EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Supply Chain Risk Assessment

Final Report

Supply Chain Risk Assessment

Final Report

July 2018

G. Rasche

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI) prepared this report.

G. Rasche

T. Whitney

B. Sooter

Report Title: Supply Chain Risk Assessment: Final Report

KEY RESEARCH QUESTION

The North American Electric Reliability Corporation (NERC) Board of Trustees requested NERC management to "(i)study the nature and complexity of cyber security supply chain risks, including risks associated with low impact assets not currently subject to the Supply Chain Standards, and develop recommendations for follow-up actions that will best address any issues identified, and (ii) NERC management provide an interim report to the Board related to the foregoing by no later than approximately 12 months after the adoption of these resolutions and a follow-up final report to the Board no later than approximately 18 months after the adoption of these resolutions." The objective of this project is to provide an independent analysis of these supply chain risks and develop recommendations for how the electric sector can address them.

RESEARCH OVERVIEW

EPRI performed this analysis by executing the following tasks:

1. Performing a Bulk Electric System (BES) product and manufacturer assessment.
2. Analyzing emerging vendor practices and industry standards.
3. Analyzing the applicability of the Critical Infrastructure Protection (CIP) standards to supply chain risks.
4. Developing recommendations for follow-up actions that will best address any issues identified.

KEY TAKEAWAYS

In summary, the analysis performed and documented in this report resulted in three categories of recommendations for further analysis and investigation:

- **Applying industry practices and guides:** EPRI identified 10 emerging practices that if applied effectively could reduce additional supply chain risks.
- **Understanding common-mode vulnerabilities for low-impact BES Cyber Systems (BCS):** EPRI recommended additional research to model and assess the impact of a common-mode exploits targeting multiple, geographically dispersed low-impact BCS to determine the extent of potential risk of a compromise in supply chain.
- **Assessing supply chain risk through data analysis to address the following topics:**
    - Pre-Audit surveys and questionnaires to help identify and assess industry practices
    - Targeted outreach to vendors that support the reliability of the Bulk Electric System
    - Development of standardized vendor supply chain practices
    - Independent testing of legacy applications and products

WHY THIS MATTERS

Modern industrial control systems, such as those in the electric power industry, have become more sophisticated and complex to deliver better services, deliver more cost-competitive products, and provide greater end-to-end, responsive control. With this evolution has come an increase in the complexity of the industrial supply chain and as well as additional interdependencies across suppliers and service providers. Managing the associated cyber security risks is critical for ensuring the reliability of the bulk electric system.

HOW TO APPLY RESULTS

This report identifies current supply chain risks for the bulk electric system and provides objective, technical recommendations to industry for mitigating risks as well as identifying areas for further analysis. The results may be used to examine current supply chain security processes and requirements to identify opportunities to reduce cyber security risk.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION AND BACKGROUND

According to a July 20, 2017 New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) report, "The NJCCIC assesses with high confidence that capable threat actors—both politically-motivated state actors and their proxies, as well as profit-driven criminals—will increasingly leverage supply chain compromises to conduct network intrusions and attacks. These incidents could result in the exfiltration, manipulation, or destruction of data and disruption to daily operations and business continuity" [1]. The difficulty of monitoring a supply chain that may include dozens of suppliers at multiple transaction levels is compounded by a lack of standardization or security integration between suppliers and buyers.

The root cause of escalating supply chain vulnerabilities lies in the increasing dependence on microelectronics, computer networks, and telecommunications. Modern industrial control systems, such as those in the electric power industry, have become more sophisticated and complex to deliver better services, deliver more cost-competitive products, and provide greater end-to-end, responsive control.

The enabling technologies for modernizing the electric power industry include some of the following infrastructure components:

- Hardware endpoint devices, system monitors, remote switches, and next-generation SCADA/remote telemetry units (RTU) based on programmable logic circuit (PLC), synchronous link control (SLC), and ASIC-based (application-specific integrated circuit) devices.

- Software for detecting and correcting errors in a power grid system, SCADA/ICS/RTU control and monitoring, PLC/SLC software interfaces, telecommunication/networking transports, and power system troubleshooting and analysis software tools.

On August 10, 2017, the NERC Board of Trustees approved the proposed Supply Chain Risk Management requirements: Cyber Security – Supply Chain Risk Management – CIP-005-6, CIP-010-3, and CIP-013-1. As part of the approval, the Board proposed additional resolutions for NERC to undertake [2].

The NERC Board of Trustees requested that NERC management "study the nature and complexity of cyber security supply chain risks, including risks associated with low impact assets not currently subject to the Supply Chain Standards, and develop recommendations for follow-up actions that will best address any issues identified, and (ii) NERC management provide an interim report to the Board related to the foregoing by no later than approximately 12 months after the adoption of these resolutions and a follow-up final report to the Board no later than approximately 18 months after the adoption of these resolutions."

The objective of this project is to support NERC in the development of its interim report through the following tasks:

1. Perform BES product and manufacturer assessment.

2. Analyze emerging vendor practices and industry standards.
3. Analyze the applicability of the critical infrastructure protection (CIP) standards to supply chain risks.
4. Develop recommendations for follow-up actions that will best address any issues identified.

2
MARKET DATA ASSESSMENT

The research activities under this task consist of assessing the product/manufacturer types used on the BES for the following areas: SCADA/control systems, network and telecommunications, and operating systems. The details of the market research market share data are from the following sources:

- Newton-Evan Research Company
- Other sources as sited in the References section of this report

By analyzing the numbers and comparing that data with the systems that are most likely tied to real-time applications as referenced in the NERC BES Cyber Asset Survey [3], the data provides insight as to the systems being currently[1] procured by asset owners and operators.

Market Share of Substation Networking Equipment

Although there appears to be a wide array of substation network equipment being purchased, half of the market share is held by only two vendors (Vendor 1 and Vendor 2). Further, Vendor 2 has a 55% world-wide enterprise network market share in the corporate environment of many industries in addition to the electric power industry.

