly burdensome or diverting resources to protecting lower risk assets.[20] FERC's NOPR agrees: "it is appropriate to await the findings from

[17] *Id.*, PP 14, 45.
[18] *Supply Chain Risk Management Reliability Standards*, 162 FERC ¶ 61,044, P 2 (2018) ("January 2018 NOPR").
[19] As discussed in Section III.G below, NERC's existing CIP standards already include requirements that help mitigate supply chain risks.
[20] January 2018 NOPR, P 13.

the [NERC Board of Trustees]-requested study on cybersecurity supply chain risks before considering whether low-impact BES Cyber Systems should be addressed in the supply chain risk management Reliability Standards."[21]

D. NERC's Efforts to Support and Enhance Implementation of its Supply Chain Standards

NERC has undertaken, or is planning to undertake, several activities supporting the industry's implementation of the supply chain standards, as well as activities beyond the scope of the standards that will further reduce supply chain risk.

NERC's standard drafting team for the supply chain standards concurrently developed an associated Implementation Guidance document, which NERC endorsed consistent with its Compliance Guidance Policy.[22] The Implementation Guidance provides that registered entities complying with the supply chain standards may use "a risk-based approach that identifies and prioritizes security controls based on the cybersecurity risks presented by the vendor and the criticality of the product or service to reliable operations."[23] NERC also intends to establish an advisory task force of registered entities to participate in an implementation study and provide feedback for further enhancement of the Implementation Guidance. This Implementation Guidance will be an important resource for registered entities developing supply chain risk management plans to comply with the standards, and may serve as a helpful point of reference for others.[24]

NERC also plans to explore opportunities with product manufacturing standards bodies—like IEEE—to ensure that supply chain risks and vulnerabilities are addressed in product specifications. And NERC is committed to exploring opportunities to assist stakeholders in developing an accreditation model for identifying vendors with strong supply chain risk management practices.[25] These activities will be particularly helpful to small registered entities with low-impact BES Cyber Systems. Small entities, with relatively little bargaining power when procuring BES Cyber System equipment and associated services, will benefit if supply chain best practices are integrated into IEEE and other product specifications. Small entities will also benefit if vendors are accredited as having strong supply chain risk management practices. If successful, these NERC efforts will help protect all BES Cyber Systems—including low-impact—from BES supply chain risks**.**

E. Broader Impact of NERC's Supply Chain Standards

NERC's proposed supply chain standards do indeed "constitute substantial progress in addressing the supply chain risks identified by the Commission."[26] Not only will the standards

---

[21] *Id.*, P 40.
[22] NERC, Petition for Approval of Reliability Standards, 29, Docket No. RM17-13, eLibrary No. 20170926-5093 ("NERC Supply Chain Petition").
[23] *Id.*
[24] NERC Supply Chain Petition, 37-38.
[25] *Id.*
[26] Jan 2018 NOPR, P 2.

directly address supply chain risk for medium and high impact BES Cyber Systems, but they also have the potential to indirectly reduce supply chain risk for all BES Cyber Systems. That indirect impact may occur in two ways.

First, most registered entities that have medium and high impact BES Cyber Systems also have large numbers of low-impact BES Cyber Systems. NERC has explained that "many of the same vendors supply products and services for all three impact categories and that the same products and services are procured for all three impact categories without differentiation."[27] APPA and NRECA members with medium impact BES Cyber Systems that were interviewed for this white paper[28] confirmed that their goal is to apply the same cybersecurity BES supply chain practices across their organizations, including to lower impact systems where doing so makes sense from a cost and reliability risk perspective. Thus, when registered entities implement their processes and procedures to comply with the new supply chain standards for their medium and high impact BES Cyber Systems, they are likely to apply those same or similar processes and procedures more broadly to their procurement and vendor management practices.

Second, as larger registered entities with more bargaining power insist that vendors comply with new supply chain risk management practices, those vendors may well adopt those practices across the board. For example, vendors may decide to include cybersecurity concepts in their product design or in their standard contract provisions. Small APPA and NRECA members with only low-impact BES Cyber Systems often use the same, well-known, established vendors that larger registered entities use,[29] so to the extent that those vendors adopt more stringent cybersecurity practices to accommodate the larger entities, small registered entities will benefit from those risk-reducing measures. Moreover, as noted in Section III.E above, NERC will be exploring opportunities to incorporate cybersecurity concepts into standard product design specifications by other bodies and to develop accreditation mechanisms for vendors. As vendors adapt to meet the supply chain risk management needs of their largest customers, all their customers stand to benefit.

F. Other Standards Impacting Supply Chain Decisions for Small Registered Entities with Low-Impact BES Cyber Systems

All registered entities have an inherent interest in procuring safe, reliable BES Cyber Systems and working with vendors that will not compromise the security of their valuable assets. As discussed in Section IV and V below, smaller registered entities have many resources available to facilitate sound decision making when procuring new assets and selecting vendors. Registered entities with low-impact BES Cyber Systems can use those resources to mitigate supply chain risks.

In addition, the existing CIP standards require registered entities to implement cybersecurity plans for low-impact BES Cyber Systems, and those plans will mitigate some supply chain risks. For example, CIP-003-6 R2, Attachment 1, Section 1 requires registered entities with low-impact

[27] NERC Petition at 19.
[28] *See* Section IV below for a description of the interview process and a synthesis of the resulting best practices.
[29] *See* Section IV.A.1 below, describing how small registered entities rely on well-known established vendors to mitigate supply chain risk.

BES Cyber Systems to have—and regularly reinforce—cybersecurity awareness practices, such as monitoring of alerts from NERC, the E-ISAC, and other sources to be aware of security threats affecting equipment sold by their suppliers. Awareness of security risks will help small registered entities avoid vendors and suppliers with known vulnerabilities.

Similarly, CIP-003-7 R2, Attachment 1, Section 5.2 (which is pending approval by FERC) requires registered entities with low-impact BES Cyber Systems to use appropriate tools to mitigate the introduction of malicious code *before* a third-party vendor may connect a transient cyber asset (e.g. the vendor's laptop) to a low-impact BES Cyber System. Those tools could include reviewing the vendor's antivirus update process, whitelisting policies, or their system hardening practices.

