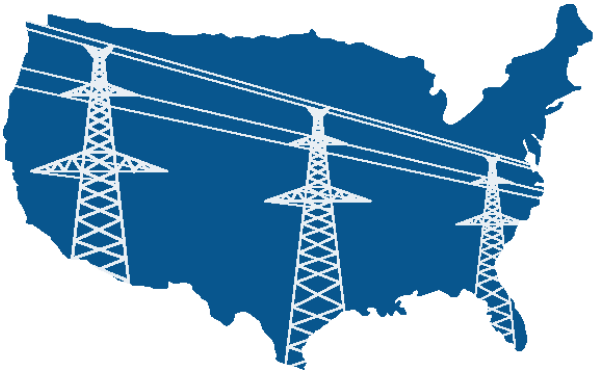
Prepared for: Protect Our Power

February 20, 2020



PROTECT OUR POWER

A Review of Power Industry's Supply Chain Security Risks

Author: **Robert Stephan**

Contributing Author: **Governor Tom Ridge**

RIDGE GLOBAL

ACKNOWLEDGEMENTS

PROTECT OUR POWER

Protect Our Power is a nonprofit, nonpartisan organization. It is comprised of experts from industry, the physical and cyber defense communities as well as finance and government. The advisory panel has a single focus of strengthening the nation's electrical power grid.

Members of the advisory panel for Protect Our Power that contributed to the direction and content of this report include:

Richard S. Mroz
James Cunningham
John Lang
Steve Naumann

RIDGE GLOBAL

Ridge Global was founded by Tom Ridge, the first U.S. Secretary of Homeland Security and 43rd Governor of Pennsylvania, to help organizations decrease security risks and to help build more resilient organizations through innovative preparedness, protection, response and education.

ABOUT THE AUTHORS

ROBERT STEPHAN

Mr. Robert Stephan previously served as Assistant Secretary of Homeland Security for Infrastructure Protection and has done extensive work with the electric industry as a private consultant following his 30-year government career.

GOVERNOR TOM RIDGE

Following the tragic events of September 11th, 2001, Tom Ridge became the first Assistant to the President for Homeland Security and later became the first Secretary of the U.S. Department of Homeland Security. The creation of the country's 15th Cabinet Department marked the largest reorganization of government since the Truman administration and another call to service for the former soldier, congressman and governor of Pennsylvania.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.0 EXECUTIVE SUMMARY

Various studies and reports commissioned in recent years by government, industry, and academia highlight the ever-increasing threats to the cyber influenced service supply chains that support the U.S. electric industry. Collectively, this body of knowledge also has called attention to a complex and diverse set of vulnerabilities and risk management challenges across these cyber influenced supply chains. These current and projected future threats and vulnerabilities vary greatly in terms of complexity, sophistication, and potential impacts. In the aggregate, they represent a clear and present danger to our national security and economy and the well-being of our citizenry.

This report provides a comprehensive assessment of the current "state of play" of cyber supply chain risk management within the U.S. electric industry from both a regulatory and non-regulatory perspective, along with a set of recommendations to address ongoing risks and challenges.

The report begins with a multi-factor assessment of the cyber supply chain risk environment — including both "buyer" and "supplier" perspectives – in the context of threat actors and vectors, the ever-increasing complexity of global supply chains, the growing convergence of the Information Technology (IT) and Operational Technology (OT) environments within the industry, and the advent of the Smart Grid including the evolution of key technologies that support local power distribution.

In consideration of these interrelated risk and operating environments, Section 4.0 of the report presents a notional "end-to-end" model framework for cyber supply chain risk management, applicable in the context of both "buyers" and "suppliers." This framework is designed to cover the "life-cycle" of a given cyber product or service and is based on a comprehensive review and compilation of cyber supply chain best practices recommended by various government agencies, industry associations, joint government-industry working forums, and vendor companies. This framework is intended to provide a comprehensive baseline against which various regulatory requirements and ongoing voluntary and collaborative activities designed to enhance cyber supply chain risk management within the U.S. electric industry can be objectively evaluated. The results of this evaluation – including answers to two principal questions that underpin the current report ("What's been done?" and "What are the remaining priority challenges and corresponding potential solutions?) – are documented in Sections 5.0-8.0 of the report.

Section 5.0 provides a summary of regulatory actions approved for implementation or currently under development that are designed to address cyber supply chain risk issues within certain segments of the U.S. electric industry (e.g., high and medium risk Bulk Electric System (BES) Cyber Systems). Also provided is an analysis of the major risk issues covered by current or proposed regulatory activities as well as the principal challenges that lie outside the scope of regulation.

Section 6.0 discusses voluntary activities being undertaken by various government agencies and a variety of entities within the U.S. electric industry – both independently and in collaboration with one another – to identify and address cyber supply chain risk management challenges that go beyond the North American Electric Corporation (NERC) regulatory baseline. These activities are relevant across all levels of BES Cyber Systems as well as local power distribution systems and their vendor supply chains.

Section 7.0 notes that cyber supply chain risk and corresponding risk management challenges are an increasingly common concern across government and other industry sectors beyond the electric industry. Accordingly, a variety of government agencies and other industries that face significant cyber supply chain risks have worked to develop, adopt, and implement standards and best practices designed to address such risks. This section presents a summation of various standards and best practices in use elsewhere that may offer solution paths to address gaps in cyber supply chain risk management not covered under the approved regulatory construct for the U.S. electric industry.

Section 8.0 discusses the notion that vendors themselves have become increasingly aware of the need to ramp up life-cycle management of the cyber supply chain risks they present. Key drivers include both recognition of the direction in which buyers are moving, as well as the need to mitigate the risks they face from sub-tier suppliers across their own supply chains. Accordingly, many vendors have pursued actions to address their cyber supply chain risk profiles, get ahead of the ball regarding compliance with more robust buyer screening and contracting requirements, and recognize and manage the risks inherent in their own cyber product and service supply chains. This section presents a number of industry case studies that employ best practices for cyber supply chain risk mitigation aligned to the model framework detailed in Section 4.0.

Section 9.0 draws from the information and analysis provided in Sections 5.0-8.0 to outline a broad-based set of recommendations to tackle key issues and challenges not addressed by or that fall outside the scope of the NERC Supply Chain Standards. These recommendations are generally relevant across all levels of the BES Cyber System (e.g., high, medium, and low impact) and local power distribution system communities. A summary of these recommendations organized by core component of the model framework presented in Section 4.0 is provided in Figure 1 below.

Figure 1. Summary of Recommendations

- ✓ Component 1: Establish Corporate Governance and Set the Direction for Cyber Supply Chain Risk Management
  - Develop a set of best practices-based considerations regarding corporate governance, oversight, and policy for cyber supply chain risk management.
  - Develop enterprise awareness, education, and training programs for cyber supply chain risk management.
  - Incorporate cyber supply chain risk considerations into company- and sector-level exercise activities.
- ✓ Component 2: Establish and Maintain Multi-dimensional Information Sharing Partnerships and Technical Capabilities
  - Expand industry "buyer" and "supplier" participation in important cyber threat and multi-dimensional public-private information sharing partnerships.
  - Support continued expansion of specific government-industry collaboration and information sharing programs to jointly address cyber supply chain risk.
- ✓ Component 3: Select the Corporate Cyber Supply Chain Risk Management Strategic Approach and Conduct Analysis to Identify/Prioritize Risks
  - Develop best practices-based guidelines and tools that help buyers and suppliers plan and conduct comprehensive assessments of cyber supply chain risk.
- ✓ Component 4: Mitigate Assessed Risk: Create and Continuously Validate a Trusted, Risk Management-focused Supplier Network
  - Develop best practices-based guidelines that help buyers and suppliers to establish and monitor traceability in supply chain processes and supplier relationships.
  - Develop best practices-based guidelines to support the "up-front" screening of potential industry vendors.
  - Support efforts to develop an accreditation model with specific criteria to identify and qualify vendors with strong supply chain risk management practices.
  - Support the establishment of a cyber product/service certification process.
- ✓ Component 5: Mitigate Assessed Risk: Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk
  - Incorporate cyber supply chain threat- and vulnerability- informed language into vendor contract specifications.
  - Support efforts to develop guidelines focused on the voluntary application of cyber supply chain risk management, plans, processes, and practices in the context of low impact BES Cyber Systems and local power distribution systems.
  - Establish best practices –based guidelines for unsupported and open-sourced technology component risk mitigation.
  - Engage with product manufacturing standards bodies to ensure that supply chain risks and vulnerabilities are addressed in cyber hardware and software specifications.
  - Support efforts to provide liability protection to allow "blacklisting" and "whitelisting" of critical cyber products used in private critical infrastructure.
  - Support the expansion of programs at DOE national laboratories to independently test vendor equipment for vulnerabilities and report the results to private companies.
  - Support major ongoing activities of the DHS Information and Communications Technologies Supply Chain Risk Management Task Force.
  - Conduct additional research to understand how insurance/re-insurance programs and policies can be leveraged to incentivize more effective cyber supply chain risk management.

2.0 INTRODUCTION

2.1 Background

Various studies and reports commissioned in recent years by government, industry, and academia call attention to the ever-increasing cyber threats to the BES and local power distribution systems. These current and projected future cyber threats vary greatly in terms of complexity, sophistication, potential impacts, and threat actor capabilities. In the aggregate, they represent a clear and present danger to our national security and economy and the well-being of our citizenry.

Against the backdrop of this dynamic cyber-threat landscape, it is important to note that the electric industry in the U.S. has become increasingly dependent on convergent IT and OT systems that work in tandem to enable the safe, efficient, and reliable generation and delivery of electricity to businesses and communities nationwide.[1] These IT and OT systems are comprised of hardware and software components and enabling technologies procured via a large and diverse mix of manufacturers and suppliers, based both domestically and internationally. The security and integrity of the processes used in the design, development, manufacture, shipping/ distribution, installation, maintenance, and disposal of these IT/OT system components are of increasing concern. This concern stems from a growing array of significant supply chain vulnerabilities – including those associated with the advent of Smart Grid technologies used to monitor, automate, and remotely operate key aspects of the U.S. electric grid – that will be discussed in further detail in this report. Important potential risks corresponding to these vulnerabilities include, but are not limited to, intellectual property theft, the introduction of counterfeits, product tampering and industrial sabotage, product theft, software and hardware corruption, and computer code manipulation that can manifest themselves at various points in the supply chain life-cycle.[2]

In response to the rapid convergence of the cyber threat and vulnerability landscapes faced by the U.S. electric industry, industry regulators recently have developed an integrated of set of cyber supply chain risk management standards targeting entities representing high and medium impact BES cyber systems that will go into effect in July 2020.[3] Collectively, this

[1] OT systems increasingly are directly connected to the Internet, so that operations can be remotely monitored or controlled or to allow third-party vendors to remotely connect to the system to perform diagnostics and maintenance. Some OT systems used by the electric industry are outdated and may lack modern security features that would typically be used to protect an internet-facing connection (e.g. firewalls, multi-factor authentication, strong passwords, logging and monitoring). Price Waterhouse Coopers, Cyber Savvy: Securing Operational Technology Assets, December 2015. See https://www.pwc.com.au/pdf/cyber-savvy-securing-operational-technology-assets.pdf.

[2] Congressional Research Service (CRS) Report R45312, Electric Grid Cybersecurity, September 4, 2018, pages 101-13. See https://crsreports.congress.gov R45312

[3] These standards are: 1) NERC CIP 013-1 (a new standard focused on addressing supply chain cyber security risks during the planning and procurement of high and medium impact BES Cyber Systems; 2) revisions to NERC CIP 005-6 (focused on

combination of new and revised existing standards will address four critical focus areas: 1) software integrity and authenticity; 2) vendor remote access; 3) information system planning; and; 4) vendor risk management and procurement controls.

In addition to these regulatory activities, government agencies such as the U.S. Department of Homeland Security (DHS), U.S. Department of Energy (DOE), and the National Institute for Standards and Technology (NIST), and various industry entities — including the North American Transmission Forum (NATF), the American Public Power Association (APPA) and National Rural Electric Cooperative Association (NRECA), North American Generation Forum (NAGF), and the Edison Electric Institute (EEI), among various others – have developed and disseminated a broad-based set of supply chain risk management best practices for consideration for adoption by electric utilities nationwide. Various individual utility systems also have put in place additional risk mitigations beyond baseline regulatory requirements to address key risk issues at their level. Finally, vendors across electric industry supply chains also have taken steps to enhance their cyber supply chain security and resilience in light of growing threats, electric and other industry requirements, and evolving corporate governance, risk postures, and business case investment considerations.

Two important questions remain for consideration: 1) What key challenges remain regarding cyber supply chain risk management within the electric industry that are not addressed either through current or soon-to-be-implemented regulatory requirements, or by voluntary practices adopted by the industry and its diverse array of suppliers? And 2) How can additional priority issues be addressed?

2.2 Purpose and Organization of the Report

2.2.1 Purpose

This report provides a comprehensive assessment of the current “state of play” and a set of recommendations to further advance cyber supply chain risk management within the U.S electric industry.

2.2.2 Organization

implementing methods to identify active vendor remote access sessions and disable active vendor remote access when necessary); and 3) revisions to NERC CIP 010-2 (focused on verifying the identity of software publishers, and the integrity of all software and patches intended for use on BES Cyber Systems). With minor exceptions (e.g., facilities, systems and equipment for the protection or restoration of the BES such as under-voltage and under-frequency load shedding systems and equipment), NERC Reliability Standards apply only to the BES and not to local distribution systems.

The report begins with an overview of the current and projected cyber supply chain risk environment impacting the U.S. electric industry, along with a discussion of corresponding challenges. The report next examines the key "What's been done?" and "What additional challenges remain?" questions in the context of a notional, best practices-based cyber supply chain risk management framework. This assessment will focus on four principal action areas: 1) regulatory actions within the electric industry; 2) voluntary industry actions and collaboration between government and industry; 3) cyber supply chain risk management approaches and best practices followed by other industries; and 4) vendor/supplier approaches. The report concludes with a series of recommendations and next steps for addressing additional challenges in electric industry cyber supply chain risk management that fall outside of regulated space.