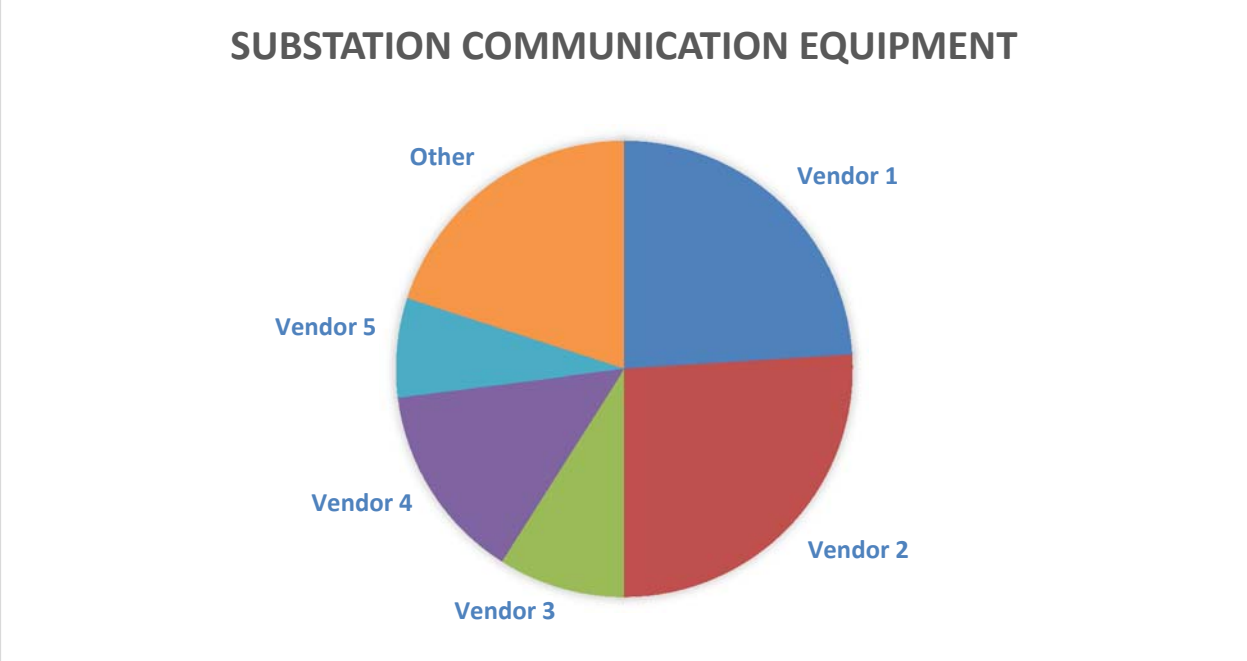

Figure 2-1
Substation communication equipment

[1] Newton-Evan Research Company research data is for equipment purchased in 2017.

Market Share of Operating Systems

The operating system used to govern BES Cyber Systems usually dictates the type of threats and vulnerabilities to which the systems are exposed. Based on the data, Microsoft Windows has an 87% market share.

As asset owners and operators develop their plans to manage supply chain risk it will be imperative that they give strong consideration to the high prevalence of systems that depend on a relatively small number of vendors and to determine the best means to address vendors that have a stake in their operations. However, asset owners and operators may find it more difficult to negotiate unique, industry-oriented or asset owner-oriented terms and conditions within procurement contracts with large multinational vendors. Unique terms may drive up product costs or cause delays in the procurement processes.

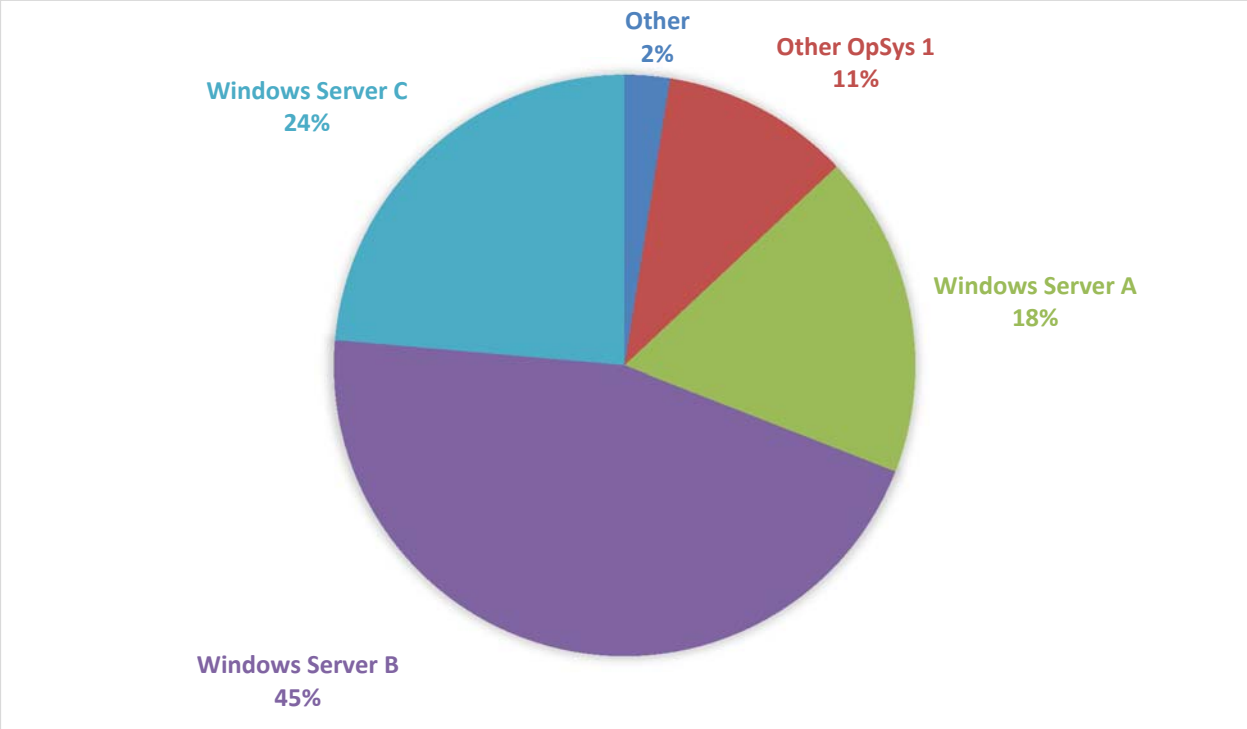

Figure 2-2
Operating systems

Market Share of Energy Management Systems

The energy-management system (EMS) platform is widely regarded as one of the most critical systems on the bulk electric system. If misused, it could result in significant damage to transmission equipment and potentially lengthy outages.

In general, EMS vendors have core customers that are primarily within the critical infrastructure sector, which means that from a supply chain risk management perspective, the electric power industry can expect reasonably responsive terms when negotiating security in comparison to vendors that may not have a primary focus in critical infrastructure. Another consideration is the limited variety of vendors that offer solutions in this category. If a vulnerability is introduced

into a critical supply chain within the system development lifecycle of one of the core vendor's in this category, the result could be significant to the reliability and security of the BES.