And CIP-003-6 R2, Attachment 1, Section 4 requires registered entities with low-impact BES Cyber Systems to identify, respond to, and (where appropriate) report on cybersecurity incidents, regardless of the source of the attack. Thus, even if a vulnerability was introduced to a BES Cyber System prior to purchase, or if an attack was launched through a third-party vendor, the standard requires the registered entity to respond to that incident.

In short, the existing CIP standards already require some basic supply chain risk management practices for low-impact BES Cyber Systems.

IV. BEST PRACTICES FOR SMALL REGISTERED ENTITIES WITH LOW-IMPACT BES CYBER SYSTEMS

To address the NERC Board of Trustees' resolution calling for the Associations to address best and leading supply chain security practices of use to smaller entities, APPA and NRECA retained the U.S. Resilience Project to interview a sample group of APPA and NRECA utility members. These interviews were undertaken with nine of the Associations' members, which were asked to detail the risks they have identified, along with the risk mitigation practices they have implemented or intend to implement. The sampled companies—including distribution cooperatives, generation and transmission cooperatives, municipal utilities, and joint action agencies—range in size and in the types of assets that they own and operate. Larger members with medium- and high-impact BES Cyber Systems, which will be subject to NERC's supply chain standards, had more tools and resources available to them to mitigate supply chain risks than the smaller members with only low-impact BES Cyber Systems. Nevertheless, the interviews showed that those smaller registered entities can—and do—implement several supply chain risk management practices that can be considered best practices commensurate with the low risk that those entities pose to BES reliability.

The sampled companies were well aware of cyber supply chain risks. The risks (and their relative magnitude) varied from entity to entity, in part based on the impact level of the entity's BES Cyber Systems and in part based on the importance of each BES Cyber System to the entity's own operations. For example, an entity might take greater supply chain risk mitigation measures for a primary Control Center that is important for serving the entity's load, even if that Control Center contains only a low-impact BES Cyber System.

Small registered entities with low-impact BES Cyber Systems face a variety of supply chain risks. One of the largest risks is that of a malware campaign infecting a product with malicious code while the product is still within the control of the vendor (i.e., before the product is received by the utility). Another supply chain risk is from employees of vendors who have remote access to BES Cyber Systems. Several best practices, discussed below, are available to small registered entities with only low-impact BES Cyber Systems to mitigate those risks.

The supply chain risks that have been identified, and the catalog of best practices to address those risks, reflect this particular snapshot in time. Supply chain risk assessment is rapidly evolving, so new risks may emerge and existing risks may be diminished. As NERC's supply chain standards are implemented, larger entities subject to those standards and their vendors will likely evolve as to how they mitigate supply chain risks, which may result in more best practices for small registered entities to consider using to mitigate their lower-impact supply chain risk.

What follows is a distillation of supply chain risk management practices that (except where otherwise noted) have already been deployed by one or more small registered entities with only low-impact BES Cyber Systems to mitigate supply chain risks. These practices are divided into five categories: (A) Organization; (B) Vendor Selection; (C) Vendor Remote Access; (D) Software Integrity and Authentication; and (E) Software Updates and Patch Management.

A. Organization

1. Leadership from senior management is an important element of mitigating supply chain risks, regardless of the size of an organization.

Senior management leadership is an important feature of a successful risk management program. Senior management's express focus on security matters, including supply chain security, assures organizational commitment and facilitates enterprise-wide coordination.

Supply chain decisions are often made by individuals working in different parts of an organization, which could include information technology, engineering, operations, legal, security, compliance, and procurement groups. Each of those groups should consider supply chain risks and take action to mitigate those risks, which may require coordination with other groups in the organization. For many organizations, the division of responsibilities for cybersecurity and supply chain risk among such groups as the Procurement, Information Technology and the Engineering and Operations Technology groups creates particular challenges. Such challenges can be addressed by engaged senior leadership that empowers and directs diverse groups to common security and reliability goals and solutions.

Having senior management provide leadership on supply chain risk management (and on cybersecurity more generally) is thus important for organizations of all sizes. One sampled company explained that a top-down approach can facilitate a culture of cross-functional cooperation and a focus on security. Another described the advantages of having a risk oversight committee consisting of the COO, CFO, Chief Legal Officer, and Customer Executive, that provided visibility into supply chain risks at the most senior level of the company. And one sampled company emphasized the importance of having clear guidance from senior management on what the organization's cyber supply chain policies are and the rationale for those policies.

2. Improving coordination and cooperation between departments in an organization mitigates supply chain risks.

In addition to leadership from senior management, inter-department coordination and cooperation are important parts of mitigating supply chain risks. Several practices can be used to improve such coordination and cooperation, depending on the organization. For example, multiple sampled companies described having regular, inter-departmental supply chain risk management meetings where key players come to the table to vet risks. Another sampled company had clearly defined roles for different departments in relation to cybersecurity and supply chain risk management, such that each team is responsible for its own role in vetting a technology or procurement before a purchase order can be released.

Another effective practice is to develop a cybersecurity team that regularly engages with and advises other departments that are making procurement or other supply chain-related decisions. One sampled company described the efforts of its cybersecurity group to identify the "value-add" that it could provide to other departments, and thus function as a trusted ally rather than an oversight group that imposed requirements on other departments. As a result of that approach, the sampled company explained that its cybersecurity group is being engaged early by other departments in their decision-making processes. For example, the cybersecurity group has worked with procurement and legal staff to draft information security requirements for contracts, provided advice for large equipment purchases and upgrades, and participated in the entity's innovation committee to help ensure that security remains a key focus when the entity considers new technologies. While creating a cybersecurity group may be a practice more suitable for larger registered entities, smaller registered entities may be able to incorporate elements of this approach into their organizations.

3. Enterprise-wide cyber risk assessments, including supply chain, help identify the most significant threats to each individual organization.

Every organization is unique, and each face different risks and vulnerabilities with respect to supply chain. Understanding an organization's specific risks and vulnerabilities, as well as understanding the specific details of their systems, is an important risk mitigation strategy. One element of such an enterprise-wide risk assessment is developing an awareness of the equipment and software that an entity has, as well as of the equipment's interconnections to the outside world. This process may result in registered entities identifying unique risks to be addressed.