2.3 Scope of the Report

2.3.1 Key Definitions

- Supply Chain: a system of organizations, people, activities, information, technologies, and resources that provide products or services to consumers.[4]
- Cyber Supply Chain Risk Management: the process of identifying, assessing, preventing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains.[5] This process covers the entire life-cycle of a specific product or service (including design/development, manufacturing, deployment, acquisition, shipping and warehousing, installation, updating/maintenance and end-of-life disposal), as specific threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any point in the life-cycle of a given product or service.
- High Impact BES Cyber Systems: Applies to BES Cyber Systems categorized as high impact according to the NERC CIP-002-5.1 identification and categorization processes.
- Medium Impact BES Cyber Systems: Applies to BES Cyber Systems categorized as medium impact according to the NERC CIP-002-5.1 identification and categorization processes.
- Electronic Access Control or Monitoring Systems (EACMS): Applies to each EACMS associated with a referenced high or medium impact BES Cyber System. Examples include,

[4] CRS, In Focus, Cyber Supply Chain Risk Management: An Introduction, June 29, 2018, page 1. See https://fas.org/sgp/crs/homesec/IF10920.pdf

[5] Definition provided is derived from a hybrid of the official definitions of "Cyber Supply Chain Risk Management" used by DHS and NIST.

but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- Physical Access Control Systems (PACS): Applies to each PACS associated with a referenced high or medium impact BES Cyber System with External Routable Connectivity.
- Protected Cyber Asset (PCA): Applies to each PCA associated with a referenced high or medium impact BES Cyber System.

2.3.2 What's In & What's Out – Scoping Parameters

The following were used as scoping parameters in the development of this report:

- The focus of this report is on cyber supply chain risk management across the life-cycle of an IT/OT[6] product or service acquired by electric industry companies, rather than on a more broad-based consideration of physical or cybersecurity writ large across the industry.
- The report considers issues associated with medium and high-impact BES Cyber Systems covered under NERC CIP 013-1, as well as those recently revised aspects of NERC CIP 005-6 and NERC CIP 010-2 that pertain directly to cyber supply chain risk management. The report does not focus on facility-level physical security issues covered under NERC CIP 014-1.
- The report considers cyber supply chain risk management issues associated with low-impact BES Cyber Systems and local distribution systems not covered under the NERC Supply Chain Standards.
- The report does not include consideration of the risk management of cyber supply chains corresponding to the nuclear energy industry that fall under the authority of the U.S. Nuclear Regulatory Commission.

2.4 Methodology Used to Develop the Report

The following comprise the principal components of the methodology used to develop the content of this report:

- Industry and government literature and document review (See Bibliography included in Appendix B)
- Industry and government leadership interviews (See list of interviewees included in Appendix C)

[6] OT systems include those associated with industrial control systems, protective relay systems, and energy management systems.

3.0 DEFINING THE PROBLEM: OVERVIEW OF THE CYBER SUPPLY CHAIN RISK ENVIRONMENT AND RELATED CHALLENGES

3.1 Emergent Trends: Threat Actors and Objectives

Various reports and studies commissioned by U.S. government agencies, regulatory bodies, and electric industry leadership forums and associations document the dynamic and ever-increasing threats to the supply chains that provide a myriad of different products and services to the U.S. electric industry. These threats are global and multi-faceted in scope, play upon multi-dimensional vulnerabilities across the vendor community and individual product and service life-cycles, are oftentimes difficult to detect, and are continuously evolving and adapting. Some threats are unintentional in nature, resulting from vendor employee negligence, poor quality control or maintenance practices (e.g., building in unprotected back doors to provide ease of access for maintenance or software update), outdated inventory management controls, resistance to acknowledging vulnerabilities in vendor hardware/software, etc.[7]

Other threats stem from the actions of a diversity of malicious actor types including disgruntled or disaffected insiders, cyber hackers and hacktivists, criminal and terrorist organizations, and hostile or economic competitor nation-states such as Russia, China, and Iran. These various categories of malicious actors represent a wide range of capabilities, motivations, and potential impacts to cyber supply chain security, integrity, and reliability within the U.S. electric industry. Importantly, malicious actors continuously adapt tactics, techniques, and procedures in ever-more sophisticated ways to achieve their desired objectives. In some cases, the skills required to negatively impact some aspect of a key electric industry cyber supply chain can be quite rudimentary. In other cases, more extensive resources and capacity including advanced technical skills, training, are required.[8]

[7] Idaho National Laboratory, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, 2016, page 15. See https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf

[8] Office of the Director of National Intelligence, Public-Private Analytical Exchange Program, Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions, 2017, page 6. See https://www.odni.gov/files/PE/Documents/11---Supply-Chain-Risks-of-SCADA-Industrial-Control-Systems-in-the-Electricity-Sector_Risks-and-Mitigations.pdf

Our adversaries have augmented their traditional intelligence operations with nontraditional methods, including economic espionage, supply chain exploitation, and the use of students, scientists, and corporate employees to collect classified and unclassified information. Crucially, some threat actors are developing offensive capabilities that could be employed in a crisis or conflict to exploit, disrupt, and damage critical U.S. infrastructure. Supply chain exploitation, especially when executed as a blended operation in concert with cyber intrusions, malicious insiders, and economic espionage, threatens the integrity of key U.S. economic sectors, critical infrastructure, and research/development that the U.S. depends upon for security and economic growth. The scale of these hostile efforts is placing entire segments of our government and economy at risk.

Source: National Counterintelligence and Security Center, "Supply Chain Risk Management," Intelligence.Gov Background Paper, 2017, p.1. See https://www.dni.gov/files/NCSC/documents/products/20170317-NCSC--SCRM-Background.pdf

Key objectives pursued via malicious attacks targeted against cyber supply chains supporting the U.S. electric industry may include: data/intellectual property or product theft; financial extortion; cyber espionage and sabotage; industrial control system, protective relay and emergency management system manipulation; and disruption or destruction of key components used to manage the generation, transmission, or delivery of electric power.

3.2 Electric Grid Supply Chain Vulnerabilities and Risk Management Challenges

Against the backdrop of the multi-dimensional threat environment described above, there are a number of diverse factors making the cyber supply chains increasingly vulnerable to disruption or exploitation. These factors are categorized below.

3.2.1 IT/OT Systems Convergence

The rapid convergence of IT and OT systems within the electric industry in recent years has resulted in improved service, increased cost-competitiveness, and more efficient system operation, monitoring and control, and maintenance. However, these benefits also come with increased risk. Specifically, IT/OT convergence within the industry has created a significant set of cyber-related vulnerabilities due to an increased dependence on microelectronics, interconnected IT networks and systems, and attendant, well-known risks associated with the Internet and integrated telecommunications as old systems are modernized and new ones are more closely integrated. In short, IT/OT systems within the industry are no longer "comfortably air-gapped."

As noted in a recent supply chain risk management report issued by the Electric Power Research Institute (EPRI), integrated IT/OT systems that have spurred grid modernization include the following infrastructure components:

- Hardware endpoint devices, system monitors, remote switches, and next-generation Supervisory Control and Data Acquisition (SCADA)/remote telemetry units (RTU) based on programmable logic circuit (PLC), synchronous link control (SLC), and ASIC (application-specific integrated circuit)-based 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.[9]

Again, the benefits derived from the integration of this sophisticated set of enabling technologies and components into industry operations are numerous. Unfortunately, this integration also can provide greater and more efficient ease of access for a wide array of malicious actors if modern IT-OT system components are not properly secured across their "cradle-to-grave" life-cycle. The EPRI report referenced above provides the following examples: 1) a 2012 incident involving an industrial automation company in which attackers installed malicious software and stole project files related to a SCADA offering; 2) a 2015 incident in

[9] EPRI, Supply Chain Risk Assessment Final Report, July 2018, page 1-1. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/EPRI_Supply_Chain_Risk_Assessment_Final_Report_public.pdf

which unauthorized code was found in Juniper Networks' firewall solution that could allow remote procedure execution; and 3) a 2017 incident in which an anti-virus company was called out for an alleged foreign entity backdoor built into their security products.[10] A key take-away is the notion that once such products are in place and used to enable the transfer of sensitive reliability information, it becomes very difficult to predict and protect against live threats. Such risk is compounded by increasing industry utilization of advanced IT (e.g., via cloud computing) and artificial intelligence services that operate within an uncertain security environment.

3.2.2 Evolving Nature of Global Cyber Supply Chains

The U.S. electric industry procures IT/OT products and services from a globally distributed, highly complex, and increasingly interconnected set of supply chains. These supply chains are characterized by an ever-growing number of vendors (both domestically and internationally); multiple tiers of component and technology outsourcing; transportation and distribution networks with multiple, unsecure points of entry; and a mix of non-standard domestic and foreign government laws, regulations, and policies (or lack thereof) and vendor practices governing their security. This situation means that a number of entities in the domestic and international marketplace (including 3rd and 4th tier suppliers and beyond whose risk characterization may be extremely difficult to assess/vet due to the increasingly opaque nature of global supply chains) may participate in the development, design, manufacturing, delivery, installation, maintenance and end-of-life disposal of a single purchased product, component, or technology. Even known/trusted vendors may be reluctant to disclose certain information they deem to represent a trade secret and/or competitive advantage.

Such ubiquitous access, if appropriately leveraged by any number of malicious actor types, may create a series of potential vulnerabilities across the life-cycle of any given component or product. The design, development, and manufacturing phases represent obvious points of entry for malicious actors, particularly those interested in generating "latent impacts" – meaning adverse effects that manifest well after the product or component is first put into service. The process of maintaining hardware and updating or "patching" software products that support IT/OT systems within the U.S. electric industry also represent critical points of vulnerability. As noted in a recent Electric Industry Security (EIS) Council report, "Software updates are especially prone to hostile efforts to gain persistent access to [critical infrastructure] networks, which adversaries could later use to launch disruptive attacks on infrastructure operations. For

[10] Ibid.

example, the Russian Dragonfly campaign initially targeted 'peripheral organizations such as third-party suppliers with less secure networks,' using them as staging targets to pivot to intended victims."[11]

The situation described in the previous paragraph is compounded by the fact that various elements of the life-cycle of a product or component used in U.S. electric industry operations may fall under the direct control or influence of governments or government-controlled or –influenced commercial entities that are hostile to the U.S. or represent key economic competitors. For example, the dominance of China in global IT and communications products and technologies markets is well established and represents a single point of vulnerability (e.g., a "malicious actor

"A major factor enabling supply chain threats has been the globalization of our supply chains, characterized by a complex web of contracts and subcontracts for component parts, services, and manufacturing extending across the country and around the world. The multiple layers and networks of suppliers in this chain are frequently not well understood by either manufacturers or consumers. Our most capable adversaries can access this supply chain at multiple points, establishing advanced, persistent, and multifaceted subversion. Our adversaries are also able to use this complexity to obfuscate their efforts to penetrate sensitive research and development programs, steal intellectual property (IP) and personally identifiable information (PII), insert malware into critical components, and mask foreign ownership, control, and/or influence (FOCI) of key providers of components and services. Individually and in total, these supply chain at-tacks erode our nation's competitive advantages in commerce, technology, and security."

Source: National Counterintelligence and Security Center, "Supply Chain Risk Management," Intelligence.Gov Background Paper, 2017, p.1. See https://www.dni.gov/files/NCSC/documents/products/20170317_NCSC_SCRM_Background.pdf

[11] EIS Council, Securing Critical Supply Chains, June 28, 2018, page 13. See https://www.eiscouncil.org/App_Data/Upload/8c063c7c-e500-42c3-a804-6da58df58b1c.pdf

monopoly" over critical products and services) for critical key infrastructure operations worldwide. Additionally, hostile nation-states and other malicious actors can "operate through multiple front companies, organizations and individuals to hide their presence, obfuscating efforts to discover and counter their actions." The "latent impact" scenario is most concerning with respect to these types of actors given corresponding global reach considerations.[12]

3.2.3 Smart Grid Technologies

The conceptual approach that underpins Smart Grid design and implementation is the integration of information and communications technologies to change the way in which electric power is delivered and consumed by end-users. According to a report issued by the U.S. Resilience Project, "What makes this construct "smart" are the two-way connections between devices — which makes the system more agile, adaptive and able to sense and pre-empt potential disturbances; gives customers more ability to respond to market signals; and gives the country the ability to integrate renewable sources of energy."[13] The report goes on to highlight potential vulnerabilities and security challenges brought about by this increasing "two-way" communications between interconnected IT/OT systems that are the backbone of Smart Grid operations:

- Increased access points: Millions of devices on the system with two-way communications capabilities will create a multitude of access points to the grid that could be exploited by malicious actors or propagate negative impacts caused by unintended human errors.
- Interconnectivity: Increasing linkages between multiple disparate networks make the Smart grid susceptible to "cross-contamination" between networks and more opportunities for malware to cross from one network to another.
- Complexity: Increasing system complexity creates opportunities for failure, even without a malicious trigger.
- Common computing technologies: Given that Smart Grid solutions are dependent on commercial IT technologies, many of the problems that exist in the office computing environment will affect the Smart Grid.