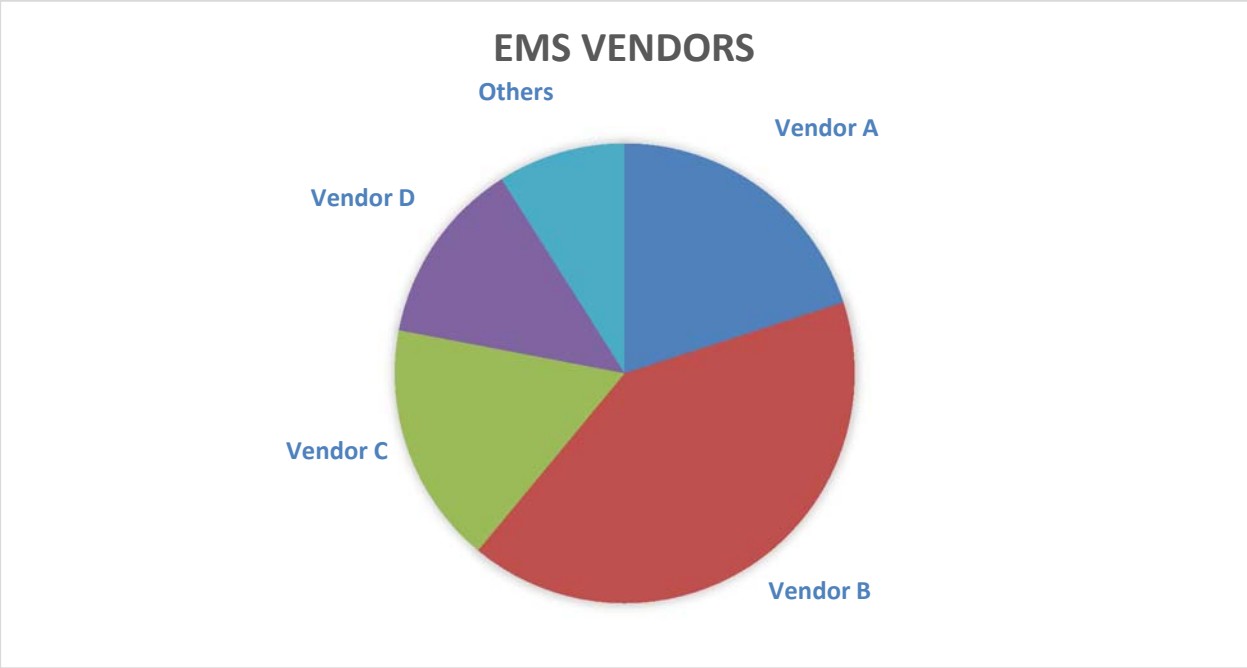

Figure 2-3
EMS vendors

Market Share of Remote Terminal Units

Remote terminal units (RTUs) are microprocessor-based devices that often perform the critical role of sending telemetry and control signals between field devices and supervisory control and data acquisition (SCADA) systems. An observation of note would be the variety of vendors in this category. No single vendor exceeds 20% market share, which is an indicator that a threat to the supply chain of SCADA systems would have a lower impact than that of the aforementioned categories.

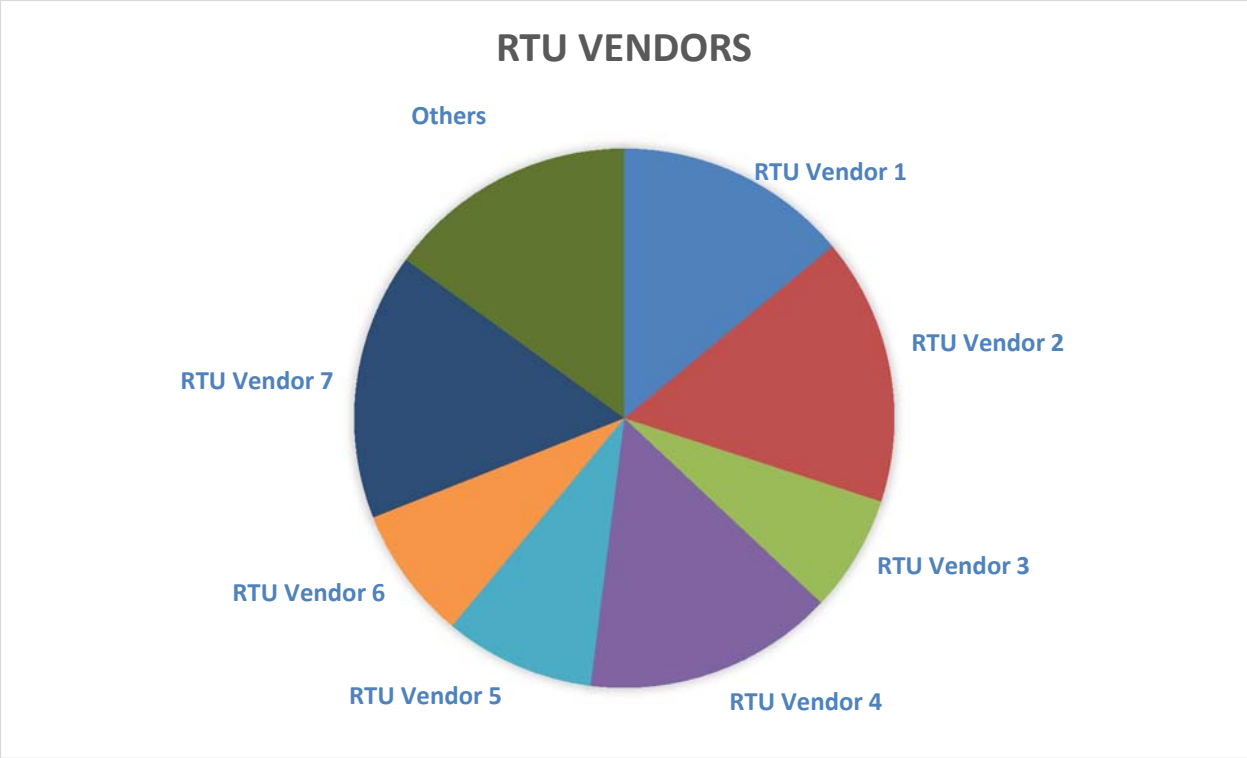

Figure 2-4
RTU vendors

3
ANALYZING VENDOR PRACTICES AND INDUSTRY STANDARDS

The research activities in this task consist of analyzing emerging best practices and standards used in other industries to mitigate supply chain risks. A key aspect of mitigating supply chain risk is ensuring that each of the product and service providers adhere to best practices and standards in security. Ultimately, it is the responsibility of both the purchaser and supplier to ensure that their security concerns are understood and that practices to mitigate risk are established. The CIP standards are designed to manage supply chain risk and consist of three core supply chain concepts:

- Development and implementation of plans and policies to manage supply chain risk (CIP-013-1)
- Testing and validation of software (CIP-005-6)
- Monitoring and control of vendor connections to BES Cyber Systems (CIP-010-3)

Although there are numerous security practices and guides applicable to many aspects of operation and information technology, this report focuses on specific standards, vendor practices, and guidelines for mitigating the risks shared by the purchaser and supplier of technologies and services. The most relevant supply chain practices and standards are referenced in Appendix B (including practices currently not considered in the scope of the CIP standards). Based on research performed on each standard or reference in Appendix B, several noteworthy approaches were identified.