The NIST Framework and the Department of Energy ("DOE") Maturity Model, both of which are described in Section V.C below, are useful frameworks for evaluating and mitigating risks. Each call for the development of organizational understanding of assets and dependencies (e.g., vendors) to manage cybersecurity risk as a starting point for a risk management program. A number of sampled companies used these two frameworks when conducting their own enterprise-wide cyber risk assessments, which included supply chain risks. Regardless of an entity's size or the impact level of its BES Cyber Systems, elements of the NIST Framework and DOE Maturity Model may be helpful when a registered entity conducts its own risk assessment.

4. Having processes to identify unusual system activity allows utilities to respond rapidly to cyber events, including those arising from supply chain vulnerabilities.

In addition to taking appropriate measures to prevent BES Cyber Systems from being compromised with malicious code resulting from a supply chain vulnerability, registered entities should seek to quickly identify and correct compromises when they do occur, to minimize the associated harm.

Malicious code and other cyber threats, including supply chain-related threats, often manifest themselves as unusual activity on a utility's systems. Just as physical security is enhanced when employees are aware of and report on unexpected individuals or materials that are present at a utility's facilities, cybersecurity can be enhanced when organizations have processes to identify unusual software on or equipment connected to their BES Cyber Systems.

One method to improve visibility and identify unusual activity is to train employees to know when their systems are behaving within normal parameters and how to report when they are not. A second method is to use automated software and hardware tools—e.g., firewall devices and intrusion detection/prevention systems[30]—that identify certain types of unusual activity, send alerts to appropriate personnel, and in some cases, take automatic mitigation actions. These automated tools may be available from vendors themselves, and information about such automated tools may be elicited in a vendor questionnaire, discussed below. A third method for identifying unusual activity is to manually analyze network traffic and system logs, though such data is often difficult to obtain from operational systems, and even when it can be obtained, the analysis requires having employees that have the time and specific training with the analysis systems. Employing one or more of these methods will improve a registered entity's visibility into its systems and will facilitate rapid response to cyber events.

B. Vendor Selection

1. Using well-known, trusted, and established vendors is a good starting point for reducing supply chain risk.

As noted above, a significant supply chain risk is that of a malware campaign infecting a product with malicious code while the product is still within the control of the vendor (i.e., before the product is received by the utility). Utilities have little to no visibility into how their vendors develop and test software or into their vendors' employment practices. While malicious code detection software and security practices (addressed below) may address these risks after receipt by the utility, the prudent selection of vendors will help mitigate these risks up front.

As a starting point, one way to mitigate the risk of infected products is to purchase products or services from well-known, trusted and established vendors. It is preferable to purchase products and services directly from the vendor[31] or, alternatively, from distributors that are also well-

[30] APPA, in collaboration with the Department of Energy, is funding pilot deployments of intrusion detection systems on public power utility networks to monitor and alert personnel of unusual cyber activity.

[31] In other words, to purchase directly from the manufacturer of a product, rather than a distributor/reseller of the product.

known, trusted and established. If a product is vulnerable and not secure, one sampled company pointed out, that product and that company will not be on the market for long. While the Associations are not in a position to recommend specific suppliers, they advise members to rely on the network of security professionals available through Association membership to develop a list of trusted vendors and to more deeply vet those less well known to purchasers.[32] The Associations will assist their members in making these contacts. In the absence of a third-party accreditation system for BES Cyber System vendors (discussed below), using established vendors reduces supply chain risk for registered entities. Large utilities with medium and high impact BES Cyber Systems also use the same well-known vendors, and will put pressure on those vendors to improve their supply chain protections. Thus, by using the same name-brand vendors, small registered entities can take advantage of the efforts of the larger utilities.

While relying on a vendors' reputation is a good starting point, small registered entities with low-impact BES Cyber Systems should adopt a "trust but verify" approach to such vendors. As discussed in Section D and E below, other practices can be used to verify the authenticity and integrity of new products and software patches from trusted vendors.

2. Reducing the number of vendors used by a utility can improve expertise in those vendors' systems and allow for better relationships with those vendors, thus reducing supply chain risk.

Many organizations purchase equipment through formal RFP process, which over time can result in having equipment from multiple vendors. Reducing the number of vendors from which a registered entity purchases can reduce supply chain risk. One sampled company noted that a decade ago, it had eight different brands of relays throughout its system and substations, and maintaining expertise on eight different manufacturers proved to be unnecessarily difficult. That organization now uses sole source purchasing for certain types of equipment, such as relays, to minimize risks. Another sampled company takes a similar approach, noting that reducing the number of vendors it works with has the benefit of keeping its systems simpler and allows the utility to build better relationships with its vendors. Better vendor relationships can facilitate better supply chain risk management practices for small registered entities by increasing their ability to obtain answers to supply chain questionnaires (*see* B.3 below) and potentially to secure improved contract provisions (*see* B.4 below).

3. Standard questionnaires can be a useful tool for vetting vendors to reduce supply chain risk.

To better evaluate vendor security practices, registered entities can employ questionnaires that form the basis of a security checklist in connection with the procurement process. Vendors' responsiveness to such questionnaires may vary, and small registered entities may have less ability to obtain meaningful responses than larger entities, but asking appropriate questions of

[32] APPA and NRECA, in coordination with our federal partners, inform members of suppliers who have been identified by the federal government as not trusted, such as the federal ban on use of Kaspersky Labs and most recently the FCC Notice of Proposed Rulemaking to Ban Huawei and ZTE telecommunications equipment.

vendors can nevertheless mitigate supply chain risks.[33] sampled companies that use such questionnaires identified the following topics for the questions:

- Whether sensitive information is stored or transmitted outside client-utility servers and the nature of associated protections;
- Nature and scope of security organization and practices, including third party or self-assessments, detection and remediation practices;
- Nature of access controls;
- Measures taken to ensure system integrity;
- Information management security; and
- Whether a mature process for change management (including patch management) is employed.

The specific questions and topics chosen for a particular vendor will vary depending on the nature of the product, whether it serves an IT or OT function, whether the vendor will have remote access, and more generally, the nature of perceived risks. Cloud vendors were identified as vendors that require close scrutiny, because those vendors store (and have access to) potentially sensitive registered entity data, although not necessarily BES Cyber System data.[34] One sampled company stated that it uses a more formalized questionnaire for cloud vendors, based on NIST 800-53 controls.[35] Other sampled companies emphasized the importance of knowing which country the cloud vendors were storing their data in.