[12] Ibid., page 15.
[13] NIST, U.S. Resilience Project, Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices, 2012, page 4. See https://usresilienceproject.org/wp-content/uploads/2014/09/report-Supply_Chain_Solutions_for_Smart_Grid_Security.pdf

- Automation: Increased automation of manual functions will compound the potential impact of operator error and making it more difficult to restore a system that has been impacted by malicious actor network activity.[14]

The data points discussed above are further corroborated by a recent report on Distributed Energy Resources (DERs) (i.e., smart inverters, weather sensors, production meters, and like devices) issued by the National Renewable Energy Laboratory (NREL).[15] This report points out that the proliferation of DERs has resulted in an increased number of devices that are owned and/or controlled by consumers and third parties. Additionally, enabling features commonly associated with DERs, such as remote access and remote control, require digital communications and control interfaces that represent an expanded potential for cyber exploitation.[16]

An additional risk associated with the advent of the Smart Grid is that its common components often are manufactured overseas via a complex network of primary and subordinate tier suppliers. As noted in a CRS report issued in 2018, "Most of the smart meter, sensor, and other equipment makers are international companies who obtain their components from multinational sources."[17] The challenge is that the reliable operation of semiconductor- and microprocessor-based devices that represent the backbone of Smart Grid technology is based on low-level firmware used to control such devices. If a malicious actor were to gain remote or insider access to them at key points in the product life-cycle, "a section of code could be covertly inserted in the device and activated in such a way as to impair its functioning in a reliable manner."[18] In such a scenario, malicious code would not need to be placed in all such devices coming off a production line. If a large enough sample was affected, the impacts realized would likely call into doubt the reliability of a whole class of such devices.[19]

[14] Ibid.
[15] NREL, An Overview of Distributed Energy Resource (DER) Interconnection: Current Practices and Emerging Solutions, Technical Report NREL/TP-6A20-72102, April 2019.
[16] Ibid., page 47.
[17] CRS, Electric Grid Cybersecurity R45312, September, 4, 2018, page 12. See https://fas.org/sgp/crs/homesec/R45312.pdf
[18] Ibid.
[19] Ibid.

3.2.4 Industry Practices

The rapid evolution of the operating and risk environments of the U.S. electric industry in recent years in many ways have outpaced the industry's ability to keep pace from a supply chain risk management perspective. Fortunately, government and industry leader have recognized this situation, and important regulatory and voluntary, best practices-based efforts are underway to change this dynamic. A synopsis of these efforts is provided in Sections 5-8 below. For now, it is important to highlight a set of common themes related to industry practices or operational realities that have aggravated the current state of play within the industry. A "representative sampling" of these issues is presented below:[20]

- Lack of holistic, integrated corporate organizational structures, policies, or processes governing cyber supply chain risk management.
- Inability or lack of process to characterize, qualify, vet, and audit multiple tiers of vendors across a given supply chain from a risk perspective, including failure to appropriately leverage independent third-party vendor assessments.
- Lack of comprehensive corporate processes to specifically assess cyber supply chain risk across the life-cycle of a product or technology.
- Failure to ensure access, chain-of-custody, and secure delivery controls across a diverse array of third-party supply chain service providers or product vendors with physical or virtual access to IT/OT systems, software code, intellectual property, etc., across a service or product life-cycle.
- Poor information security and physical access practices on the part of lower-tier suppliers.
- Software security vulnerabilities in supply chain management or supplier systems and compromised software or hardware purchased from suppliers.
- Counterfeit hardware or hardware with embedded malware.
- Insufficient vetting of third-party data storage or data aggregators.
- Insufficient threat-informed contracting language or cyber supply chain requirements for vendors built into the procurement process.
- Inability or lack of systems to enable real time visibility on all endpoints existing in an enterprise wide network environment that extends into supply chain networks.

4.0 NOTIONAL "END-TO-END" MODEL FRAMEWORK FOR

[20] The bulleted items represent a compilation of data from various government and industry sources, including joint government-industry workshops and other discussion forums conducted within the past five years.

CYBER SUPPLY CHAIN RISK MANAGEMENT

4.1 Overview

As noted previously, cyber supply chain risk spans the life-cycle of any given product, technology, or service, beginning with engineering design and development; and continuing through production, shipping and warehousing, ongoing maintenance and software update; and terminating in end-of-life disposal. Cyber supply chain risks – including those impacting security, integrity, and resilience – must be addressed both comprehensively and holistically across this life-cycle.

"Rogue code could be inserted into the software long before devices are connected — or kill switches or back doors could be built into the hardware to enable remote access which could both steal data and disable the system. Counterfeit items, which can degrade system performance, enter the supply chain in transit, in the warehouses and in distribution centers. Maintenance and repair activities — software upgrades and equipment services — whether onsite or done remotely, create opportunities to corrupt or compromise systems. And faulty end-of–life disposal can create new counterfeiting opportunities."

Source: U.S. Resilience Project, Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices, 2010, page 5. See https://usresilienceproject.org/wp-content/uploads/2014/09/report-

This section posits a notional "end-to-end" model framework for cyber security supply chain risk management, applicable in the context of both "buyers" and "suppliers" based on a comprehensive review and compilation of cyber supply chain best practices recommended by various government agencies, industry associations, joint government-industry working forums, and vendor companies over the past several years. A listing of the various sources of these best practices is provided in Appendix B.

This notional end-to-end model framework is intended to provide a comprehensive baseline against which various regulatory requirements and ongoing voluntary and collaborative

activities designed to enhance cyber supply chain risk within the U.S. electric industry can be objectively evaluated. The results of this evaluation – including answers to two principal questions that underpin the current report ("What's been done?" and "What are the remaining priority challenges and corresponding solutions?) – are documented in Sections 5-9 below.

4.2 Key Components of a Model Framework

Figure 2 depicts the key components of a best practices-based model framework for cyber supply chain risk management.

- ✓ **Establish** Corporate Governance and Set the Direction for Cyber Supply Chain Risk Management
- ✓ **Establish and Maintain** Multi-dimensional Information Sharing Partnerships and Technical Capabilities
- ✓ **Select** the Corporate Cyber Supply Chain Risk Management Strategic Approach and Conduct Analysis to Identify/Prioritize Risks
- ✓ **Mitigate** Assessed Risk (1): Create and Continuously Validate a Trusted, Risk Management-focused Supplier Network
- ✓ **Mitigate** Assessed Risk (2): Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk

Figure 1. Key Components of a Model Cyber Supply Chain Risk

4.2.1 Establish Corporate Governance and Set the Direction for Cyber Supply Chain Risk Management

Achieving effective cyber supply chain risk management begins with the establishment of a comprehensive and integrated corporate governance structure. First and foremost, this governance structure must clearly articulate oversight authority and foster Board of Directors, "C-suite," and other senior manager awareness of, commitment to, and engagement in supply chain risk management issues and decisions. Facilitated by senior leadership engagement, it also must ensure the vertical integration of enterprise cyber supply chain risk management strategies and policies (including procurement and acquisition) between the headquarters and geographically distributed operating arms of the corporation to eliminate potential inconsistencies and gaps in risk management approaches employed at various levels of the corporation. It also must drive an inclusive and integrated approach between the various organizational stakeholders within a typical corporate structure that have individual authorities, responsibilities, and equities that must be woven together to effectively and efficiently manage cyber supply chain risk across the life-cycle of applicable products and services. These include, but are not necessarily limited to, the following functions: corporate risk management, compliance, research & development (R&D), engineering, operations/lines of business, IT and physical security, safety, human resources, procurement/contracting, finance, legal, etc. This

functional integration also is key to creating horizontal synergy between the corporate IT and OT enterprises in close coordination with procurement. It also helps establish clear and consistent supply chain risk communications with external stakeholders, including regulatory authorities, vendors, and other supply chain partners.

Setting the direction for enterprise cyber supply chain risk management involves the development of a comprehensive corporate program policy and implementation strategy that drive vertical and horizontal integration of key corporate stakeholders in a unified approach. This includes the articulation of risk management processes with clearly defined criteria, risk evaluation, and risk response components. This program policy and implementation strategy must be subject to a rigorous audit protocol to ensure compliance and get senior leaders the feedback they need to assess performance and make course corrections over time.

- ✓ **Designate** senior executive oversight authority
- ✓ Identify key corporate stakeholders
- ✓ Establish a vertically and horizontally integrated governance process including key corporate staff functions and lines of business
- ✓ **Develop, issue, and audit** compliance with an enterprise cyber supply chain risk management program policy, implementing strategy, and supporting protocols
- ✓ **Develop and implement** risk management processes with clearly defined criteria, risk evaluation, and risk response components
- ✓ **Develop** a risk-based approach to cyber supply chain security that prioritizes key components and technologies based on potential impacts stemming from a major supply chain disruption
- ✓ **Incorporate** supply chain risk management considerations into business continuity and emergency response plans and emergency preparedness activities (i.e., training, drills and exercises)
- ✓ **Conduct benchmarking** against other companies and sectors on an ongoing basis

Figure 2. Establishing Corporate Governance and Setting the Direction

4.2.2 Establish and Maintain Multi-dimensional Information Sharing Partnerships and Technical Capabilities

An effective approach to cyber supply chain risk management includes developing and maintaining a variety of information sharing partnerships within and external to any given corporation, as well as the technical capabilities that enable the trusted exchange of information between partners. Internal information sharing stakeholders include the diverse mix of senior executive leadership, functional area managers, and line of business managers with roles, responsibilities, and equities in supply chain risk management as discussed in the previous section. External stakeholders include regulatory authorities; federal state, and local government cybersecurity, intelligence, and law enforcement agencies; industry cyber information sharing organizations such as the Electric Sector Information Sharing and Analysis Center (E-ISAC)[21]; Electric Subsector Coordinating Council (ESCC)[22]; industry associations; peer companies within the sector; and a wide array of vendors and service providers.

The goal of these information sharing partnerships is multi-fold:

- Provide situational awareness regarding ongoing cyber threats and associated vulnerabilities;
- Inform decision making (including real-time visualization tools and "heat maps") in the context of ongoing threat prevention and mitigation, as well as the response to and recovery from emergent threats and incidents in progress;
- Promote communication and transparency between industry buyers and suppliers;
- Facilitate participation in government-industry planning, training and exercise activities; and
- Facilitate the exchange of cyber supply chain risk management best practices between government, industry, and supply chain partners.

Information sharing partnerships are supported by a variety of technical capabilities and systems, many of which rely on trusted access protocols and electronic communications encryption techniques to assure the secure exchange of data and communications between partners.

[21] https://www.eisac.com/
[22] See: https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_Brochure_July2019.ashx?la=en&hash=6895DE9CB737C2EB81D9E8CA063F0223F6F0B471

- ✓ **Identify** key internal and external cyber supply chain partners
- ✓ **Determine** information sharing needs and requirements
- ✓ Establish formal partnerships and processes and protocols to facilitate information exchange
- ✓ **Develop and maintain** technical capabilities and systems to support trusted, secure information sharing among partners

Figure 3. Establishing and Maintaining Multi-dimensional Information Sharing Partnerships and Technical Capabilities

4.2.3 Select the Corporate Cyber Supply Chain Risk Management Strategic Approach and Conduct Analysis to Identify/Prioritize Risks

Selection of an appropriate strategy or strategies that will allow a corporation to develop a comprehensive understanding of its supply chain risks and inform important risk mitigation and risk response activities is critically important. A corporation may select from a variety of different approaches to guide the development of such a strategy(ies). A recent white paper developed by the NATF identifies the following possibilities:[23]

- Enterprise Strategy – A single strategy to identify and assess cyber supply chain risk for all hardware, software, and services regardless of asset type, software, service, or supplier.
- Supplier Strategy – A separate strategy to identify and assess cyber supply chain risk for each individual supplier or service provider.
- Asset Type Strategy – A separate strategy to identify and assess cyber supply chain risk based on the type of asset or service being acquired (e.g., entity has a separate strategy for an energy management system than for substation relays).
- Hybrid Strategy – A strategy involving the identification and assessment of a combination of hardware, software, and services at a point in time (e.g., a variety of hardware, software, and services acquired to support a specific project).

Of the approaches defined above, a corporate entity will decide which is most effective within its organizational context and whether or not the selected approach will change over time. Additional considerations include selection of the approach through the defined corporate governance process for cyber supply chain risk management, comprehensive documentation as

[23] NATF, Cyber Security Supply Chain Risk Management Guidance, 2018, page 9. See https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NATF%20Cyber%20Security%20Supply%20Chain%20Risk%20Management%20Guidance.pdf

to why a particular approach was selected, continuous assessment of the risk environment associated with the approach selected, and auditing of the approach throughout its implementation to enable necessary course corrections.

Once an appropriate cyber supply chain risk management strategy has been selected, the core elements of the corporation's governance structure for cyber supply chain risk management must work together to assess and prioritize supply chain-related risks to high-consequence business, services, and products (e.g., hardware, software, and services and their relevance to BES reliability in the context of the U.S. electric industry). According to NATF, "This assessment should include an analysis of likelihood and magnitude of impact from unauthorized access, use, disclosure, disruption, modification, or destruction of the [IT/OT] system (industrial control system hardware, software, and computing and networking services), or portion thereof, being procured and the information it processes, stores, or transmits."[24] Additionally, the assessment should consider all relevant aspects of corporate cyber supply chain risk management policy and should be aligned to the overall corporate risk profile and potential additional risk exposure.[25]

With respect to the last point made above, corporate risk exposure based on the specific product, technology, or service in consideration is dependent upon a variety of factors including corporate risk governance, business strategy, enterprise cyber/physical security controls and systems, etc. As noted by NATF, a corporation should consider the following factors with respect to its own risk exposure in conjunction with overall supplier-based risks:[26]

- Usage/function of hardware, software, or service
- Physical location of hardware, software, or service provided
- Quantity of hardware, software, and/or services procured from a single supplier
- Type of access (read or control) provided to supplier
- Quantity and nature of information provided to or accessible by supplier
- Corporate IT and Technology Strategy
- Supplier history
- Financial impact to change supplier if necessary
- Reliability impact to change supplier if necessary

[24] Ibid., page 10.
[25] Ibid., pages 10-11.
[26] Ibid., page 10.