1. Off-premise Supplier Services

In the scenario, where a supplier performs services for an entity involving BES Cyber Assets that are not on the Registered Entity's premises, the FedRAMP standards provide assurance to government entities and suppliers, such as cloud service providers. The ISO/IEC 27017, "Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services," specifies various requirements that recognize that cloud services are a type of supply chain risk. The following is stated in ISO/IEC 27017 regarding a way to address the risk of cloud service providers:

> *Cloud service customers and cloud service providers can also form a supply chain. Suppose that a cloud service provider provides an infrastructure capabilities type service. In addition, another cloud service provider can provide an application capabilities type service. In this case, the second cloud service provider is a cloud service customer with respect to the first, and a cloud service provider with respect to the cloud service customer using its service. This example illustrates the case where this Recommendation | International Standard applies to an organization both as a cloud service customer and as a cloud service provider. Because cloud service customers and cloud service providers form a supply chain through the design and implementation of*

the cloud service(s), clause "15.1.3 Information and communication technology supply chain" of ISO/IEC 27002 applies."

Although ISO/IEC 27017 is not widely adopted now, if asset owners and operators decide to move certain aspects of their operation off-premise, they should be aware of FedRAMP and the ISO/IEC 27017 standards.

2. Third-Party Accreditation Processes

Suppliers that provide products to various customers may use accredited standards that are independently verified. Standards such as FedRAMP, ISO9001, and ISO27001 use independent third parties to assess their adherence to established standards. The entities that are acquirers or purchasers of companies that have received accreditation may rely on the work of the independent auditors to manage supply chain risks. Currently, neither the CIP standards nor the NERC Rule of Procedures allow for vendors or suppliers (non-Registered Entities) to be audited via NERC or the Regional Entities. In the context of CIP compliance, a supplier or vendor may be audited only if they operate a CIP-applicable asset, but the audit results are applicable to only the Registered Entity. The Regional Audit reports are not provided to any entity other than the Registered Entity that is directly involved in the audit. It is worth consideration to determine methods to share the results of auditing vendor security with Registered Entities to address compliance to the CIP standards supply chain risk management. This concept is currently contemplated and encouraged in APPA's *Managing Supply Chain Risk-Best Practices for Small Entities* [4].

3. Secure Hardware Delivery

Many BES Cyber Assets purchased and deployed on the Bulk Electric System are hardware appliances that are configured to perform very specific real-time functions. The programming is often coupled tightly with the physical operation of the device. In those cases, it might be easy to overlook these types of appliances in the context of supply chain risk management. Appliances such as remote terminal units, switches, relays, or other intelligent electronic devices may not seem like software applications, but they often possess code that can be manipulated in a manner that causes them to misoperate in and potentially affect the BES. Recognizing this risk, the Energy Sector Control Systems Working Group (ESCSWG) that developed the Cybersecurity Procurement Language for Energy Delivery Systems identified controls for hardware delivery to help reduce the risk of compromise during transport:

3.6.1. The Supplier shall establish, document, and implement risk management practices for ICT supply chain delivery of hardware, software, and firmware. The Supplier shall provide documentation on its: • Chain-of-custody practices • Inventory management program (including the location and protection of spare parts) • Information protection practices • Integrity management program for components provided by sub-suppliers • Instructions on how to request replacement parts • Maintenance commitment to ensure that for a specified time into the future, spare parts shall be made available by the Supplier. The Supplier shall use trusted channels to ship critical energy delivery system hardware, such as U.S. registered mail.

4. Provenance

As referenced in NISTIR 7622, NIST 800-161, and other guidelines, provenance, or the ability to provide traceability in the supply chain processes and supplier relationships, improves transparency and improves vendor assessment processes. Provenance is described in NIST 7622 as follows:

Acquirers and their system integrators should maintain the provenance of systems and components under their control to understand where the systems and components originated, their change history while under government control, and who might have had an opportunity to change them. Provenance allows for changes from the baselines of systems and components to be reported to specific stakeholders. Creating and maintaining provenance within the ICT supply chain helps government agencies to achieve greater traceability in case of an adverse event and is critical for understanding and mitigating risks.

The concept of provenance is a central to concept of supply "chain" practices because each link or step in the supplier's process is provided within its provenance documentation. Some challenges with provenance controls may include the following:

- Clarity regarding what constitutes a component with a system
- Ambiguity regarding the authority which has the ability to enforce provenance controls
- Given the limited number of Bulk Electric System vendors in certain market categories, provenance requirement may have diminishing value, due to similarity of supply chains for various entities being supplied by the same vendor

5. Threat Modeling

Threat modeling as described by the IEC 62443-4-1 Secure Product Development Life-Cycle Requirements is "…a process shall be employed to ensure that all products shall 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 Bulk electric System. EPRI applied part of its risk management and supply chain guidance, Technical Assessment Methodology[2], from the threat modeling concept. For instance, if an entity was procuring a new remote access system to its medium-impact substations, the threat model should reflect the impact of the remote access system's effect to the BES, and the requirements for that purchase should be applied according to its elevated risk and system-specific vulnerabilities.

6. Assessing Supply Chain Deficiencies

NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition, Section SA-12 (15) states:

[2] https://www.epri.com/#/pages/product/3002008023/?lang=en

> *The organization establishes a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.*

Clearly 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. By using this method of mitigating risk by identifying key process deficiencies, asset owners and operators may decrease their supply risk by implementing timely organizational assessments.