The Associations can facilitate relationships between members that will enable them to share the details of vendor questionnaires and related best practices with one another.

4. As these issues mature, standard contract language for vendors may become viable tools for all registered entities, large and small, to mitigate supply chain risk.

Negotiating contract terms with vendors to reduce a registered entity's supply chain risk can be an effective mitigation tool. However, many small registered entities with only low-impact BES Cyber Systems lack the bargaining power to demand that their vendors agree to specific contract terms. At this time, none of the sampled companies who are small registered entities with only low-impact BES Cyber Systems indicated that they have successfully negotiated supply chain risk reducing contract provisions with vendors. As larger entities begin compliance with NERC's supply chain standards and become more proactive about supply chain risks, they will have greater incentive to negotiate appropriate contract terms with vendors. Over time, vendors may start including such supply chain risk management contract terms as standard terms for all registered entities, or at least become more accustomed to requests for risk-reducing contract terms. For example, larger registered entities may pressure vendors to include, as a standard contract term, that their employees with remote access to BES Cyber Systems will be subject to

[33] None of the sampled companies who are small registered entities with only low-impact BES Cyber Systems stated that they currently use standardized questionnaires, but this practice may merit consideration.
[34] No sampled companies indicated that they store BES Cyber System data on the cloud.
[35] NIST 800-53 Revision 4 (Security and Privacy Controls for Federal Information Systems and Organizations) provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizations from a diverse set of threats, including cyber-attacks. https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

background checks. Vendors may then be more willing to extend those terms to small registered entities, making that a more viable option.

5. Third-party accreditation and vendor self-certification would improve the ability of all entities, particularly small registered entities, to select reliable vendors.

As noted above, utilities, particularly small registered entities, have little to no visibility into vendors' internal security practices. Even the largest of the interviewed members noted that it is very difficult for individual utilities to force vendors to provide contract assurances about the integrity of their products.

One potential future solution to this problem would be to develop third-party accreditation that would allow small entities to have more confidence in the vendors they select. Two sampled companies identified a model similar to the Underwriters Laboratories that could be used to vet code and verify that it has not been corrupted or tampered with. As noted in Section III.D above, NERC is committed to exploring opportunities to develop such an accreditation model.

An additional option may be for vendors to self-certify that they comply with the requirements of available security models, such as the NIST Framework, AICPA SOC,[36] supply chain standards published by the International Organization for Standardization (ISO),[37] and FedRAMP.[38]

C. Vendor Remote Access to Systems

All the interviewed members identified remote access to their systems by vendors as a risk they address. While one sampled company stated that it prohibits vendor remote access, that sampled company noted the significant cost associated with only allowing on-site vendor support. Other sampled companies allow some vendor remote access, but take action to mitigate the risks associated with that activity. Small registered entities with only low-impact BES Cyber Systems have several effective tools available to mitigate remote access risks, including (1) restricting *where* on the system vendors can have remote access; (2) restricting *when* vendors can have remote access; and (3) monitoring *what* the vendor does while having remote access.[39]

---

[36] *See* https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html (describing the American Institute of Certified Professional Accountants' suite of service offerings for System and Organization Controls (SOC)).

[37] For example, ISO/TEC 27036-1:2014 and ISO/TEC 27001:2013 are standards on information security for supplier relationships and security management systems, respectively. *See* https://www.iso.org/standard/59648.html, https://www.iso.org/standard/54534.html.

[38] *See* https://www.fedramp.gov/about/ (describing the Federal Risk and Authorization Management Program (FedRAMP)).

[39] In addition to the practices described here, NERC's CIP-003-7 (which is still pending before FERC) will require registered entities with low-impact BES Cyber Systems to implement security plans for Electronic Access Control and Transient Cyber Asset Risk Mitigation. These requirements will further mitigate supply chain risks associated with vendor remote access to low-impact BES Cyber Systems.

1. Limiting the systems that can be accessed remotely reduces supply chain risk.

Limiting the systems to which vendors have remote access reduces supply chain risk. Multiple sampled companies discussed the importance of having a thorough understanding of the tasks the vendor needs to perform in providing their services, and restricting their access to only those systems that are required to complete those tasks. This, in turn, counsels a "least privilege" approach to vendor access, ensuring that vendors operate at privilege levels no higher than necessary to perform their assigned functions.

Different tools can be used to restrict access. Separating SCADA systems from the internet and from corporate IT systems, whether through isolation or secure firewalls, are techniques that may warrant consideration where it is achievable and depending on how the systems are configured.

Other alternatives may also warrant consideration. For example, creating specific user accounts on a registered entity's system for vendors, and locking down those accounts to only allow permission for certain actions. In addition, the use of firewalls and other hardware/software tools can limit remote access to specific areas of a registered entity's networks. By restricting access, utilities can reduce the risk of a vendor compromising other parts of their systems.

2. Restricting vendor remote access to specific service requests reduces supply chain risk.

Another effective risk-reducing technique is to allow vendors remote access to BES Cyber Systems only when a specific service has been requested. One sampled company explained that if a vendor needs remote access to support equipment, a firewall is turned on for that one entrance into the system, and then access is turned off once the support request is completed. Two sampled companies described a two-factor authentication system using vendor access tokens, which remain in the utility's possession, that authorize a vendor's remote access and that are revoked once a support ticket is completed. By limiting vendor access to only the times when a there is need for specific support, utilities can reduce the risk of a vendor gaining remote access to their system at other times.

3. Monitoring vendor remote access can be done in real-time or by reviewing logs after vendor remote access is complete.

In addition, registered entities should consider using monitoring tools to verify that vendors are doing what they are supposed to when they have authorized remote access to the systems. Some sampled companies analogized remote access monitoring to providing escorted physical access to outside personnel. sampled companies described different tools for monitoring vendor remote access.

One effective technique is to have an employee continuously monitor vendors while the vendor has remote access to their systems. One sampled company explained that it only allows vendor remote access through a screen-sharing system, in which the vendor could see the screen but the utility's employee would be the one typing commands or executing the work required. Another sampled company described a similar screen-sharing process that allows the vendor to conduct

the required maintenance activity, but enables an employee to watch the screen to monitor what the vendor is doing. sampled companies discussed the benefits of both of these approaches, but also noted that they are costly approaches that require additional utility staff.