- Corporate Entity supply chain procurement process – master services agreement, contract addendums

✓ **Determine** the corporate strategic approach to cyber supply chain risk management based on supplier, product/service, or project
✓ **Map strategy** selected to corporate cyber supply chain risk management policy to ensure alignment
✓ **Assess and prioritize** supply chain-related risks to high-consequence business, services, and products
✓ **Determine** corporate risk exposure based and map to cyber supply chain risk management strategy selected

4.2.4 Mitigate Assessed Risk: Create and Continuously Validate a Trusted, Risk Management-focused Supplier Network

Figure 4. Selecting the Strategic Approach and Conducting Analysis

This section and the next of the model framework focus on the need to establish and implement comprehensive policies, processes, and procedures to scrutinize suppliers to establish confidence in the products and services being sourced; the quality of design, development, and manufacturing processes employed by suppliers; and the security practices of primary and subordinate tier vendors across the product/service life-cycle.

Building and maintaining a transparent, "trusted" supplier network is a key aspect of effective cyber supply chain risk management. This process begins with the development of an understanding of exactly who one's suppliers are across an array of critical products and services. This task is daunting driven the sheer numbers and types of multi-tier suppliers supporting any given product or service procurement within an industry as complex as the U.S. electric industry. Once primary (tier 1 & 2) suppliers are identified, a company can begin the process of vetting them and identifying corresponding risks against comprehensive evaluative criteria using a variety of different techniques, including multi-source legal, financial, and security background checks and independent, third-party audits of vendor-provided information.[27] Once a trusted relationship has been established, a company may elect to "pre-qualify" assessed vendors for particular types of procurements, implement "product certification" programs, and/or certify certain aspects of vendor supply chain risk management programs. Companies can next work with trusted primary vendors to assess, qualify and

[27] In a report issued in 2018, the NAGF includes a comprehensive listing of criteria and supporting definitions for use in evaluating vendor-associated risk, including, but not limited to: country of origin, type of industry represented, core business, business history, principal source(s) of product/component supply, personnel surety practices, remote access practices, hardware/software life-cycle security practices, vulnerability testing processes, etc. See NAGF, Chain Cyber Security Supply Management White Paper, September 18, 2018, pages 7-9.
https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NAGF%20SC%20White%20Paper%20final.pdf

manage their subordinate tier suppliers using the approach discussed above. Companies should establish open and transparent channels of communications with vendors beyond the initial vetting and pre-qualification processes jointly identify and mitigate continuously evolving risk, respond to changes in the procurement environment, stay aware of emergent best practices, etc.

- ✓ **Map** out primary supplier networks and identify corresponding risks
- ✓ **Work** with primary suppliers to identify subordinate tier suppliers and corresponding risks
- ✓ **Develop** a comprehensive set of vendor risk evaluation criteria for use in evaluating the risk profile of potential vendors
- ✓ **Conduct** up-front security reviews, third-party accreditation, and multi-source financial, legal, and background checks on vendors
- ✓ Clearly **articulate** security requirements to vendors
- ✓ Establish criteria for event-driven and periodic reassessment of vendor suitability
- ✓ **Perform** independent third-party audits on vendor-provided information
- ✓ **Establish** and deploy "trusted vendor" and "product certification" programs (in partnership with government and industry peers)
- ✓ **Maintain** ongoing communications and information exchange with vendors across the life-cycle of a product or service

Figure 5. Creating and Validating a Trusted Supplier Network

4.2.5 Mitigate Assessed Risk: Implement Controls to Manage Cyber Supply Chain "Life-Cycle"

Life-cycle risk management involves three principal components: security, integrity, and resilience. Security refers to controls that maintain the confidentiality, integrity, and availability of information that (1) describes the supply chain, including parties involved in the supply chain as well as information describing the supply chain in both a physical and virtual sense; or 2) traverses the supply chain across its life-cycle, including intellectual property embedded in products and services. Integrity is focused on controls ensuring that the products or services in the supply chain are genuine, unaltered, and that they will perform according to stated requirements. Resilience means the supply chain employs controls that ensure required products and services continue to perform under conditions of stress or failure. Figure 7 below highlights a number of representative examples of controls that can be employed by companies to help ensure security, integrity, and resilience across the life-cycle of a given product of service provide by external vendors.

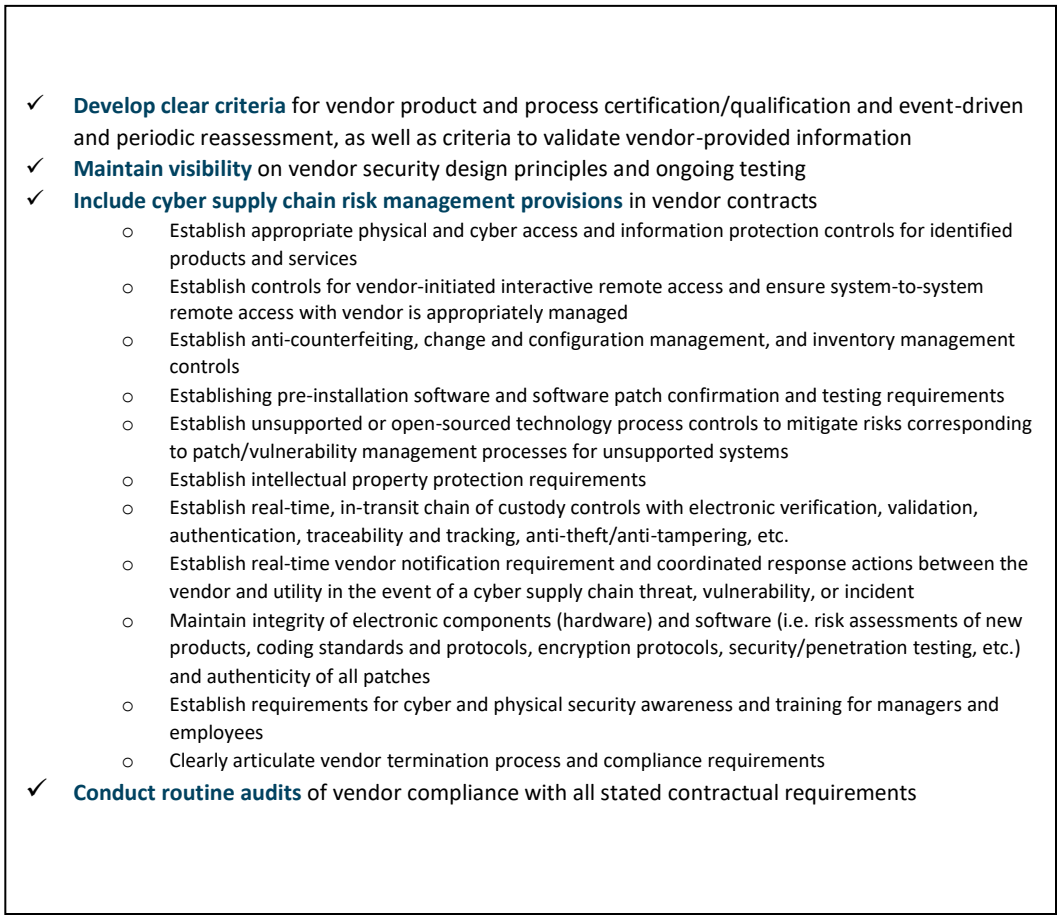


Figure 6. Implementing Controls to Manage Cyber Supply Chain "Life-Cycle"

5.0 ASSESSING WHAT'S BEEN DONE: REGULATORY ACTIONS

5.1 Overview

This section begins with a summary of regulatory actions approved for implementation or currently under development that are designed to address supply chain risk issues within certain segments of the U.S. electric industry. Following this summation, this section will provide a mapping of the NERC supply chain risk management standards and additional NERC-proposed cyber supply chain risk mitigation actions against the various individual components of the model framework discussed in Section 4 above. The resultant gaps will then be discussed in further detail and will feed the best practices discussion provided in Sections 6-8.

5.2 Summary of NERC CIP Cyber Supply Chain Risk Management Standards

In 2017, NERC developed a new reliability standard (CIP-013-1, Cybersecurity – Supply Chain Risk Management) and revised two existing reliability standards (CIP-005-6, Cyber Security – Electronic Security Perimeter(s)), and CIP-010-3, (Cyber Security – Configuration Change Management and Vulnerability Assessments) to help address cyber supply chain risk in the context of high and medium-impact BES Cyber Systems.[28] These standards have three principal areas of focus: 1) Development and implementation of plans and processes to manage cyber supply chain risk (CIP 013-1); 2) Monitoring and control of vendor connections to BES Cyber Systems (CIP-005-6); and 3) Validation of software from identified sources (CIP-010-3).[29] Collectively, these standards will require covered entities within the electric industry to develop processes to ensure they manage supply chain risks to high and medium impact BES Cyber Systems. These standards take effect on July 1, 2020. A summary of the specific requirements contained in the NERC Supply Chain Standards is provided in Table 1 below.

[28] Neither low impact BES Cyber Systems nor local distribution systems are not covered under the NERC Supply Chain Standards.
[29] See EPRI, Supply Chain Risk Assessment Final Report, July 2018, page 3-1. See: https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/EPRI_Supply_Chain_Risk_Assessment_Final_Report_public.pdf

Table 1. NERC CIP Cyber Supply Chain Risk Management Standards

CIP 013-1 Cybersecurity – Supply Chain Risk Management	
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.	
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. **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 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 R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	
R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months.	
Source: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf	
CIP-005-6 Cyber Security – Electronic Security Perimeter(s)	
R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-6 Table R2 –Remote Access Management.	
2.4.	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).
2.5.	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).
Source: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-6.pdf	
CIP-010-3 Cyber Security – Configuration Change Management and Vulnerability Assessments	
R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-3 Table R1 – Configuration Change Management.	

1.6	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2 & 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: **1.6.1.** Verify the identity of the software source. **1.6.2.** Verify the software obtained from the software source. Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.
R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-3 Table R3– Vulnerability Assessments.	
3.1	At least once every 15 calendar months, conduct a paper or active vulnerability assessment. (Applicable to high and medium impact BES Cyber Systems only).
3.2	Where technically feasible, at least once every 36 calendar months (Applicable to high impact BES Cyber Systems only): **3.2.1** Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and **3.2.2** Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.
3.3	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset (Applicable to high impact BES Cyber Assets only)
3.4	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items. (Applicable to high and medium impact BES Cyber Systems only)
Source: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-3.pdf	

Representative examples of specific risks addressed by the NERC Supply Chain Standards are provided in Table 2 below.

Table 2. Cyber Supply Chain Standards – Risk Mitigation Mapping Examples

	Identified Risk				
	Exploitation of legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System	Vendor remote access-related threats, including stolen vendor credentials used to access a BES Cyber System without responsible entity's knowledge as well as a compromise at a trusted vendor traversing over unmonitored connection into a responsible entity's BES Cyber System	Responsible entities unintentionally planning to procure and install vulnerable equipment or software within their information systems or unintentionally failing to anticipate security issues that may arise due to their network architecture or during technology and vendor transitions	Risk that products procured by a responsible entity fail to meet minimum security criteria	Compromised vendor not providing adequate notice of security events and vulnerabilities and related incident response to responsible entities with whom that vendor is connected
NERC Report	Relevant Section				
CIP-013-1	R1 Part 1.2.5	R1 Parts 1.2.3 & 1.2.6	R1 Part 1.1	R1 Parts 1.1 & 1.2	R1 Parts 1.2.1, 1.2.2 & 1.2.4
CIP-005-6		R2 Parts 2.4 & 2.5			
CIP-010-3	R1 Part 1.6		R3 Parts 3.1-3.4	R3 Parts 3.1-3.4	

Source:https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf, page 5.

Based on an additional directive contained in Federal Energy Regulatory Commission (FERC) Order No. 850, and as informed by further evaluation by NERC staff, the NERC is also moving forward with further revision of the Supply Chain Standards to address risks to high and medium-impact BES Cyber Systems associated with EACMS and PACS (excluding monitoring and logging in the

context of both EACMS and PACS).[30] According to Order No. 850, these modifications must be submitted to the FERC within 24 months after the effective date of the final rule (July 1, 2020). NERC also plans to work with its Critical Infrastructure Protection Committee (CIPC) Supply Chain Working Group to develop a guideline to assist industry entities in the evaluation of their PCAs on a case-by-case basis to determine if any additional supply chain protections may be warranted.[31]

Regarding low impact BES Cyber Systems, the NERC staff will conduct additional evaluation via industry surveys and questionnaires following Supply Chain Standard implementation to determine whether or not these standards should be modified in the future to include such systems. This information gathering effort will include a spotlight on actual market and entity practices and the extent to which these practices may help reduce risks linked to supply chains for low-impact BES Cyber Systems.[32] NERC also has committed to working with the CIPC Supply Chain Working Group to develop a guideline to assist in the voluntary application of supply chain risk management plans to low impact BES Cyber Systems.[33]

Although not included within the final Supply Chain Standards or as part of the additional EACMS- or PACS-focused modifications currently under development, NERC has identified numerous best practices that it recommends the industry consider to further mitigate cyber supply chain risk.[34] These include:

- **Cyber Hardware Integrity:** Various hardware assets supporting the BES may be defective or possess code that can be manipulated across the product life-cycle to impact system operability. Hardware should be validated and tested appropriately to prevent and/or mitigate the impacts of unintentional defects of deliberate manipulation.
- **Third-Party Accreditation Processes:** Many segments of the industry currently utilize independent assessments or third-party accreditations of their vendors as part of their supply chain risk management strategy. NERC has committed to work with industry to develop an accreditation model for identifying vendors with strong supply chain risk management practices.
- **Threat-Informed Procurement Language:** Industry entities should tailor cyber supply chain risk mitigation specifications contained in vendor contracts to specific risks as identified via product- and service- specific threat and vulnerability modeling.

[30] NERC, Cyber Security Supply Chain Risks: Staff Report and Recommended Actions, May 17, 2018, page v. See: https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf
[31] Ibid., pages v-vi.
[32] Ibid., page 20.
[33] Ibid.
[34] Ibid. pages 3-4.

- **Unsupported or Open-Sourced Technology Component Risk Mitigation:** Industry entities should develop plans to mitigate potential risks posed by systems where patch sources are no longer available, as well as for patching and otherwise supporting systems or components that rely upon open source technology. NERC has committed to work with the CIPC Supply Chain Working Group to develop an appropriate guideline.