7. Recognizing External Dependencies

The Department of Energy's Cyber Security Capabilities Maturity Model (C2M2) highlights manners to assess the effectiveness of various security processes within utility organizations. One aspect considered by the 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 the entity's ability to highlight and mitigate supply chain risks. The C2M2 adds:

> *Supply chain risk is a noteworthy example of a supplier dependency. The cybersecurity characteristics of products and services vary widely. Without proper risk management, they pose serious threats, including software of unknown provenance and counterfeit (possibly malicious) hardware. Organizations' requests for proposal often give suppliers of high-technology systems, devices, and services only rough specifications, which may lack adequate requirements for security and quality assurance.*

8. Policy for Handling Supplied Products or Services That Do Not Adhere to Procurement Processes

The U.S. Nuclear Regulatory Commission (NRC) identified processes to manage supplier risks. In its standard, the NRC considered a control to mitigate risks when products or services are supplied that do not adhere to supply chain policies. The NRC recognizes that companies may introduce third-party supplied systems that may not fully adhere to policy but still provides a transparent method to mitigate risks in those events. The NRC states the following in Appendix B, Part 50, Article XV:

> *Measures shall be established to control materials, parts, or components which do not conform to requirements in order to prevent their inadvertent use or installation. These measures shall include, as appropriate, procedures for identification, documentation, segregation, disposition, and notification to affected organizations. Nonconforming items shall be reviewed and accepted, rejected, repaired or reworked in accordance with documented procedures.*

9. Unsupported or Open-Sourced Technology Components

Although the grid is constantly being modernized by the addition of various technologies, there are still legacy systems that are not supported by a vendor. In these cases, it does not mean the supply chain risk management plan is not applicable to these systems. Instead, different processes must be considered to effectively mitigate their risk while updating systems or system

components during the end-of-life phase of the product. NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition states the following regarding unsupported system components:

> *The organization: a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.*

The concept of replacing or developing a plan for an unsupported system or system components is a vital aspect of grid security. Currently CIP-007's Patch Management requirement does not mandate that any compensating controls are implemented when a patch source is not available (i.e. the system is no longer supported). If these systems are left unchecked, significant risk could remain unmitigated on the BES.

Related to products that are not supported by the vendor, many products are based on open sourced applications. The Open Group[3] created a set of standards and certification processes titled the "Open Trusted Technology Provider™ Standard (O-TTPS) Certification Program." The O-TTPS standard identifies several supply chain-related controls for purchasers. One of its standards addresses open-sourced providers and requires the following in Section 4.2.1.10 of the O-TTPS and ISO/IEC 20243:2015:

> *In the management of Open Source assets and artifacts, components sourced shall be identified as derived from well-understood component lineage.*
>
> *In the management of Open Source assets and artifacts, components sourced shall be subject to well-defined acceptance procedures that include asset and artifact security and integrity before their use within a product.*
>
> *For such sourced components, responsibilities for ongoing support and patching shall be clearly understood.*

10. Concluding Supplier Relationships

An important aspect of managing suppliers is knowing how to terminate relationships with third parties in manner that limits the operational impact of losing the product or service. The UTC's "Supply Chain Risk Management for Utilities" paper highlights approaches that utilities can consider when concluding the supplier relationship. On page 13, it states the following:

> *[U]tilities need to be very conscious of organizing supplier relationship termination processes that minimize security risks after the relationship is completed. Specifically, utilities should ensure that the ending of a relationship with a supplier that involves a transition between different suppliers or from a supplier to the utility involves an organized transition plan where the current supplier's responsibilities and activities are assumed by the receiving party.*

[3] https://ottps-cert.opengroup.org/

4
COMPARING MARKET DATA AND PRACTICES TO THE CIP SUPPLY CHAIN STANDARDS

The research activities in this task consist of analyzing the results of the market assessment in Task 1 to compare the supply chain risk of different categories of NERC applicable systems such as:

- High and Medium Impact BES Cyber Systems (BCS)
- Electronic Access Control or Monitoring Systems (EACMS)
- Physical Access Control Systems (PACS)
- Low Impact BES Cyber Systems (BCS)

Applicability of the Supply Chain Standards to the Bulk Electric System

The CIP Standards are applicable to three categories of assets on the Bulk Electric System (BES): high, medium, and low. The *high* and *medium* impact categories have the most requirements, while *low* impact has the least. The Supply Chain Standard (CIP-013-1) is applicable to high and medium impact categories BES Cyber Systems only. Figure 4-1 (created from data supplied by NERC) shows that roughly 21% of the BES, or 270 Registered Entities, have either high or medium impact BES Cyber Systems. The remaining 79% of the assets, or 992 Registered Entities, are low impact and are not applicable to the supply chain requirements.