Another monitoring approach is to use software that logs all actions the vendor took while having remote access to the system. This allows employees to review the logs after the fact to determine what the vendor did during its remote access session. This less costly approach is appropriate when the risk does not justify having an employee do live monitoring.

4. Monitoring of remote access points reduces supply chain risk.

Malicious actors may attempt to gain access to a small registered entity's system through the remote access points that are intended to be used by vendors. Routinely monitoring those remote access points will help identify malicious intrusion attempts, thus reducing the risk associated with vendor remote access. Some sampled companies identified automated tools for network monitoring, however those tools can be expensive and may not be justifiable for the risk posed by small registered entities with only low-impact BES Cyber Systems. Depending on a risk assessment, a small registered entity could decide to limit the use of automated monitoring tools to the highest priority remote access points. Alternatively, registered entities could monitor the firewalls and remote access points that permit interactive access using the built-in tools, such as alerts, that are available on those devices.

D. Software Integrity and Authentication

1. Risk assessments should be conducted as part of the decision to upgrade BES Cyber Systems.

As technology improves, upgrading to new software and hardware can be attractive in terms of cost and functionality. But the decision to jump to the newest technology should be taken with great care, because the introduction of new technology might increase supply chain risk. One sampled company noted the importance of being intentional and deliberate about adding new software to an environment, and planning to have processes and resources to maintain the software. Another sampled company explained that new software packages must be vetted by the utility's enterprise cybersecurity team, with an emphasis on looking at the history of vulnerabilities for that particular package. Consultants can also advise a small registered entity on the cyber risks associated with new software. Small registered entities should therefore consider including a supply chain risk assessment as part of the decision to upgrade BES Cyber Systems or purchase new BES Cyber Systems.

2. New software should be thoroughly tested prior to installation.

As noted above, utilities have limited ability prior to delivery to identify when software or equipment received from a vendor includes malicious code. Even when using well-known, established vendors (*see* B.2), small registered entities can further reduce risk by adopting a process to test new software before installing it on their production systems. The depth of the testing, and the environment that the software will be tested in, will depend on the risk associated with installing that software.

The strongest method is to install and test software in a separate testing environment that is identical to the production environment, prior to transferring the new software into production. This method requires a registered entity to maintain a separate physical test environment, which is more feasible to do for IT systems but harder to do for SCADA systems.

Maintaining a separate physical test environment for SCADA systems may not be warranted for small registered entities with only low-impact BES Cyber Systems. It is nevertheless advisable to test new software prior to its installation in the production environment. Small registered entities can consider alternative testing methods, including: using virtual systems for testing, taking advantage of vendors' laboratory facilities, or partnering with local universities to gain access to test facilities.

E. Software Updates and Patch Management

1. Especially for SCADA systems, patch management contracts can help to mitigate supply chain risks.

Software patches allow vendors to close security vulnerabilities that have been identified, so failing to apply software patches in a timely fashion can leave a utility's system unprotected from known risks. However, knowing which patches to install and when, and deploying those patches across an organization, can be a complicated task.

One approach, used by several sampled companies, to help ensure patches are timely applied is to enter into patch management contracts with vendors. Sampled companies found this to be particularly true for SCADA systems. Multiple sampled companies reported that they have patch management contracts with their SCADA system vendor under which the vendor tests and validates patches, and reports on which patches can be applied without concern and which should be applied with caution. Patch management can also be managed by the company. These decisions are unique to each company.

2. Testing patches prior to their implementation mitigates supply chain risk.

Just as with new software, it is very important to test software patches prior to their installation on production systems. Thus, the processes described in Section D.1 above also merit consideration with respect to software patches. Some sampled companies emphasized the necessity of being particularly deliberate when installing patches on operational systems, because of the risk that a patch will damage the system or adversely impact performance. Unlike applying a compromised patch to an email server, applying a compromised patch to a SCADA system has greater risk to grid reliability and thus should be tested carefully.

3. Confirming patch authenticity prevents the insertion of malicious code while the patch is being transmitted.

Many patches are downloaded over the Internet, so there is a risk that a patch could be altered as it is being transmitted. Recognizing that risk, sampled companies identified various tools that are available to confirm the authenticity of software patches that are downloaded. One sampled

company stated that when a vendor provides the option to download patches over an encrypted channel, using that encrypted channel is preferable. Other sampled companies use the hash value provided by the vendor to confirm software authenticity. Verifying hash values is an effective way to ensure that you received what the vendor sent you, though it does not verify that what the vendor sent is good.

V. CYBER SUPPLY CHAIN RISK MITIGATION PROGRAMS – THE ASSOCIATIONS' PROGRAMS AND OTHER KEY RESOURCES

In addition to complying with applicable NERC standards and employing appropriate best practices, the Associations' members continue their focus on cybersecurity risks, including supply chain risk, through the use of voluntary programs being developed by the Associations and others that go beyond the NERC standard development process. Public power and cooperative efforts to strengthen cybersecurity broadly and supply chain risk specifically, apply broadly to all their members and are not limited to NERC registered entities. Therefore, voluntary programs that any company can take advantage of are key to public power and cooperative utilities, especially smaller companies.

Through the Associations' participation in the Electricity Sub-Sector Coordinating Council (ESCC), the organizations' members can be informed of the broad array of security risks and appropriate mitigation. A key outgrowth of increased collaboration with government partners has been each of the Associations establishing cybersecurity-related programs with the DOE that include supply chain modules.

A. APPA and DOE Cooperative Agreement

APPA has partnered with the Department of Energy ("DOE") in a Cooperative Agreement, to undertake an extensive multi-year, multi-task project of improving the cyber resiliency and security posture of public power utilities. The project goal is to improve the resiliency and cybersecurity infrastructure within public power utilities. In this project, APPA will accelerate its efforts to help public power utilities to better understand and implement resiliency, cybersecurity and cyber-physical solutions, including refining and improving the adoption of advanced control concepts, where applicable, to achieve security infrastructure improvements.

Supply chain is one of the important modules contained within the APPA/DOE effort. One of the key aspects of the effort is the recognition that sufficient security relies on the successful implementation of the collective effort. Security cannot depend solely on the successful implementation of supply chain protocols alone.