According to a recent joint report issued by APPA and NRECA, NERC also is committed to undertaking the following additional activities beyond the scope of the Supply Chain Standards:[35]

- Exploring opportunities with product manufacturing standards bodies to ensure that supply chain risks and vulnerabilities are addressed in product specifications; and
- Assisting industry stakeholders in developing an accreditation model for identifying vendors with strong supply chain risk management practices.

The report further states that "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 [Institute of Electrical and Electronics Engineers] (IEEE) [standards] and other product specifications. Small entities will also benefit if vendors are accredited as having strong supply chain risk management practices."[36]

As discussed in the next section, the "beyond regulation" best practices identified above represent key potential solutions for consideration based on risk issues that are not addressed in the current cyber chain risk management regulatory construct for the U.S. electric industry.

5.3 Regulatory Analysis

5.3.1 Overview

This section provides a visual mapping of the various risk mitigation requirements contained in the approved NERC Supply Chain Standards to the Cyber Supply Chain Model Risk Management Framework discussed in Section 4 above, along with a narrative analysis of key risk issues not covered by the soon-to-be implemented regulatory standards and proposed next steps post-implementation. Although important, this analysis does not include discussion of the proposed modifications to the approved NERC Supply Chain Standards as related to EACMS or PACS, as these modifications are still in the developmental phase and their precise mitigation language

[35] APPA and NRECA, Managing Cyber Supply Chain Risk-Best Practices for Small Entities, April 25, 2018, Page 8. See: https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Managing%20Cyber%20Supply%20Chain%20Risk.pdf
[36] Ibid.

remains unknown. In overall terms, however, they undoubtedly will serve to address critical issues in these two areas.

Table 3. Mapping NERC Supply Chains Standards Requirements to Key Components of a Model Cyber Supply Chain Model Risk Management Framework

Model Framework Components	CIP-013-1	CIP-005-6	CIP 010-3
Establish Corporate Governance and Set the Direction for Cyber Supply Chain Risk Management	Partially Covered (R1 Part 1.1)*	Not Specifically Covered	Not Specifically Covered
Establish and Maintain Multi-dimensional Information Sharing Partnerships and Technical Capabilities	Partially Covered (R1 Parts 1.2.1 – 1.2.4)**	Not Specifically Covered	Not Specifically Covered
Select the Corporate Cyber Supply Chain Risk Management Strategic Approach and Conduct Analysis to Identify/Prioritize Risks	Partially Covered (R1 Part 1.1)***	Not Specifically Covered	Not Specifically Covered
Mitigate Assessed Risk (1): Create and Continuously Validate a Trusted, Risk Management-focused Supplier Network	Not Specifically Covered	Not Specifically Covered	Not Specifically Covered
Mitigate Assessed Risk (2): Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk	Partially Covered (R1 Parts 1.2.1 – 1.2.6)****	Covered (R2 Parts 2.4 & 2.5) (Vendor remote access risk only)	Partially Covered (R1 Parts 1.6.1 & 1.6.2) (Software source identification and software verification only)***** (R3 Parts 3.1-3.4) (Technical vulnerability assessment and testing)

***Note:** Partially covered rating indicates that the technical plan/process requirements listed are more "tactical" in nature and do not address corporate governance structure or process for cyber supply chain risk management.
****Note:** Partially covered rating indicates that only vendor-to-entity information sharing requirements are covered.
***Note: Partially covered rating indicates that the technical requirements listed are deliberately general in nature and do not provide for the implementation of any specific measures.

****Note:** Partially covered rating indicates that the technical requirements listed do not cover the full spectrum of malicious actor threats or entry points across a product or service life cycle-cycle of a given as discussed in the model framework. Also, R2 specifies that plan implementation does not apply to existing contracts, the actual terms and conditions of a procurement contract, or vendor performance and adherence to a contract.
*****Note:** R1 specifies that plan implementation does not apply to existing contracts, the actual terms and conditions of a procurement contract, or vendor performance and adherence to a contract

5.3.2 Model Framework Component 1: Establish Corporate Governance and Set the Direction for Cyber Supply Chain Risk Management

The NERC Supply Chain Standards are deliberately focused on the technical aspects of mitigating identified risk. They do not contain any specific requirements regarding the more strategic elements of the model framework discussed in Section 4 including senior executive oversight and governance, vertical and horizontal integration of core staff functions and lines of business, overarching enterprise supply chain risk management policy and processes, etc. Of note, R3 of CIP-013-1 does require responsible entities to review and obtain "CIP Senior Manager" or delegate approval of its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months. However, this R3 requirement is not reflective of a more overarching governance approach. Additionally, the R1 Part R1.1 requirement for "responsible entities to identify one or more processes used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES from vendor products or services resulting from procuring and installing vendor equipment and software or transitioning from one or more vendor to another" is non-specific in nature. No individual process or plan component requirements are specified.

5.3.3 Model Framework Component 2: Establish and Maintain Multi-dimensional Information Sharing Partnerships and Technical Capabilities

The NERC Supply Chain Standards do not contain any information sharing partnership and technical information capability requirements beyond those associated with vendor vulnerability and threat/incident reporting. This includes information sharing partnerships and technical system connectivity with federal, state, and local government partners; industry ISACs; industry associations; or industry peers.

5.3.4 Model Framework Component 3: Select the Corporate Cyber Supply Chain Risk Management Strategic Approach and Conduct Analysis to Identify/Prioritize Risk

As mentioned above, the CIP-103-1 R1 Part R1.1 requirement for responsible entities to identify one or more processes used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES from vendor products or services resulting from procuring and installing vendor equipment and software or transitioning from one or more vendor to another is ambiguous and non-prescriptive in nature. No specific process or plan requirements or risk assessment and management approach criteria are provided. The minimum baseline construct as to what comprises an acceptable risk assessment is also undefined.

5.3.5 Model Framework Component 4: Mitigate Assessed Risk: Create and Continuously Validate a Trusted, Risk Management-focused Supplier Network

The NERC Supply Chain Standards are product- and service-centric with respect to risk assessment and management. They do not make specific reference to a trusted vendor concept across a product/service life-cycle; objective evaluation of vendor risk profile; vendor suitability checks (initial, event-driven, or recurring); product/service certification programs; or independent third-party audits of vendor-provided information.

5.3.6 Model Framework Component 5: Mitigate Assessed Risk: Implement Controls to Manage Cyber Supply Chain Life-Cycle

This aspect of the NERC Supply Chain Standards has the most direct and specific linkages to the model framework. All three of the standards address a number of critical threat vectors and technical mitigation actions across a number (but not all) of critical entry points across the product or service life-cycle. Specific requirements address vendor remote access, software provider identification, and software/patch verification and testing, and vendor supply-chain-related threat, vulnerability, and incident reporting and coordination. Critical areas not covered include hardware integrity; intellectual property theft controls; anti-counterfeiting and inventory management controls; integrity controls utilized by subordinate suppliers; real-time, in-transit chain of custody controls; third party accreditation; unsupported or open-sourced technology process controls; vendor personnel surety, security awareness and training requirements; and the use of threat-informed procurement language (or any specific requirements regarding the procurement process). The Supply Chain Security Standards do not apply to existing contracts, the actual terms and conditions of a procurement, contract or vendor performance and adherence to a contract. This leaves open the possibility that an existing contractual relationship that does not fully align with the standards may remain in effect and represent a critical vulnerability.

5.3.7 Other Considerations

The NERC Supply Chain Standards do not apply to low impact BES cyber systems. This means that approximately 79 percent of all Registered Entities fall outside the NERC Supply Chain Standards regulatory construct.[37] Additionally, the NERC Supply Chain Standards do not apply to local power distribution systems.

Regarding BES Systems, one risk represented by "low impact" systems is that many of them are, in fact, owned by entities that also own medium and high impact systems. The potential danger here is that a malicious actor could use a presumably less secure, low impact system to "cross-contaminate" a higher-impact system owned by the same entity. NERC acknowledges this risk, but counters that such risk also may be addressed indirectly via implementation of the Supply Chain Standards across the medium and high impact BES Cyber System community. In the case of entities that own a spectrum of high, medium, and low impact facilities, it is assumed that such entities would apply similar supply chain controls across all asset types under their ownership where it makes sense to do so from a cost and risk mitigation perspective. NERC also assumes that many other low-impact BES Cyber System owners will voluntary put in place best practice-based cyber supply chain controls that have achieved widespread awareness through the Supply Chain Standards development process.[38]

NERC also holds that "smaller entities that own only low impact BES Cyber Systems often purchase from the same, well-established vendors that larger entities with higher risk assets use. As larger entities with medium and high impact BES Cyber Assets demand certain supply chain practices from vendors, vendors may choose to apply those supply chain practices to all of their products sold to the electric power industry."[39] A recent joint APPA-NRECA report supports this premise, stating: "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, 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."[40]

---

[37] EPRI, Supply Chain Risk Management: Final Report, July, 2018, page 4-2. See: https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/EPRI_Supply_Chain_Risk_Assessment_Final_Report_public.pdf

[38] NERC, Cybersecurity Supply Chain Risks, September 17, 2018, pages 17-18. See: https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[39] Ibid., page 18.

[40] APPA and NRECA, Managing Cyber Supply Chain Risk-Best Practices for Small Entities, April 25, 2018, Page 9. See: https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Managing%20Cyber%20Supply%20Chain%20Risk.pdf

A recent EPRI report expresses concern that an additional concern that "low-impact" BES Cyber Systems may represent a collective risk known as "common-mode vulnerability."[41] In one example, the EPRI report states: "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."[42] The report goes on to suggest that risks corresponding to common-mode vulnerabilities can be mitigated if supply chain security practices are applied uniformly across cyber asset types, regardless of BES cyber system impact level. A sequenced approach to address this potential risk includes the following steps:[43]

- Identify the types and quantities of vendor-supplied products used to support BES Cyber Systems;
- Research and model the impact of a common-mode exploits targeting multiple, geographically dispersed low-impact BES Cyber Systems to determine the extent of potential risk; and
- Direct, targeted outreach to those vendors that have the largest potential risk to the grid across all BES Cyber System impact levels.

In an effort to more comprehensively identify, assess, and mitigate the nature of the threat posed by low-impact BES Cyber Systems, NERC has committed to work with industry to acquire additional information to more comprehensively frame the risk and develop interim best practices tailored to the low-impact BES Cyber System operating and risk environments.

6.0 ASSESSING WHAT'S BEEN DONE: VOLUNTARY AND COLLABORATIVE ACTIONS ON THE PART OF THE ELECTRIC INDUSTRY AND GOVERNMENT

6.1 Overview

As noted in the previous section, the implementation of the new NERC Supply Chain Standards will have a marked effect on cyber supply chain risk management within and across key segments of the U.S. electric industry. However, the current regulatory structure is not, nor is it intended to be, an all-encompassing "silver bullet;" rather, it represents an important new risk-informed baseline for cyber supply chain security, integrity, and resilience for medium and high

[41] EPRI Report, page 4-2.
[42] Ibid.
[43] Ibid, page 5-1.

impact BES Cyber Systems. Additionally, as previously discussed, the new Supply Chain Standards are likely to have many important "spill over" benefits including best practices for lower impact systems and multi-tier suppliers that service all levels of BES Cyber System customers. These same best practices are likely to be of great additional benefit to local distribution systems and the vendors that service them.

It is important to note that various government agencies and a variety of entities within the U.S. electric industry (including the ESCC, EIS Council, E-ISAC, EEI, individual corporations, trade associations, and industry working forums, among various others) are pursuing voluntary efforts, both independently and in collaboration with one another, to identify and address cyber supply chain risk management challenges that go beyond the NERC regulatory baseline for high and medium-impact BES Cyber Systems and that have direct relevance to low impact BES Cyber Systems and local power distribution systems and their vendor supply chains. This section provides an overarching survey of a number of these efforts as related to the key challenges identified in Section 5.0 above. Survey results will be presented in alignment with the model framework discussed in Section 4.0 above.

6.2 Survey Results Organized by Model Framework Component

6.2.1 Establish Corporate Governance and Set the Direction for Cyber Supply Chain Risk Management

- NATF Report, Cyber Security Supply Chain Risk Management Guidance.[44] This report includes a best practices-based discussion of corporate governance, vertical and horizontal functional area and line-of-business integration, overarching policy development and objectives setting, and defining corporate risk exposure in the context of cyber supply chain risk management.

- APPA and NRECA Report, Managing Cyber Supply Chain Risk-Best Practices for Small Entities.[45] This report identifies a catalog of best practices for cyber supply chain risk management for consideration by small registered entities with low impact BES Cyber Systems. Among these is a series of considerations to gain senior leader commitment, foster cross-functional collaboration, and inform the corporate governance structure and process for cyber supply chain risk management across the various staff and operational components of a small business enterprise.

- NIST, U.S. Resilience Project, Best Practices in Cyber Supply Chain Risk Management.[46] This report addresses the importance of creating cross-functional collaboration within a utility at an enterprise level to create synergy between three different elements: 1) OT systems which oversee plant operations and control equipment, and are vulnerable to cyberattacks like Stuxnet or malware/low quality counterfeits in key components; 2) IT systems, which include the security of all information technology systems and software; and 3) Supply Chain, which oversees providers of components, systems, software suppliers and services. The report includes a variety of governance concepts to facilitate the cross-integration of these three primary groups, as well as other important staff functions at the enterprise level, to address cyber supply chain risk in an informed and integrated way. Beyond governance, the report also identifies and provides best practices examples in support of four overarching enterprise priorities: 1) Determining high-level supply chain security principles and guidelines using an “end-to-end” philosophy (i.e. across the life-cycle of a given product or service and ensuring that business continuity and supply chain risks are

[44] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NATF%20Cyber%20Security%20Supply%20Chain%20Risk%20Management%20Guidance.pdf

[45] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Managing%20Cyber%20Supply%20Chain%20Risk.pdf

[46] NIST, U.S. Resilience Project, Best Practices in Cyber Supply Chain Risk Management https://www.nist.gov/system/files/documents/itl/csd/USRP_NIST-Utility_100115.pdf

considered in tandem); 2) Manage overall procurement risks; 3) Mitigate vendor risks; and 4) Maintain ongoing assurance.