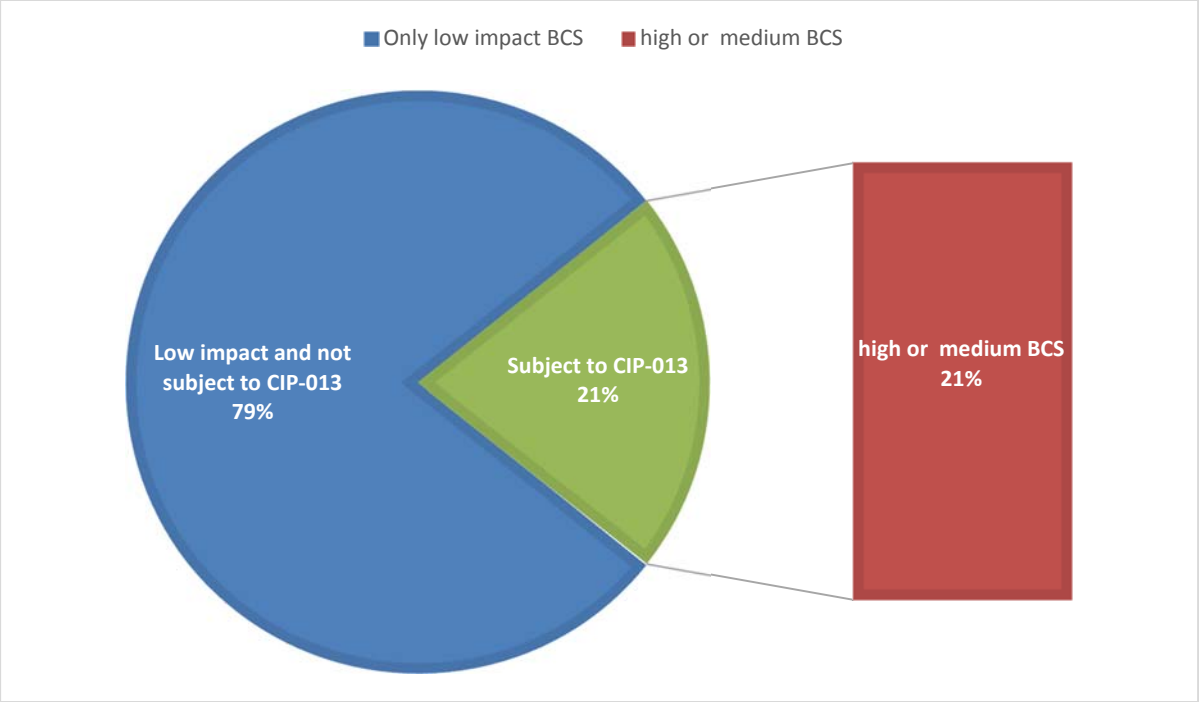

Figure 4-1
1262 Registered Entities have BCS

Understanding the Risk Basis of the CIP Standards

The CIP Standards employ an asset-centric, risk-based approach to securing the BES. This approach requires systems or facilities that have the highest impact to the grid receive the highest level of protections. Conversely, the lowest impact categories receive the fewest security requirements. This concept may mitigate the risk of threat actors targeting specific assets or electric power entities because of their potential impact to the grid. Threats originating from supply chain vulnerabilities, however, may challenge this asset-centric approach. If a major vendor with sizeable market share unintentionally supplies a compromised product to a sizeable percentage of the industry, the impact to the reliability of the BES could be significant because the vendor may supply hundreds of products at all impact categories. This type of compromise may result in the aggregate risk of misuse to numerous low impact BES Cyber Systems, which could potentially equal the impact of the compromise of any single high or medium impact BES Cyber System. This type of risk is described as a "common-mode vulnerability," where a single configuration-based vulnerability reaches exposure to large quantities of similarly configured devices. Many risks associated with cyber threats have common-mode vulnerabilities. Virus, worms, and malware programs work in this manner. Given that 79% of the Registered Entities possessing BES cyber systems are not applicable to the supply chain standard, future assessments of the effectiveness of requirements related to the supply chain should be considered to evaluate how well the supply chain requirements have a "trickle-down" effect into the low-impact categories of BES Cyber Systems.

Supply Chain Risk Considerations for CIP Applicable Assets

While the Supply Chain requirements are applicable to high and medium BES Cyber Systems, they are currently not applicable to all types of CIP applicable systems within the high- and medium-impact categories. Table 4-1 summarizes the applicability of the supply chain standards based on the various CIP asset categories. Blue boxes indicate that the asset category is subject to the referenced standards. The white boxes are not subject to the referenced standards.

Table 4-1
CIP Asset Categories

Requirement	CIP-013-1	CIP-005-6 R2.4	CIP-010-3 R1.6
High Impact BES Cyber Systems			
High Impact Protected Cyber Asset			
High Impact Physical Access Control Systems			
High Impact EACMS			

Medium Impact BES Cyber Systems			
Medium Impact Protected Cyber Asset			
Medium Impact Physical Access Control Systems			
Medium Impact EACMS			

Processes-Based Procurement Requirements

The supply chain requirements are applicable to BES Cyber Systems at the high and medium impact categories. CIP-013-1 requires the following:

> *R1: Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include:*
>
> > *1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*
> >
> > *1.2. One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:*
> >
> > > *1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*
> > >
> > > *1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;*
> > >
> > > *1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*
> > >
> > > *1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;*
> > >
> > > *1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and*
> > >
> > > *1.2.6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).*

R2: Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

It is important to note that the standard is not stating that every BES Cyber System should be procured in a certain manner with specific controls. Rather, the standard is requiring Registered Entities to institute processes in the procurement function to ensure the required elements are being addressed by their vendors. While the standard is only applicable to asset owners that have BES cyber systems at high and medium impact categories, the supply chain processes can easily be ported to all applicable asset types that may have an impact on the Bulk Electric System. The asset categories that are not included in the scope of the Supply Chain requirements are EACMS, PACS, and Protected Cyber Assets (PCAs).

PCAs are difficult to assess their risk generically. PCAs are often servers or networking equipment that resides on the same network as BES Cyber System. From a procurement language perspective, negotiating supply chain security requirements would be highly dependent on the system in question and its risk to other BES Cyber Systems. Entities may need to assess the risk of PCAs on a case-by-case basis to determine whether procurement processes are needed to mitigate the risk of associated BES cyber systems.

The systems that make up EACMS and PACS often are the systems used to secure and monitor the most critical systems on the BES. These types include firewalls, routers, switches, intrusion-detection systems, log monitors, and access control systems. Depending on specific configurations, EACMs or PACS systems—if compromised, misused or rendered unavailable—could have a real-time impact on the reliability and security of the bulk electric system. For instance, if a firewall used to protect BES Cyber Systems within an Electronic Security Perimeter (ESP) was compromised due to supply chain vulnerability, each system within the ESP could be exposed due to its logical proximity to the compromised firewalls. This scenario is common among many of the EACMS types of assets, therefore Registered Entities—regardless of impact level or CIP applicable asset type—should consider applying the same process-based controls to procurement processes uniformly across various cyber assets.

5
SUMMARY AND ANALYSIS OF CONCLUSIONS

In summary, the analysis performed and documented in this report concluded three categories of recommendations for further analysis and investigation:

- Applying industry practices and guidelines.
- Mitigating the risk of common-mode vulnerabilities for low-impact BES Cyber Systems.
- Assessing risk through data analysis.

Applying Industry Practices and Guidelines

Section 3 identified noteworthy techniques that are not required by the CIP standards. While the CIP standards addresses many fundamental elements of effective processes to manage the risk of a supply chain, the following four noteworthy approaches, if applied correctly, can reduce residual supply chain risks:

- Third-Party Accreditation Processes – verifying that standardized processes and measures were achieved to mitigate supplier risks.
- Secure Hardware Delivery – protecting hardware and software during physical transport.
- Threat-Informed Procurement Language – tailoring security specifications to the specific risk of the purchaser's environment.
- Unsupported or Open-Sourced Technology Component Processes – to mitigate residual risks for patch/vulnerability management processes for unsupported systems.

Using Supply Chain Controls to Mitigate Common-Mode Vulnerabilities

In conclusion, the existing CIP 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. The supply chain standards will be applied to the highest-risk systems that have the greatest impact to the grid. Additional consideration may need to be given to processes to ensure that vendors and entities are applying techniques to mitigate supply chain risk to lower impact levels. Risks of common-mode vulnerabilities, as described in Section 4, can be mitigated if supply chain security practices are applied uniformly across cyber asset types. Uniform application of supply chain security practices may also mitigate the risk of EACMS and PACS vulnerabilities. To more fully assess the risk of common-mode vulnerabilities and the CIP standards, the following points of analysis should be considered:

- Identify the types and quantities of vendor-supplied products used as BES Cyber Systems.

- Research and model the impact of a common-mode exploits targeting multiple, geographically dispersed low-impact BCS to determine the extent of potential risk.

- Direct, targeted outreach to those vendors that have the largest potential risk to the grid irrespective of BES Cyber System impact level.

Going Forward: Assessing the Risks Through Data Analysis

Although the standard has not been approved by FERC during the time of this study, EPRI identified methods to obtain additional information for future evaluation, so that prior to any changes in regulatory policy, data can be obtained, assessed, and discussed in a transparent manner. The following information-gathering methods should be considered to address the recommendations included in this report:

- **Pre-Audit Surveys and Questionnaires to Help Identify and Assess Industry Practices** – Voluntary efforts to obtain risk data in the preliminary stages of Compliance, Monitoring & Enforcement Program activities can be used to obtain information about the (1) installed base of systems used on the BES, (2) procurement language in contracts negotiated with key vendors, and (3) data describing which CIP applicable systems have benefited from procurement language stemming from the CIP supply chain standards.