Through the program APPA evaluated its members and concluded that many mid-to-small-sized public power utilities outside of the NERC Registry have unique organizational structures including systems control and monitoring, internal or city information technology departments, varied leadership/governance models, and use of third party service providers. Because of the multi-layer structure of these organizations, a program was needed that could respect both the legal and regulatory parameters of utilities and city government to improve identification and mitigation of cyber risks threats.

APPA conducted outreach to members and engaged over 400 individuals using facilitated exercises, training sessions on implementing the DOE Electricity Sector Cybersecurity Capabilities Maturity Model (ES-C2M2), on-site vulnerability assessments and threat information sharing analysis. The initial evaluation showed that public power utilities want additional education, coordination, capability building, and pre-established resources to monitor and detect threats, maintain situational awareness among decision makers, and respond properly to threats and indicators of varying degrees. The evaluation results included addressing the threat to their supply chain.

To meet that demand for additional education and awareness APPA contracted with four training organizations and developed a catalog of low cost training sessions to be offered to members. Training is essential to ensure the public power workforce understands the risk and takes appropriate action to further enhance their cybersecurity maturity level. Each year APPA provides several conferences and standalone training opportunities for its members and they rely on these sessions to provide low cost opportunities to educate their employees. In addition, APPA has facilitated technical workshops, exercises and/or roundtable discussions to challenge assumptions and test out models developed in the DOE project including tabletop exercises.

The APPA conducted 14 tabletop exercises modeled around the 2015 Ukraine cyber-attack to discuss threat information sharing and the challenges of communicating sensitive information to a broad audience of over 2000 utilities. In the past, APPA has cascaded E-ISAC threat information, including supply chain threat information, to its members through emails and in person meetings. This had limited reach as many small utilities may not have the resources to participate in Association's activities. Therefore, it was determined that the Joint Action Agencies and State Associations would be a better forum to build trust partnerships for small utilities to receive threat information. APPA is still recommending that members sign up for the E-ISAC alert portal, but in the future, we hope to build a hub and spoke information sharing network to help reach the smaller utilities with supply chain threat information.

Finally, APPA used the DOE ES-C2M2 tool to develop a simplified Cybersecurity Scorecard to facilitate the self-assessment process. Within the scorecard is a section addressing supply chain and recommendations on how a utility can address this risk. The scorecard output is an action plan report identifying opportunities for improvement and recommendations for next steps. In the next phase of this work APPA will provide a Cyber Resiliency and Security Roadmap (Roadmap) that will outline the strategic and tactical steps needed for public power utilities to harden their systems to achieve cyber resiliency. The Roadmap will address supply chain risk along with policies and procedures templates, incident response case studies, a cyber asset tracker methodology, a procurement guide, and metrics on tracking overall progress toward improving cyber and physical maturity.

B. NRECA and DOE Collaborative Partnership

In 2016, NRECA received funding through a collaborative partnership with the U.S. Department of Energy's Cybersecurity for Energy Delivery Systems (CEDS) program. As a result, NRECA created its Rural Cooperative Cybersecurity Capabilities Program (RC3) to support cooperatives as they work to improve the cyber and physical security of their organizations, including procurement and supply chain issues.

RC3 is focused on developing tools and resources appropriate for small- and mid-sized cooperatives that lack the resources to employ significant information technology staff. The RC3 program also provides collaboration, education, and training opportunities that are available to all cooperatives. Tools, products, and resources developed in the RC3 program will be available to all cooperatives.

As part of the RC3 program, NRECA has been holding a series of Cybersecurity Summits around the country. These summits bring co-ops together to hear from industry experts on cybersecurity and learn from each other in peer-to-peer discussions. Input from attendees also helps shape RC3 program directions to ensure our efforts are on target with co-op cybersecurity needs. Six summits were offered in 2017 and more are planned for 2018:

Through the RC3 Self-Assessment Research Program, NRECA is working with cooperatives to test a new cybersecurity self-assessment tool. The tool, developed by NRECA, will help cooperatives understand their cybersecurity posture. Results of the self-assessment can be used by the cooperative to prioritize mitigation actions and develop a cybersecurity action plan for their organizations.

Lessons learned during the testing and deployment of the tool will be used to make improvements to the self-assessment tool. Once finalized, the RC3 self-assessment tool will be released for the use and benefit of the cooperative community as a whole.

In 2017, the RC3 program offered two courses. One covered issues associated with managing cybersecurity risk in purchasing decisions, and the second course focused on how to procure and manage cybersecurity vulnerability assessment providers. Additional cybersecurity courses will be offered in 2018.

Like safety, cybersecurity is a responsibility of everyone at a cooperative. However, each job role in a co-op may have unique cybersecurity responsibilities. RC3 is developing a series of cybersecurity guidebooks to provide information pertinent to specific job roles within a cooperative. The first guidebook is focused on staff that have responsibilities in communications, member services and public relations, and the second guidebook will focus on cybersecurity issues relevant to attorneys and legal staff that work with cooperatives.

Receiving timely alerts on cybersecurity threats and implementing mitigation actions quickly are two key components for protecting cooperatives from cyber incidents. The RC3 program provides training and resources to increase awareness and access to existing organizations that provide threat alerts, and supports research and development projects that will improve the cooperative community's capabilities to respond to threats.

NRECA has also shared other resources with its members, including the DOE ES-C2M2, the ESCC Cyber Mutual Assistance (CMA) program, and the NIST Cybersecurity Framework. Previously, NRECA developed its Guide to Developing a Cybersecurity and Risk Mitigation Plan and Template and provided that to cooperatives for their consideration and use.

C. Other Key Resources Available on Supply Chain Risk Management Practices

A substantial body of resources prepared for entities within and outside the electric industry is available to NERC registered entities interested in addressing supply chain risk in greater depth.

Practices reflected in these resources were not designed with small, low-impact registered entities specifically in mind, and may not be appropriate for such entities given their limited BES Cyber System, and in turn reliability risk, resource capabilities and other circumstances. However, these resources may include elements or concepts that, if appropriately modified or adapted, may be of help to such an entity as it develops risk mitigation.

The following is a high-level overview of some of the more prominent of these resources.