6.2.2 Establish and Maintain Multi-dimensional Information Sharing Partnerships and Technical Capabilities

- DHS, Tri-Sector Executive Working Group.[47] The Tri-Sector Executive Working Group is a public-private partnership that facilitates and integrates a collaborative approach to risk management through prioritization, planning, and response across the Financial Services, Communications, and Electricity Sectors. Executive Working Group membership includes senior industry representatives from the Financial Services Sector, Communications Sector, and Electricity Sub-sector and senior government representatives from the Departments of Homeland Security, Treasury, and Energy. The Executive Working Group thus far has launched efforts to help direct intelligence collection requirements, build cross-sector risk management playbooks, and better understand systemic risk.

- DOE Multiyear Plan for Energy Sector Cybersecurity.[48] This plan provides a detailed discussion of DOE's cybersecurity relationship with the private sector, including key cyber supply chain considerations. Specifically, the plan puts forth an integrated strategy to reduce cyber risks in the U.S. energy sector by pursuing high-priority activities that are coordinated with other DOE offices, and with the strategies, plans, and activities of the federal government and the energy sector.[49] Key elements of this plan with direct relevance to supply chain risk management include, but are not limited to: 1) The Cyber Risk Information Sharing Program (CRISP), currently managed by the E-ISAC, which provides energy sector owners and operators with a capability to voluntarily share cyber threat data in near-real-time, analyze this data using U.S. intelligence, and receive machine-to-machine threat alerts and mitigation measures; 2) Actions to identify and take appropriate steps to mitigate supply chain cybersecurity risks and facilitate the building of trust between owners and operators and Energy Sector Industrial Control System (ICS) manufacturers; and 3) Establishment of a robust cyber-physical testing capability at national laboratories to analyze systems and component vulnerabilities, malware threats, and impacts of zero-day threats on energy infrastructure; and to support initiatives to harden the supply chain.

- ESCC.[50] The Electricity Subsector Coordinating Council (ESCC) serves as the principal liaison between the federal government and the electric power industry, with the mission of

[47] https://www.dhs.gov/cisa/tri-sector-executive-working-group
[48] DOE, Multiyear Plan for Energy Sector Cybersecurity, March 2018. file:///F:/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf
[49] Ibid.
[50] https://www.eei.org/issuesandpolicy/Documents/ESCC%20Brochure.pdf

coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. The ESCC includes electric company CEOs and trade association leaders representing all segments of the industry. Its counterparts include senior Administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations. The ESCC currently is working with government partners to convene government and industry officials and vendors, to identify and share best practices to identify and address systemic supply chain risks and vulnerabilities within the electric industry.[51]

- The Public-Private Analytic Exchange Program, Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions.[52] This report calls for improved information sharing among federal, state, and industrial organizations involved in managing the risk corresponding to cyber supply chain security within the U.S. electric industry. Specific recommendations include: white papers detailing best practices, enhanced warning and attack intelligence, post-attack forensics, peer-to-peer information exchange, and access to classified threat briefings and more context in unclassified reports. The report also advocates a government-industry partnership to develop industry tools and avenues for testing IT/OT systems and their components across a product life-cycle. The report holds that DOE should lead this collaborative work to help identify and minimize IT/OT attack surfaces, prioritize and isolate key elements of electricity generation and delivery from internal and public networks, and enable system recovery. The report goes on to suggest development of a test program, possibly through DOE's national laboratories, to examine grid components, evaluate cyber malware impacts to components in a simulated environment, and assess the posture of the cybersecurity supply chain.

- NIST, U.S. Resilience Project, Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices.[53] This report recommends a focused effort on benchmarking supply chain best practices in security and resilience within the Electric Sector, including ongoing dialogue between IT/OT and supply chain professionals, and between utilities and their suppliers. Categories of best practices highlighted in the report include: Risk-based frameworks; Visibility down the supply chain tiers; Chain of custody controls; Training, new technology applications and ongoing communications with vendors, shippers and

[51] EIS Council Report, page 22.
[52] The Public-Private Analytic Exchange Program, Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions, 2017. https://www.odni.gov/files/PE/Documents/11---Supply-Chain-Risks-of-SCADA-Industrial-Control-Systems-in-the-Electricity-Sector_Risks-and-Mitigations.pdf
[53] NIST, U.S. Resilience Project, Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices, 2012. https://usresilienceproject.org/wp-content/uploads/2014/09/report-Supply_Chain_Solutions_for_Smart_Grid_Security.pdf

customers; and Secure design principles and ongoing testing. Leveraging supplier summits to establish common expectations and requirements for supply chain security, integrity and resilience was also discussed. The report also calls for clarification of roles and responsibilities between the public and private sectors regarding cyber supply chain risk management, including a discussion of what needs to be done, and who has the expertise to do it. Increased recognition of the "joint" nature of the problem is also highlighted in the report.

6.2.3 Select the Corporate Cyber Supply Chain Risk Management Strategic Approach and Conduct Analysis to Identify/Prioritize Risks

- NATF Report, Cyber Security Supply Chain Risk Management Guidance. This report includes a discussion of the various approaches an entity may choose from to manage cyber supply chain risk including enterprise-level, vendor-specific, asset type-specific, or hybrid approaches. It also includes a discussion of the specific components of a standard cyber supply chain risk assessment, including threats (both unintentional and malicious actor related), vulnerabilities (both entity and supplier-related), and the potential impacts stemming from a breach in supply chain security, integrity, or reliability. Also discussed is the importance of aligning the risk assessment to the entity's specific risk tolerance and overarching corporate cybersecurity policies. Finally, the report provides a discussion of entity-supplier interaction during the risk assessment process, including independent third-party verification of a wide array of vendor-provided information used to support the risk assessment. This discussion also includes specific criteria for triggering an event-driven or periodic re-assessment of the risk corresponding to a particular vendor or vendor-supplied product or service.

- NAGF Report, Cyber Security Supply Chain Management White Paper.[54] This report includes a detailed listing of "vendor risk attributes" that it recommends for consideration as part of a vendor supply chain risk assessment to help determine the appropriate level of supply chain controls. Primary risk attributes include the following: country of origin, type of industry, core business, vendor history, originating source of products/services provided, remote access requirements, hardware/software life-cycle integrity and testing processes, and specific vendor product/service security attributes.

- APPA and NRECA Report, Managing Cyber Supply Chain Risk-Best Practices for Small Entities. This report includes a discussion of various model frameworks that can support an

[54] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NAGF%20SC%20White%20Paper%20final.pdf

enterprise approach to enterprise-level cyber supply chain risk assessment and prioritization.

- DOE Cyber Security Capabilities Maturity Model (C2M2). This model considers supply chain risk management as a function of identifying and managing external dependencies. Recognizing dependencies and those that are most critical to operations can improve an entity's ability to highlight and mitigate supply chain risks.

6.2.4 Mitigate Assessed Risk (1): Create and Continuously Validate a Trusted, Risk Management-focused Supplier Network

- APPA and NRECA Report, Managing Cyber Supply Chain Risk-Best Practices for Small Entities. This report includes a detailed discussion of the use of well-known, trusted, and established vendors as a principal foundation for reducing supply chain risk across of a product or service life-cycle, including leveraging the influence of larger companies within the U.S. electric industry to drive more robust supply chain controls across key elements of the vendor community. The report also discusses the importance of independent third-party assessment of vendor risk and products/services-related information.
- NIST, Best Practices in Vendor Selection and Management.[55] This document contains a listing of NIST recommended best practice considerations regarding vendor selection and ongoing management, including approved vendor lists. Key focus areas discussed in the document include:
    - Security Governance
    - Manufacturing/Operational Security
    - Software Engineering and Architecture
    - Asset Management
    - Incident Management
    - Transportation Security
    - Physical and Environmental Security
    - Personnel Surety
    - Information Protection
    - Sub-tier partner security (lower tiers, service providers, cloud)

[55] NIST, Best Practices in Vendor Selection and Management. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Vendor-Selection-and-Management.pdf

- Personnel Training

- NIST, U.S. Resilience Project, Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices.[56] This report includes a discussion of supply chain transparency and trust, including the following best practices:
  - Vetting vendors as part of the Request for Proposal (RFP) process through upfront security review and analysis.
  - Performing risk assessments on all new suppliers, and requiring third-party evaluation of significant new vendor-sourced components.
  - Gaining visibility into who suppliers are by using multiple sources to perform financial, legal, and background checks on vendors to make sure they are qualified.
  - Qualifying supplier manufacturing processes and procedures.
  - Validating vendor supply chain security practices: real-time chain of custody controls with electronic verification, validation and authentication.
  - Working with trusted vendors to assess, qualify and manage their suppliers.
  - Engaging in face-to-face interaction with multiple tiers of suppliers to communicate needs and expectations for security, integrity, and resilience.
- Utilities Telecom Council (UTC), Cyber Supply Chain Risk Management for Utilities — Roadmap for Implementation. [57] This report includes a discussion of best practices for identifying and prioritizing vendors and sub-tier suppliers and cyber security practices utilized by each. The report points out that various standards and best practices use different terms for different types of suppliers, based on the complexity (i.e., system integrator vs. minor component supplier) and length in time of the utility-vendor relationship. Also discussed is knowledge of vendor practices such as explicit processes to purchase parts from authorized resellers, having standardized contractual language that addresses security concerns, and propagating those security requirements down the supply chain, etc.

6.2.5 Mitigate Assessed Risk (2): Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk

[56] NIST, U.S. Resilience Project, Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices, 2012. https://usresilienceproject.org/wp-content/uploads/2014/09/report-Supply_Chain_Solutions_for_Smart_Grid_Security.pdf
[57] Utilities Telecom Council, Cyber Supply Chain Risk Management for Utilities — Roadmap for Implementation, April 2015. https://utc.org/wp-content/uploads/2018/02/SupplyChain2015-2.pdf

- The President's National Infrastructure Advisory Committee (NIAC) Report, Transforming the U.S. Cyber Threat Partnership.[58] This report provides two critical recommendations relevant to cyber supply chain security: 1) Provide liability protection to allow blacklisting and whitelisting of critical cyber products used in private critical infrastructure, similar to the authority provided in 10 CFR Part 21 for the nuclear industry and to the DOE enhanced procurement authority; and 2) Continue and expand programs at DOE national laboratories and other ongoing sector-specific initiatives to independently test vendor equipment for vulnerabilities and report the results to private companies.

- NATF Report, Cyber Security Supply Chain Risk Management Guidance. This report offers a variety of detailed considerations regarding vendor requirements that should form part of an entity's cyber supply chain risk management plan above and beyond NERC regulatory requirements: 1) Vendor Asset, Change, and Configuration Management Controls; 2) Vendor Supply Chain Risk Management Governance Structure and Processes; 3) Logging and Monitoring Procedures; and 4) Information Protection Procedures.

- APPA and NRECA Report, Managing Cyber Supply Chain Risk-Best Practices for Small Entities. This report includes an assessment of the potential importance of standard contract language for vendors as a viable tool for all registered entities, large and small, to mitigate supply chain risk. Third-party accreditation of vendor-provided hardware and software or vendor self-certification against recognized national-level supply chain standards also are discussed as an important potential measure above and beyond current regulatory requirements. Additional vendor controls discussed include: vendor remote system access and software and patch integrity, authentication, and testing.

- DOE Cybersecurity Procurement Language for Energy Delivery Systems.[59] This model procurement language by the ESCC's Energy Sector Control Systems Working Group as a baseline for cybersecurity procurement language applicable to OT systems, although it can be applied more broadly. The model language incorporates the following: 1) General cybersecurity procurement language (software specifications; access control; account management, authentication, password policy, logging and auditing, malware detection and protection); 2) 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 3) Intrusion detection (host intrusion; network intrusion).

[58]NIAC Report, Transforming the U.S. Cyber Threat Partnership, December 19, 2019, page 11. https://www.cisa.gov/sites/default/files/publications/NIAC-Transforming-US-Cyber-Threat-PartnershipReport-FINAL-508.pdf

[59] DOE, Cybersecurity Procurement Language for Energy Delivery, April 2014. See: https://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014.

- EEI, Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk.[60] This document contains model procurement language corresponding to the Requirement R1.2 as specified in CIP-013-1. This model language below provides Registered Entities a consistent, tailorable set of contract provisions to address CIP-013-1 security controls within their own respective contracting environments.
- EIS Council Cyber Product International Certification (CPICTM) Commission Initiative.[61] This report argues for the establishment of a private sector-led and endorsed cyber product certification process developed in coordination with government agencies and grounded in supply best practices and recognized international standards.

- The Public-Private Analytic Exchange Program, Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions.[62] This report provides a series of recommendation to address cyber supply chain risk by: 1) decreasing the likelihood of risk across a product/service life-cycle; and/or 2) decreasing the consequences of risk. Novel recommendations not covered by other reports in this section include the following: 1) Prioritize and apply resources to change business models to better protect the electricity grid (including improved risk valuations with insurance companies and accounting for security processes and capital investments as part of an entity's business valuation); and 2) Incorporate entity employee and vendor education, training, and awareness relating to cyber supply chain security into corporate policy and practices.

- NIST, U.S. Resilience Project, Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices.[63] This report calls for increased use of technology on the part of both industry entities and suppliers to help mitigate cyber supply chain risk within the U.S. electric industry. This includes "track and trace" technologies and sensor networks to enhance shipment security, intelligent packaging to thwart counterfeiting, anomaly detection tools, and analytic tools to identify geographic-related and vendor-specific risks and assess risk holistically, automate risk assessment, identify anomalies, and map supply chain tiers. Additional countermeasures discussed in the report include the following:
    - Adopting secure software development methodologies that make it harder to insert modifications.
    - Instituting secure coding standards.