- **Targeted Outreach to Vendors that Support the Reliability of the Bulk Electric System** – Based on the Market Data Assessment performed in Section 2, 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 customer's responsibility to meet the rigor required by the CIP standards. It is encouraged that industry work with their vendor points of contacts to ensure that technical and contractual considerations are addressing the CIP 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. EPRI encourages the work of the Critical Infrastructure Protection Committee to develop an open letter to vendors about the CIP standards and recommends that further consideration 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.

- **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 bulk-electric systems 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 and implementations of green-field system.

6
REFERENCES

1. New Jersey Cyber Security & Communications Integration Cell (NJCCIC), "Supply Chain: Compromise of Third-Parties Poses Increasing Risk." Accessed July 20, 2017, https://www.cyber.nj.gov/threat-analysis/supply-chain-compromise-of-third-parties-poses-increasing-risk.
2. NERC, "Proposed Additional Resolutions for Agenda Item 9.a: Cyber Security– Supply Chain Risk" http://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf.
3. NERC, "Informational Filing of the North American Electric Reliability Corporation Regarding The Bes Cyber Asset Survey." https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Info_Filing-BES_Cyber_Asset_Survey_RM13-5_02032015.pdf.
4. APPA and NRECA, "Managing Supply Chain Risk-Best Practices for Small Entities." Accessed April 25, 2018, https://www.cooperative.com/programs-services/government-relations/regulatory-issues/documents/supply%20chain%20white%20paper%204-25%20final.pdf.
5. "Overview of the 2017-2020 U.S. Transmission and Distribution Equipment Market: Substation Automation Series Complete Set." Newton-Evans Research Company, Ellicott City, MD: 2018.
6. "Overview of the 2017-2020 U.S. Transmission and Distribution Equipment Market: Control Systems Series Complete Set." Newton-Evans Research Company, Ellicott City, MD: 2018.
7. "Market Share of Enterprise Networks Vendors Worldwide in 2015 and 2017." Statista. 2018. https://www.statista.com/statistics/540779/enterprise-network-market-share-by-vendor/
8. Gartner, G. Keizer. "Windows Comes Up Third in OS Clash Two Years Early." *ComputerWorld,* 2016. https://www.computerworld.com/article/3050931/microsoft-windows/windows-comes-up-third-in-os-clash-two-years-early.html
9. "Desktop Operating System Market Share Worldwide." Statcounter, Dublin, Ireland: 2018. http://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-201803-201803-bar
10. "Usage of Operating Systems for Websites." W3Techs. Austria: 2018. https://w3techs.com/technologies/overview/operating_system/all
11. P. Tsai. "Server Virtualization and OS Trends." Spiceworks Austin, TX:2016. https://community.spiceworks.com/networking/articles/2462-server-virtualization-and-os-trends

A
APPLICABLE STANDARDS

Standard Name/Reference	Description/Topic	Notable Content
Federal Risk and Authorization Management Program (FedRAMP)	A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.	3PAOs play a critical role in the FedRAMP security assessment process, as they are the independent assessment organizations that verify cloud providers' security implementations and provide the overall risk posture of a cloud environment for a security authorization decision. These assessment organizations must demonstrate independence and the technical competence required to test security implementations and collect representative evidence. 3PAOs must: § Plan and perform security assessments of CSP systems § Review security package artifacts in accordance with FedRAMP requirements
ISO9001: Quality Management Systems	Specific sections of the standard contain information on topics such as: • Requirements for a quality management system, including documented information, planning and determining process interactions • Responsibilities of management • Management of resources, including human resources and an organization's work environment • Product realization, including the steps from design to delivery • Measurement, analysis, and improvement of the QMS through activities like internal audits and	3rd party accreditation process and independent verifications of entities.

Standard Name/Reference	Description/Topic	Notable Content
	corrective and preventive action	
ISO/IEC 27017 Information Security Management Systems	Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.	Section 4.2: “Cloud service customers and cloud service providers can also form a supply chain. Suppose that a cloud service provider provides an infrastructure capabilities type service. In addition, another cloud service provider can provide an application capabilities type service. In this case, the second cloud service provider is a cloud service customer with respect to the first, and a cloud service provider with respect to the cloud service customer using its service. This example illustrates the case where this Recommendation | International Standard applies to an organization both as a cloud service customer and as a cloud service provider. Because cloud service customers and cloud service providers form a supply chain through the design and implementation of the cloud service(s), clause "15.1.3 Information and communication technology supply chain" of ISO/IEC 27002 applies.”
ISO/IEC 20243 Open Trusted Technology ProviderTM Standard (O-TTPS) -- Mitigating maliciously tainted and counterfeit products	A standard of The Open Group, provides a set of guidelines, recommendations and requirements that help assure against maliciously tainted and counterfeit products throughout commercial off-the-shelf (COTS) information and communication technology (ICT) product lifecycles. *Mitigating Maliciously Tainted and Counterfeit Products*) that addresses supply-chain security and secure engineering.	Open Source Handling *4.2.1.10*- Open Source components are managed as defined by the best practices within the O-TTPS for Product Development/ Engineering methods and Secure Development/Engineering methods. The O-TTPS is an open standard containing a set of organizational guidelines, requirements, and recommendations for integrators, providers, and component suppliers to enhance the security of the global supply chain and the integrity of commercial off-the-shelf (COTS) information and communication technology (ICT).

Standard Name/Reference	Description/Topic	Notable Content
Energy Sector Control Systems Working Group (ESCSWG) - Cybersecurity Procurement Language for Energy Delivery Systems	DOE sponsored guidance documented focused on two areas: • The cybersecurity-related procurement language in this document is intended for use by Acquirers, Integrators, and Suppliers. • The procurement language presented in this document is not intended to be inserted (or attached) directly or verbatim into a procurement contract. The Acquirer and Supplier will need to involve their respective contracting offices in selecting and customizing their procurement contract language.	Section 3.6 Secure Hardware Delivery – 3.6.1. The Supplier shall establish, document, and implement risk management practices for ICT supply chain delivery of hardware, software, and firmware. The Supplier shall provide documentation on its: • Chain-of-custody practices • Inventory management program (including the location and protection of spare parts) 28 • Information protection practices • Integrity management program for components provided by sub-suppliers • Instructions on how to request replacement parts • Maintenance commitment to ensure that for a specified time into the future, spare parts shall be made available by the Supplier The Supplier shall use trusted channels to ship critical energy delivery system hardware, such as U.S. registered mail.
NISTIR 7622 - Notional Supply Chain Risk Management Practices for Federal Information Systems	Purpose: to provide federal departments and agencies with a notional set of repeatable and commercially reasonable supply chain assurance methods and practices that offer a means to obtain an understanding of, and visibility throughout, the supply chain.	Section 4.3: Establish and Maintain the Provenance of Elements, Processes, Tools, and Data “Provenance can be achieved through both physical and logical techniques, such as Configuration Management (CM) for tracking changes to the elements and documenting the individuals who approved and executed these changes; robust identity management and access control to establish and record authorized or unauthorized activities or behaviors; and identification/tagging of elements, processes, roles, organizations, data, and tools.”
NIST SP 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations	Acquirers and their system integrators should maintain the provenance of systems and components under their control to understand where the systems and components originated, their change history while under government control,