1. Department of Energy ("DOE") Cybersecurity Procurement Language for Energy Delivery Systems[40]

Developed through the Energy Sector Control Systems Working Group, this resource is represented as a baseline for cybersecurity procurement language applicable to operational technology ("OT"), including control centers, though it can be applied more broadly. Recommendations are drawn from supplier and acquirer community surveys and include the following:

- General cybersecurity procurement language (software specifications; access control; account management, authentication, password policy, logging and auditing, malware detection and protection);

- Supplier life cycle security program management (secure development practices; documentation and tracking of vulnerabilities, patch management and updates; supplier personnel management and secure hardware and software delivery); and

- Intrusion detection (host intrusion; network intrusion).

2. Utilities Telecom Council, Cyber Supply Chain Risk Management for Utilities – Roadmap for Implementation[41]

UTC's whitepaper recommends that utility-purchasers take a series of steps in connection with asset procurement, including:

- Identification of critical assets, systems, and processes, and prioritization;
- Identification of critical data/information;
- Supplier identification;
- Assessment and prioritization of supplier risk;
- Establish general security requirements by priority;
- Establish how information on vulnerabilities and incidents can be shared with suppliers;

[40] DOE, Cybersecurity Procurement Language for Energy Delivery (Apr. 2014), available at https://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014.
[41] 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.

- Establish how supplier adherence to requirements will be monitored;
- Internal training;
- Contingency planning; and,
- Risk analysis.

3. NIST – Framework for Improving Critical Infrastructure Cybersecurity[42]

Draft Version 1.1 of the Cybersecurity Framework addresses supply chain risk management (RM) in the context of NIST's maturity model for cyber risk management. The methodology is focused on the development of relevant security outcomes (e.g., product or service integrity), and the evaluation of suppliers (information technology, "IT", and OT) against identified criteria. The Framework includes the following core elements:

a. Objectives: Identification, assessment, and mitigation of risk associated with products and services that may contain malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain.

b. Strategic Options:

- Determining cybersecurity requirements for suppliers;
- Enacting cybersecurity requirements through formal agreement (e.g., contracts);
- Communicating to suppliers how cybersecurity requirements will be verified and validated;
- Verifying that cybersecurity requirements are met;
- Governing and managing the above activities.

4. DOE Electricity Subsector Cybersecurity Capability Maturity Model ("ES-C2M2")[43]

Similar to NIST's Cybersecurity Framework (addressed above), DOE's ES-C2M2 is a cybersecurity maturity model for cyber risk management, and includes supply chain risk management as one of its recommended domains (areas of competence). The ES-C2M2 identifies three objectives for supply chain risk management and details associated practices at

[42] NIST – Framework for Improving Critical Infrastructure Cybersecurity, available at https://www.nist.gov/cyberframework/draft-version-11.
[43] DOE, ES-C2M2, Version 1.1, Section 7.8 (Feb. 2014), available at https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf. Additional information about the DOE C2M2 program (of which the ES-C2M2 is a component) is available at https://www.energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program.

increasing levels of sophistication that may be adopted. The objectives, and illustrative examples of the associated practices, are as follows:

- Identify dependencies: At the lowest level of competence, IT and OT dependencies are identified. Activities associated with a more sophisticated approach calls for risk-based ranking of dependencies.
- Manage dependency risk: At the lowest level of competence, significant cybersecurity risks are identified. At higher levels of competence, risks are ranked, vendors are chosen based on cybersecurity risk evaluation, supplier agreements reflect cybersecurity management practices, risk information is shared, risk management protocols are detailed and supplier practices are subject to periodic review.
- Management activities: At a lower level of competence, an organization will follow documented supplier chain risk management practices. At higher levels of accomplishment, compliance objectives may be established and reviewed.

5. NIST – Special Publication 800-161 – Supply Chain Risk Management Practices for Federal Information Systems and Organizations[44]

NIST's Special Publication 800-161 provides guidance to federal agencies on identifying, assessing, and mitigating information and communications technology (ICT) supply chain risks. The intent is to increase the ability of organizations to manage ICT supply chain risks over the entire life cycle of systems, products, and services. The security controls addressed in the publication include: Access control; Security assessment and authorization; Configuration management; Contingency planning; Identification and authentication; Incident response; Maintenance; Media protection; Physical and environmental protection; Provenance; Risk assessment; System and services acquisition; System and communications protection; and System and information integrity.

6. DHS, ICS-CERT, Cybersecurity Procurement Language for Control Systems[45]

[44] NIST, Special Publication 800-161 – Supply Chain Risk Management Practices for Federal Information Systems and Organizations (Apr. 2015), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf. Building on the NIST 800-series of publications, NIST Special Publication 800-161 applies the multitiered risk management approach from NIST Special Publication 800-39, by providing ICT supply chain risk management guidance at organization, mission, and system tiers. It also contains an enhanced overlay of specific ICT supply chain risk management controls, building on NIST SP 800-53 Revision 4. See NIST Special Publication 800-39 – Managing Information Security Risk (2011), available at http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf; NIST Special Publication 800-53 Revision 4 – Security and Privacy Controls for Federal Information Systems and Organizations (2013), available at http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[45] DHS ICS-CERT, Cyber Security Procurement Language for Control Systems (Sept. 2009), available at https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf.

The work reflected in this document was undertaken collaboratively by DOE, DHS, and industry cybersecurity and control system subject matter experts, and addressed to security principles and controls associated with the design and procurement of control system products and services (e.g., software, systems, maintenance, and networks).

The document focuses on the reduction of energy delivery systems' cybersecurity risk through use of security procurement language that calls for suppliers to work together with systems purchasers in managing known vulnerabilities. It includes a collection of security procurement provisions mapped to critical vulnerabilities observed in current and legacy control systems. The document identifies a series of topics, each addressing a particular control system security area of concern. Illustrative areas of focus include: system hardening; perimeter protection; malware detection and protection, remote access; physical security; network partitioning. For each such topic, the document provides:

- The basis of potential exposures/vulnerabilities associated with a problem;
- Guidance on procurement language and samples;
- Factory acceptance test measures;
- Site acceptance test measures;
- Maintenance guidelines;
- References (i.e., external supporting information, practices and standards); and
- Dependencies (i.e., internal topics that should be in concert with the topic).