[60] EEI, Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk, March 2019.
[61] EIS Council, Securing Critical Supply Chains, June 19, 2018. See: https://www.eiscouncil.org/App_Data/Upload/8c063c7c-e500-42c3-a804-6da58df58b1c.pdf
[62] The Public-Private Analytic Exchange Program, Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions, 2017. See: https://www.odni.gov/files/PE/Documents/11---Supply-Chain-Risks-of-SCADA-Industrial-Control-Systems-in-the-Electricity-Sector_Risks-and-Mitigations.pdf

[63] NIST, U.S. Resilience Project, Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices, 2012. https://usresilienceproject.org/wp-content/uploads/2014/09/report-Supply_Chain_Solutions_for_Smart_Grid_Security.pdf

- Including contract language regarding supplier security and quality standards, and requirements for certification testing and vendor management controls.
- Using stringent test protocols, including penetration testing to check attack vectors and develop internal databases to understand attack surfaces of products.
- Conducting security, interoperability, and functional tests prior to product installation.

- Institute of Electrical and Electronics Engineers (IEEE) Standards. IEEE has developed and issued a number of standards that address cyber security concerns, including those related to DERs.[64] These include:
  - IEEE 547-2018—IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Power Systems Interface
  - IEEE 1547.3—IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems
  - IEEE C37.240—IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems
  - IEEE 1686—IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities
  - IEEE C118 series of standards—Data management and protection of synchrophasors
  - IEEE 1711—IEEE Standard for Serial SCADA Protection Protocol for Substation Serial Link Cybersecurity

7.0 SUPPLY CHAIN STANDARDS AND BEST PRACTICES EXTERNAL TO THE ELECTRIC INDUSTRY: LEARNING FROM OTHERS

7.1 Overview

To this point, this report has provided an assessment of cyber supply risk and regulatory measures and best practices to help mitigate that risk within the U.S. electric industry. Importantly, cyber supply chain risk and corresponding risk management challenges are an increasingly common concern across government and other industry sectors as well. Accordingly, a variety of government agencies and other industries that face significant supply chain risks have worked to develop and/or adopt and implement standards and best practices designed to address such risks. This section presents a summation of various standards and best practices in use elsewhere that may offer solution paths to address gaps in cyber supply chain

[64] NREL, An Overview of Distributed Energy Resource (DER) Interconnection: Current Practices and Emerging Solutions, Technical Report NREL/TP-6A20-72102, April 2019, page 48.

risk management not covered under the approved regulatory standards construct for the U.S. electric industry.

7.2 Summary of "Out-of-Sector" Standards and Best Practices

Table 4 below presents a summary of "out-of-sector" standards (or portions thereof) and best practices with the potential to enhance cyber supply chain security within the U.S. electric industry. This summary is presented in alignment with the model framework discussed in Section 4.0 above.

Table 4. Summary of "Out-of-Sector" Standards and Best Practices

Title	National Supply Chain Risk Management Practices for Federal Information Systems (NISTR 7622)
Responsible Organization	NIST
Purpose/Highlights	Provide federal 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
Risk Issue(s) Addressed	- Traceability in supply chain processes and supplier relationships - Security controls
Relevance to Model Framework	- Create and Continuously Validate a Trusted, Risk Management-focused Supplier Network - Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk
Title	Secure Product Development Life-Cycle Requirements (IEC 62443-4-1)
Responsible Organization	International Electrotechnical Commission (IEC)
Purpose/Highlights	Defines secure development life-cycle (SDL) for developing and maintaining secure products, including security requirements definition, secure design and coding, installation, verification/validation, defect management, patch management and product end-of-life disposal
Risk Issue(s) Addressed	- Product-specific threat modeling - Life-cycle security processes, including secure coding
Relevance to Model Framework	- Establish and Maintain Multi-dimensional Information Sharing Partnerships and Technical Capabilities - Select Strategic Approach and Conduct Analysis to Identify/ Prioritize Risks - Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk
Title	Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition (NIST SP 800-53)

Responsible Organization	NIST
Purpose/Highlights	SA-12 – Supply Chain Protection SA-3 - System Development Life Cycle SA-22 Unsupported System Components
Risk Issue(s) Addressed	- Access control - Security assessment - Configuration management - Contingency planning - Identification and authentication - Incident response Maintenance - Physical and environmental protection - Provenance - Risk assessment - System and services acquisition - System and communications protection - Unsupported technologies update - System and information integrity
Relevance to Model Framework	Strategic Approach and Conduct Analysis to Identify/ Prioritize Risks - Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk
Title	Federal Risk and Authorization Management Program (FedRAMP)
Responsible Organization	General Services Administration
Purpose/Highlights	A federal government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services
Risk Issue(s) Addressed	Independent assessment of cloud providers' security implementations and overall risk posture of a cloud environment
Relevance to Model Framework	- Select Strategic Approach and Conduct Analysis to Identify/ Prioritize Risks - Create and Continuously Validate a Trusted, Risk Management-focused Supplier Network - Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk
Title	Information Security Management (ISO/IEC 27017)
Responsible Organization	International Standards Organization (ISO)/IEC
Purpose/Highlights	Systems Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
Risk Issue(s) Addressed	Security controls for cloud services
Relevance to Model Framework	- Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk

Title	Supply Chain Risk Management Practices for Federal Information Systems and Organizations (NIST SP 800-161)
Responsible Organization	NIST
Purpose/Highlights	Provides guidance to federal agencies on identifying, assessing, and mitigating information and communications technology (ICT) supply chain risks over the entire life-cycle of systems, products, and services
Risk Issue(s) Addressed	Traceability in supply chain processes and supplier relationships (including integrators and sub-tier suppliers)
Relevance to Model Framework	- Select Strategic Approach and Conduct Analysis to Identify/ Prioritize Risks - Create and Continuously Validate a Trusted, Risk Management-focused Supplier Network - Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk
Title	Quality Management Systems (ISO9001)
Responsible Organization	ISO
Purpose/Highlights	- Requirements for a quality management system, including documented information, planning, and determining process interactions - Management of resources, including human resources and organizational work environment - Product realization, including steps from design to delivery - Measurement, analysis, and quality assurance via internal audits and 3rd party accreditation process and independent reviews
Risk Issue(s) Addressed	- Quality process controls - Independent assessments of vendors and vendor-provided information
Relevance to Model Framework	- Select Strategic Approach and Conduct Analysis to Identify/ Prioritize - Risks - Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk
Title	Notional Supply Chain Risk Management Practices for Federal Information Systems (NISTIR 7622)
Responsible Organization	NIST
Purpose/Highlights	Provide federal 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
Risk Issue(s) Addressed	- Provenance of Elements, Processes, Tools, and Data via Configuration Management (CM) for documenting and tracking changes - Robust identity management and access control to establish and record authorized or unauthorized activities or behavior - Identification/ tagging of elements, processes, roles, organizations, data, and tools

Relevance to Model Framework	- Create and Continuously Validate a Trusted, Risk Management-focused Supplier Network - Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk
Title	Open Trusted Technology Provider Standard (O-TTPS) -- Mitigating maliciously tainted and counterfeit products (ISO/IEC 20243)
Responsible Organization	The Open Group
Purpose/Highlights	Provides a set of guidelines to help mitigate the threat posed by assure against maliciously tainted and counterfeit products throughout commercial off-the-shelf (COTS) information and communication technology (ICT) product lifecycles
Risk Issue(s) Addressed	- Design and engineering controls - Open source handling
Relevance to Model Framework	- Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk
Title	Information technology — Security techniques — Information security for supplier relationships (ISO/IEC 27036)
Responsible Organization	ISO/IEC
Purpose/Highlights	Part 1: provides an overview and concepts of information security in supplier relationships Part 2: outlines a high-level framework for establishing information security requirements and expectations in supplier relationships Part 3: provides guidelines to acquirers and suppliers for managing information security risks associated with information and communication technology (ICT) products and services supply chain Part 4: provides guidelines to vendors and customers for information security of cloud computing services throughout the supplier relationship life-cycle
Risk Issue(s) Addressed	- Supplier relationship management - Product/service life-cycle risk controls
Relevance to Model Framework	- Create and Continuously Validate a Trusted, Risk Management-focused Supplier Network - Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk
Title	Software and Supply Chain Assurance Forum
Responsible Organization	Co-led by DHS, GSA, and DOD
Purpose/Highlights	Provide actionable information about supply chain risks and mitigations to users, buyers, manufacturers and sellers of tech products

Risk Issue(s) Addressed	- Supply chain risk assessment capability - Communications, notification, and information sharing regarding cyber supply chain risks - Qualified bidder and manufacturer lists through implementation of a robust process for validating and approving the security practices of companies and the security characteristics of ICT products and services - Technical assistance in developing and implementing supply chain risk management capabilities
Relevance to Model Framework	- Establish and Maintain Multi-dimensional Information Sharing Partnerships and Technical Capabilities - Create and Continuously Validate a Trusted, Risk Management-focused Supplier Network - Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk

7.3 Cyber Supply Chain Risk Management Industry Case Studies

In addition to its ongoing work with respect to standards development, benchmarking, and continuous improvement, the NIST has engaged with leaders across numerous industries to compile a series of case studies highlighting best practices for cyber supply chain risk management. These case studies represent "success stories" that should be considered by leaders within the U.S. electric industry to address key cyber supply chain risk management challenges that currently fall outside of regulated space. The following case studies provide representative best practice applications that cut across many or all of the individual components of the model framework presented in Section 4.0 above:

- **Dupont: Crop Protection Operating Disciplines for Supply Chain Sustainability, Risk Management and Resilience.**[65] Specific areas of focus discussed in this case study include:
  - Integrated supply chain operations across lines of business
  - Cyber supply chain risk management governance (vertical and horizontal)
  - Risk assessment and prioritization via quantified scoring
  - Contract manufacturer selection, oversight, and differentiated management
  - Supply chain quality
  - Security in transit
- **Northrop Grumman Corporation: Trusted, Innovative, World-Class Supply Chain.**[66] Specific success areas discussed in this case study include:
  - Overarching, cross-business governance structure and Supply Chain Leadership Council used to coordinate best practices and information sharing across the company
  - Program-level, cross-functional subcontractor management teams that collaborate to oversee all aspects of supplier performance
  - Supplier Assessment Management System (SAMS) providing objective measurement criteria for supplier performance in eight major categories
  - Life-cycle approach to the management of cyber supply chain risks

[65] See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_DuPont_071315.pdf
[66] See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Northup_081615.pdf

  - Use of an automated tool to measure supplier supply chain management performance

- **John Deere: Supply Chain Risk Management.**[67] Specific areas of focus discussed in this case study include:
  - Board of director engagement in supply chain continuity, and compliance and mitigation actions
  - Use of a Enterprise Supply Chain Risk Council as a voice representing different divisions and regions of the company to promote common tools to manage, mitigate, and rate capacity planning or financial risks across all platforms
  - Conduct of strategic risk assessments before a supplier or product is chosen
  - Engagement of an independent company to analyze the financial health of private and public suppliers
  - Use of "approved supplier" lists and including a compliance check, financial audit, advanced quality audits, and assessments prior to onboarding a supplier
  - Requirement of mitigation plans developed by suppliers to address identified risks
  - Close coordination between supply chain and business continuity focal points
- **Resilinc: Leveraging Supply Chain Risk Intelligence for Strategic Advantage.**[68] Specific success areas discussed in this case study include:
  - Leveraging the power of advanced supply chain intelligence by enabling the broader organization to access it and leverage it for various purposes
  - Automated solutions to map complex supply chains to the first and sub-tier levels, including component, product, and equipment data. Solutions employed extend to assessments of supplier business continuity plans, corporate social responsibility compliance, and parts change notifications
  - Automated data collection from suppliers utilizing standardized questionnaires, improved system access for suppliers, and information sharing networks linking primary and sub-tier suppliers

[67] See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Deere_081915.pdf
[68] See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Resilinc_081915.pdf

- **Exelon Corporation: Cybersecurity Supply Chain Risk Management.**[69] Specific areas of focus discussed in this case study include:
  - Addresses supply chain risk management through an extended definition of supplier, including the entire supply chain ecosystem of vendors and their suppliers, service providers, and third parties
  - Cross-functional vendor management including supply chain, security, legal and IT representatives to assess contract terms and conditions and ensure that appropriate contract controls are in place
  - Use of extensive vendor security questionnaires that include a wide variety of questions related to vendor cyber supply chain policies, process, and controls
  - Adoption of specific security control and audit provisions in vendor contracts
- **Procter & Gamble: Excellence in Supply Chain Risk Management.**[70] Specific success areas discussed in this case study include:
  - Overarching corporate governance model for cyber supply chain risk management in which Corporate Engineering oversees supply chain risk management (SCRM) efforts and works with Product Supply teams within the Global Business Units to promote SCRM best practices and processes.
  - Frequent reporting on SCRM efforts and progress to the Board of Directors and CEO.
  - Supply chain risk evaluated from a "risk versus reward perspective" by front line management, and then pushed up the management chain for decision
  - Multi-functional and multi-level risk assessments
  - Conduct of a variety of audits and reviews with tier one suppliers, ranging from rigorous multi-day onsite audits to periodic reviews

8.0 ASSESSING WHAT'S BEEN DONE: VENDOR ACTIONS

8.1 Overview

[69] See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Exelon_102215_05.pdf
[70] See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_PandG_072415.pdf

As demonstrated by many of the standards and best practices discussed in the summaries provided in the previous two sections, supply chain risk factors increasingly are being evaluated by entities within the U.S. electric industry as part of the supplier vetting process. Additionally, many companies include various supply chain control requirements in supplier agreements and contract language. Key cyber supply chain risk management considerations evaluated for supplier vetting and included in contract requirements include things like documentation of the supplier risk profile, security governance, risk assessment processes (including assessment of risks represented by sub-tier suppliers), physical/cybersecurity and access controls, personnel surety, security awareness and training programs, software and hardware integrity and testing, component security in-transit, self- and third party-audit programs, etc.