Standard Name/Reference	Description/Topic	Notable Content
		and who might have had an opportunity to change them. Provenance allows for changes from the baselines of systems and components to be reported to specific stakeholders. Creating and maintaining provenance within the ICT supply chain helps government agencies to achieve greater traceability in case of an adverse event and is critical for understanding and mitigating risks.
IEC 62443-4-1 Secure Product Development Life-Cycle Requirements	It defines a secure development life-cycle (SDL) for the purpose of developing and maintaining secure products. This life-cycle includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life.	Section 6.3.1: A process shall be employed to ensure that all products shall have a threat model specific to the current development scope of the product The implementation processes shall incorporate security coding standards that are periodically reviewed and updated and include at a minimum: a) avoidance of potentially exploitable implementation constructs – implementation design patterns that are known to have security weaknesses; b) avoidance of banned functions and coding constructs/design patterns – software functions and design patterns that should not be used because they have known security weaknesses; c) automated tool use and settings (for example, for static analysis tools); d) secure coding practices; e) validation of all inputs that cross trust boundary. f) error handling

Standard Name/Reference	Description/Topic	Notable Content
ISO/IEC SO/IEC 27036-1 – Information Security in Supplier Relationships	Provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships.	Provides cloud service customers and cloud service providers with guidance on a) gaining visibility into the information security risks associated with the use of cloud services and managing those risks effectively, and b) responding to risks specific to the acquisition or provision of cloud services that can have an information security impact on organizations using these services.
NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition	SA-12 – Supply Chain Protection SA-3 - System Development Life Cycle SA-22 Unsupported System Components	Section SA-12 (15): The organization establishes a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements. Section SA-22 UNSUPPORTED SYSTEM COMPONENTS Control: The organization: a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.
UTC Supply Chain Risk Management for Utilities	A roadmap tailored to the utility space on how to successfully organize supplier management activities while addressing associated security risks. It is based on practical experience, numerous discussions with utilities and vendors, and recently published	Concluding supplier relationships Pg 13: “utilities need to be very conscious of organizing supplier relationship termination processes that minimize security risks after the

Standard Name/Reference	Description/Topic	Notable Content
	standards and best practice documents	relationship is completed. Specifically, utilities should ensure that the ending of a relationship with a supplier that involves a transition between different suppliers or from a supplier to the utility involves an organized transition plan where the current supplier's responsibilities and activities are assumed by the receiving party"
APPA Managing Supply Chain Risk-Best Practices for Small Entities	Summary of the best practices that are currently in use by one or more of their small members that have only low-impact BES Cyber Systems.	Best Practice B5: Third-party accreditation and vendor self-certification would improve the ability of all entities, particularly small registered entities, to select reliable vendors.
DOE C2M2	C2M2 is a public-private partnership effort that was established as a result of the Administration's efforts to improve electricity subsector cybersecurity capabilities, and to understand the cybersecurity posture of the grid. The C2M2 helps organizations—regardless of size, type, or industry—evaluate, prioritize, and improve their own cybersecurity capabilities. Supply Chain and External Dependencies Management	Pg:. 39: The Supply Chain and External Dependencies Management (EDM) domain comprises three objectives: 1. Identify Dependencies 2. Manage Dependency Risk 3. Management Activities Of note: the C2M2 focuses on identifying dependencies where suppliers provide a critical function to operations.
US Nuclear Regulatory Commission Appendix B Part 50	Control of Purchased Material, Equipment, and Services Measures shall be established to assure that purchased material, equipment, and services, whether purchased directly or through contractors and subcontractors, conform to the procurement documents.	Policy for handling supplied products or services that do not adhere to procurement processes: XV. Nonconforming Materials, Parts, or Components Measures shall be established to control materials, parts, or components which do not conform to requirements in order to prevent their inadvertent use or installation. These measures shall include, as appropriate, procedures for

Standard Name/Reference	Description/Topic	Notable Content
		identification, documentation, segregation, disposition, and notification to affected organizations. Nonconforming items shall be reviewed and accepted, rejected, repaired or reworked in accordance with documented procedures.

B
EXAMPLE VENDOR PRACTICES

Cisco

https://www.cisco.com/c/en/us/about/trust-center/gdpr.html#~tab-ourcommitment

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/building-trustworthy-systems-with-CSDL.pdf?dtid=osscdc000283

Microsoft

https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx

OSI

http://www.osii.com/solutions/technology/architecture.asp

ABB

https://www.nerc.com/pa/comp/Supply%20Chain%20Webinars%20DL/Supply%20Chain%20Webinar.pdf

https://new.abb.com/about/supplying/cyber-security

https://new.abb.com/about/technology/cyber-security

GE

http://www.gesustainability.com/building-things-that-matter/supply-chain/

http://www.gesustainability.com/how-ge-works/integrity-compliance/privacy-cyber-security/

Siemens

https://www.siemens.com/global/en/home/company/about/corporate-functions/supply-chain-management/collaborating-with-siemens/supplier-management.html

SEL

https://cdn.selinc.com/assets/Literature/Product%20Literature/Flyers/SecureSupplyChain_PF00551.pdf?v=20161219-111622

C
MARKET DATA ABBREVIATIONS

BCS	Bulk Electric System Cyber System
BES	Bulk Electric System
CIP	Critical Infrastructure Protection
COTS	Commercial off-the-shelf
C2M2	Cybersecurity Capability Maturity Model
DMS	Distribution Management System
ESP	Electronic Security Perimeter
EMS	Energy Management System
EACMS	Electronic Access Control or Monitoring Systems
FERC	Federal Energy Regulatory Commission
HMI	Human Machine Interface
ICS	Industrial Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information technology
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NRC	Nuclear Regulatory Commission
NERC	North American Electric Reliability Corporation
OT	Operations technology
O-TTPS	Open Trusted Technology Provider™ Standard

PACS	Physical Access Control System
RTAC	Real-Time Automation Controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management
VM	Virtual Machine

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com