7. Nuclear Regulatory Commission Regulations – 10 C.F.R. Part 50, Appendix B[46]

Nuclear Regulatory Commission (NRC) regulations require vendors to implement quality assurance programs meeting NRC requirements. Areas addressed in the regulations include:

- **Procurement Control:** Procurement documentation must address applicable regulatory requirements, design bases, and other requirements needed to assure adequate quality.

- **Control of Purchased Material, Equipment, and Services:** NRC regulations call for purchasers to establish measures assuring that purchased material, equipment, and services, whether purchased directly or through contractors and subcontractors, conform to the procurement documents. Prescribed measures include source evaluation and selection; objective evidence of quality furnished by suppliers; and inspection.

[46] 10 C.F.R. Part 50, Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants, available at https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appb.html.

8. ISO/IEC 27036 – Information technology — Security techniques — Information security for supplier relationships

ISO/IEC 27036 is a four-part international standard addressed to supplier security for information and information systems.

- Part 1 provides an overview and concepts of information security in supplier relationships.[47]

- Part 2 is a high-level framework for establishing information security requirements and expectations in supplier relationships. The framework includes governance, life cycle processes, and relevant high-level requirements statements.[48] These requirements also may serve as additional certification criteria for the purpose of ISO/IEC 27001 certification or other certification schemes used by the acquirer (e.g., an acquirer may require that a supplier be certified in accordance with ISO/IEC 27001 and include additional requirements and applicable controls in accordance with all or portions of ISO/IEC 27036.

- Part 3 provides guidelines to acquirers and suppliers for managing information security risks associated with the information and communication technology (ICT) products and services supply chain. It builds on the requirements in Part 2 and provides additional practices that augment the high-level requirements from Part 2.[49]

- Part 4 provides guidelines to vendors and customers for information security of cloud computing services.[50] It covers management of information security risks associated with cloud computing services throughout the supplier relationship lifecycle.

9. ISO/IEC 27001:2013 – Information technology — Security techniques — Information security management systems — Requirements[51]

ISO/IEC 27001 provides a framework through which an organization may identify, analyze and address information security risks. The standard enumerates the design for an Information

[47] ISO/IEC 27036-1:2014 - Information security for supplier relationships — Part 1: Overview and concepts, available at http://standards.iso.org/ittf/PubliclyAvailableStandards/c059648_ISO_IEC_27036-1_2014.zip.
[48] ISO/IEC 27036-2:2014 - Information security for supplier relationships — Part 2: Requirements, available for purchase at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=59680.
[49] ISO/IEC 27036-3:2013 - Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security, available for purchase at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59688.
[50] ISO/IEC 27036–4:2016 - Guidelines for security of cloud services, available for purchase at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59689&commid=45306.
[51] ISO/IEC 27001:2013 – Information technology — Security techniques — Information security management systems — Requirements, available for purchase at https://www.iso.org/standard/54534.html.

Security Management System, and can be used as the basis for a formal compliance assessment by accredited certification auditors.

10. NIST – Conformity Assessment[52]

NIST's conformity assessment is intended to ensure that the products, services, systems, etc. have certain required characteristics, and that these characteristics are consistent across products, services and systems. This assessment can come in the form of a supplier's declaration of conformity, or third-party certification or inspection. Some regulatory agencies in the U.S. use a supplier's declaration of conformity as a means of assuring compliance of a product/service with technical regulations (e.g., FCC regulation; motor vehicle standards; etc.).

VI. CONCLUSION

APPA and NRECA believe that, consistent with the NERC BOT's August 2017 resolution, this white paper will serve as a cybersecurity resource for small entities, specifically with regards to supply chain risk management. The paper provides smaller registered entities with a catalog of low-impact BES Cyber Systems best practices and additional resources they can consider using to either add or amend their existing programs. Moreover, APPA and NRECA have programs in place to support their members as they work to improve the cyber and physical security of their organizations, including procurement and supply chain issues.

The Associations believe that the supply chain risk management practices identified in this white paper, along with the additional resources available to Association members, will be a useful resource for small registered entities with low-impact BES Cyber Systems seeking to strengthen their supply chain risk management practices.

[52] NIST, Draft SP200-01: ABC's of Conformity Assessment (Dec. 2017), available at https://www.nist.gov/file/416646; NIST, Draft SP200-02: Conformity Assessment Considerations for Federal Agencies (Dec. 2017), available at https://www.nist.gov/file/416651.

APPENDIX I

APPA and NRECA, Member Descriptions and NERC Registrations

APPA is the national service organization representing the interests of the nation's 2,000 not-for-profit, community-owned electric utilities. Public power utilities account for 15 percent of all sales of electric energy (kilowatt-hours) to ultimate customers and collectively serve over 49 million people in every state except Hawaii. Approximately 261 public power utilities are registered entities subject to compliance with NERC mandatory reliability standards.
Of the public power utilities that are registered with NERC, most are distribution companies that may own some transmission or generation. The NERC registry functional breakdown of public power utilities for the 261 registered companies, is as follows:

Balancing Authority (BA)	30
Distribution Provider (DP)	212
Generation Owner (GO)	93
Generation Operator (GOP)	88
Planning Authority (PA)	20
Resource Planner (RP)	68
Reserve Sharing Group (RSG)	1
Transmission Owner (TO)	126
Transmission Operator (TOP)	55
Transmission Planner 2(TP)	57
Transmission Service Provider (TSP)	17

NRECA is the national service organization representing the interests of the nation's more than 900 not-for-profit, consumer-owned electric cooperatives. Electric cooperatives account for 13 percent of all sales of electric energy (kilowatt-hours) to ultimate customers and collectively serve over 42 million people in 47 states. Approximately 110 electric cooperatives are registered entities subject to compliance with NERC mandatory reliability standards.
Of the electric cooperatives that are registered with NERC, there are approximately 70 distribution and 40 generation and transmission cooperatives registered for various functions. The NERC registry functional breakdown of electric cooperatives for the approximately 110 registered companies, is as follows:

Balancing Authority (BA)	8
Distribution Provider (DP)	104
Generation Owner (GO)	36
Generation Operator (GOP)	30
Planning Authority (PA)	5
Resource Planner (RP)	28
Reserve Sharing Group (RSG)	1
Transmission Owner (TO)	59
Transmission Operator (TOP)	23
Transmission Planner (TP)	34
Transmission Service Provider (TSP)	13