Vendors themselves have become increasingly aware of the business drivers behind the need to ramp up life-cycle management of the cyber supply chain risks they present. These drivers include both recognition of the direction in which buyers are moving, as well as the need to mitigate the risks they face from sub-tier suppliers across their own supply chains. Accordingly, many vendors have pursued actions to address their cyber supply chain risk profiles, get ahead of the ball regarding compliance with more robust buyer screening and contracting requirements, and recognize and manage the risks inherent in their own cyber product and service supply chains.

Additionally, many vendors have engaged in partnerships with various government agencies to seek collaborative solutions to address cyber supply chain risks. One such partnership is the **DHS Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force.**[71] The ICT SCRM Task Force's participants include 20 federal partners as well as 40 of the largest companies in the Information Technology and Communications Sectors, many of which are key electric industry suppliers. Task Force activities include assembling an inventory of existing supply chain risk management efforts across government and industry, as well as four ongoing work streams:

- Development of a common framework for the bi-directional sharing of supply chain risk information between government and industry;
- Identification of processes and criteria for threat-based evaluation of ICT supplies, products, and services;
- Identification of market segment(s) and evaluation criteria for Qualified Bidder and Manufacturer List(s); and

[71] See https://www.dhs.gov/cisa/supply-chain-risk-management

- Producing policy recommendations to incentivize the purchase of ICT from original manufacturers or authorized resellers.[72]

8.2 Cyber Supply Chain Risk Management Vendor Case Studies

In addition to its ongoing work with the "buyer" community, the NIST has engaged with leaders across the IT/OT and communications vendor communities to develop a series of case studies highlighting best practices for cyber supply chain risk management from the supplier perspective. These case studies represent additional "success stories" that should be reviewed by leaders within the U.S. electric industry for consideration with respect to supplier screening and contracting requirements. The following case studies provide best practice applications that cut across many or all of the individual components of the model framework presented in Section 4.0 above.

- **Cisco®: Managing Supply Chain Risks End-to-End.**[73] Specific areas of focus discussed in this case study include:
  - Integrated approach to corporate governance for cyber supply chain supply chain including horizontal collaboration across 30 business units and key headquarters functional areas, including: Resilience, Quality, Physical and Cyber Security, Sustainability, and Compliance.
  - Use of a comprehensive supply chain security master specification that sub-tier suppliers must abide by, including 180 requirements across 11 security domains.
  - Up-front vetting of sub-tier suppliers against a number of criteria, including performance, financial stability, quality, and security.
  - Regular audits of sub-tier suppliers by security and IT security teams, as well as audits on financial and regulatory risks.
  - Controls focused on the risks of counterfeit or tainted products and misuse of intellectual property.
  - Jointly investments with contract manufacturers to achieve Highly Protected Risk (HPR) status from the property insurer for critical sites.
  - Use of high-powered analytics to determine which components, suppliers, and manufacturing sites are most at risk.

[72] Ibid.
[73] See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Cisco_071515.pdf

- Supply chain risk trend analysis and a multi-pronged 24/7 "sensing function" supported by a live feed of events around the world that could impact supply chain locations and operations.
- Establishment of a supply chain incident management team and routine supply chain event drills.
- Sub-tier supplier mapping and regular update of robust supplier data inventories across functional areas.
- Robust component and technology testing prior to production.
- Use of a propriety software system that provides real-time visibility into the production processes and quality controls of outsourced manufacturers, including yields, component defect rates, test results, and all other production information from all sites.

- **Juniper Networks: Ensuring a Remarkable Customer Experience.**[74] Specific success areas discussed in this case study include:
  - Establishment of a Supply Chain Risk Council which convenes functional area representatives from throughout the organization to regularly and proactively review risks, as well as mitigation plans.
  - Up-front sub-tier supplier vetting across key corporate functional areas.
  - Robust supplier relationship management program which is developed and strengthened through a number of program elements, including regular performance reviews, strategy alignment sessions, and performance metrics.
  - Comprehensive supplier management framework including the following key components: Supplier Performance Evaluation (includes a Supplier Excellence Framework and Business Continuity Maturity Matrix); Verification and On-site Audit; Certification and Internal Accountability to ensure compliance with the Juniper Networks Code of Conduct; and Training.
  - Uses of an external vendor to monitor global events, map supply chains and corresponding risks, and identify potential impacts.
  - Institution of a Software Development Lifecycle Program with various specific controls to improve the security, quality, and performance of software products (includes security training for developmental engineers).

[74] See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Juniper_081415.pdf

- Component integrity by limiting outsourced purchases to known, authorized vendors.
- Robust in-transit component security program including active monitoring and tracking.
- Routine physical audits on contract and original design manufacturers.

- **Intel Corporation: Managing Risk End-to-End in Intel's Supply Chain.**[75] Specific areas of focus discussed in this case study include:
  - Supply chain risk management spans multiple business units and functional groups, coordinated through a centralized Technology and Manufacturing Group (TMG) with oversight over all wafer fabrication factories, assembly and test plants that convert the wafer into finished integrated circuits, warehousing and shipping of finished goods, and commodity management of all incoming materials used by these operations.
  - Use of specialized tools and methods to audit provenance claims of a part at any location in the supply chain, prior to installation into a platform, and in-situ.
  - Supplier selection process that considers many factors such as quality, availability, and security to develop mitigation plans that compensate for sub-tier suppliers that do not represent a previous long-term relationship and proven track record with Intel.
  - Institution of a set of policies, procedures, tools, indicators, and consulting practices that cover the Security Development Lifecycle (SDL) to help the company determine whether a product meets technical specifications, delivers to security specifications, supports the protection of privacy and personal information, and does not contain malicious software or hardware when shipped.
  - Use of specific security controls to guard against the infiltration of malicious firmware, counterfeit sub-assemblies, and counterfeit Integrated Circuits (ICs).
  - Robust product testing and evaluation.
- **NetApp: Anticipate, Mitigate, Improve.**[76] Specific success areas discussed in this case study include:

[75] https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Intel_100715.pdf

[76] See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_NetApp_062315.pdf

- Employment of cross-functional teams that address specific risks which cut across the enterprise, including information security and supply chain risks.
- Use of a risk scoring methodology for both components and suppliers, built from NetApp's Bill of Materials (BOM) and based on information from industry tools, such as Silicon Expert, which provides engineering, life-cycle status, available inventory and environmental compliance data on 300 million electronic components — and NetApp's own supplier risk assessments.
- Use of U.S.-based, third party certifiers to audit suppliers, verify that all requirements have been met, and provide consistent reporting.
- Comprehensive mapping of supply chain and assessed time-to-recovery for each supplier site in case of disruption to identify the hot spots and areas in need of attention.
- Robust hardware and software integrity policies and programs extended to outsourced providers.
- Achievement of U.S. government Customs-Trade Partnership Against Terrorism (CTPAT) certification — a process that help build bridges and stronger lines of communication between supply chain risk management, security, and NetApp's suppliers.

- **Fujitsu Network Communications: Managing Supply Chain Risks in Optical and Wireless Networking.** [77] Specific areas of focus discussed in this case study include:
  - Multi-component, cross-functional governance for cyber supply chain risk management.
  - Multi-level vendor screening including financial assessment, quality control system processes and systems assessment, and verification that individual vendor products meet Fujitsu specifications.
  - Use of site assessments for new suppliers with quality and security as key points of focus.
  - Conduct of quarterly key Supplier Performance Reviews (SPR) of individual suppliers.
  - Introduction of a structured New Product Introduction (NPI) process for hardware products, including the performance of numerous product performance validation tests and periodic re-testing throughout the NPI process.

[77] https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Fujitsu_091615.pdf

- Use of robust software verification and testing processes.
- Development of advanced threat intelligence and analytics capability with near real time and trend reporting components.
- Use of a Secure Remote Development Extranet for partner communications and data-sharing.
- Use of the Global Information Security Controls (GSIC) framework, closely modeled on the ISO 27001 standard, to provide a baseline for IT risk assessment and management and carried forward into the supplier's contractual obligations for certain risk levels.

9.0 SYNOPSIS OF RECOMMENDATIONS

9.1 Overview

Section 5.0 above provided an analysis of the NERC CIP Supply Chain Standards, including a look at regulatory requirements that collectively represent an important new baseline for enhancing cyber supply chain risk management for covered high and medium-impact BES Cyber Systems across numerous key risk issues. Aspects of the various measures to be put in place to achieve compliance with these requirements also can help inform efforts and approaches to improve cyber supply chain risk management in the context of non-regulated segments of the industry, such as low-impact BES Cyber Systems and local power distribution systems. This will become more evident as information is collected and lessons learned are compiled as part of the standards implementation process. The various non-regulatory activities being pursued by the NERC concurrent with the standards implementation process as highlighted in Section 5.0 undoubtedly will offer additional insight and inform the development of a variety of guidelines that should be considered for adoption by the non-regulated aspects of the U.S. electric industry.

Going beyond the regulatory framework, Sections 6.0-8.0 above highlighted a number of ongoing activities, initiatives, public-private sector collaboration forums, and government and industry best practices that represent additional non-regulatory approaches to strengthen cyber supply chain risk management across the U.S. electric industry. These approaches – including the additional information provided via the "out-of-sector" standards references and model case studies examined in Sections 7.0 and 8.0, respectively – also should be considered by "buyers" and "suppliers" (including both integrators and sub-tier component suppliers) alike within the industry to jointly achieve shared cyber supply chain risk management objectives.

This section of the report draws from the information and analysis provided in Sections 5.0-8.0 above to outline a broad-based set of recommendations to tackle key issues and challenges not

addressed by or that fall outside the scope of the NERC Supply Chain Standards. These recommendations are generally relevant across the BES Cyber System (all impact levels) and local power distribution system communities. The recommendations summary that follows is presented in alignment with the model framework discussed in Section 4.0 above.

9.2 Recommendations Organized by Model Framework Component

9.2.1 Establish Corporate Governance and Set the Direction for Cyber Supply Chain Risk Management

- **Develop a set of best practices-based considerations regarding corporate governance, oversight, and policy for cyber supply chain risk management.** Increasing corporate senior executive attention, fostering appropriate vertical and horizontal coordination and synchronization of the approach to supply chain risk issues, and establishing comprehensive enterprise supply chain risk management policies and practices are fundamental to achieving success. As evidenced by the information captured in Sections 6.0-8.0, there is a wide body of knowledge currently available to help inform corporate governance approaches regarding cyber supply chain risk management. The idea is not to attempt to develop a "one-size-fits-all" approach, but rather to provide examples of best practices-based approaches and case study successes to help companies consider a variety of different factors when putting in place the governance model that best meets their needs. With this in mind, major associations within the U.S. electric industry should work together to develop a compendium of best practices and case studies that provide insight into proven cyber supply chain governance models and policy options. The NATF Report, Cyber Security Supply Chain Risk Management Guidance, APPA and NRECA Report, Managing Cyber Supply Chain Risk-Best Practices for Small Entities, and the NIST - U.S. Resilience Project Report, Best Practices in Cyber Supply Chain Risk Management, and the various case studies included in sections 7.0 and 8.0 above collectively represent a solid baseline of information to support such an effort.

- **Develop enterprise training programs for cyber supply chain risk management.** Managing the risks associated with complex and distributed cyber supply chains requires the development and implementation of appropriate training programs at various levels of corporate governance and across various functional areas of a given buyer or supplier company. DHS, DOE, and organizations such as the ESCC and major industry associations should work together to develop model training programs including core elements addressing supply threats, life-cycle vulnerabilities, business impacts, and corresponding mitigations.

- **Incorporate cyber supply chain risk considerations into company- and sector-level exercise activities.** In recent years, DHS, DOE, and an array of private sector entities within the U.S. electric industry have collectively and/or individually designed, developed, and conducted a variety of exercise activities that explore the ever-growing cyber threat to industry assets and systems. These activities should be expanded to address various cyber supply chain risk scenarios. Incorporation of cyber supply chain risk issues into the design, development, and conduct of national level exercises such as GRIDEX and the DHS National Exercise Program also should be strongly considered.

9.2.2 Establish and Maintain Multi-dimensional Information Sharing Partnerships and Technical Capabilities

- **Expand industry "buyer" and "supplier" participation in important cyber threat and multi-dimensional public-private information sharing partnerships.** Engagement in core partnership activities with entities and working forums such as the E-ISAC, Multi-State ISAC, ESCC, DHS ICT SCRM Task Force, Tri-Sector Executive Working Group, Public-Private Analytic Exchange Program, etc., provides access to a variety of cyber security information ranging from threat alerts and warnings, to information regarding mitigation of common vulnerabilities, to best practices and lessons learned from the response to real-world cyber threats. Various examples of successful, proven public-private partnerships with direct relevance to cyber supply chain risk management are provided in Sections 6.0-8.0 above.

- **Support continued expansion of specific government-industry collaboration and information sharing programs to jointly address cyber supply chain risk.** An example of a proven capability in this regard is the Cyber Risk Information Sharing Program (CRISP). Co-funded by DOE and industry and managed by the E-ISAC, CRISP is designed to provide electric utilities the capability to voluntarily share cyber threat data in near-real-time, analyze this data using federal government-derived intelligence, and receive time-sensitive machine-to-machine threat alerts and mitigation measures. DOE and DHS should undertake a concerted effort to expand industry participation in CRISP, as well as to share anonymized threat information more broadly across the industry. Similarly, industry should support the continued evolution of DOE's Cybersecurity for the OT Environment (CyOTE™) program. CyOTE™, in its current pilot phase, is focused on demonstrating two-way data sharing and analysis within the complex OT environment, where utilities currently have less mature tools for threat detection. The results from these pilots are expected to inform the development of a repeatable, standardized approach that industry can use to support real-time OT threat data sharing and analysis.

9.2.3 Select the Corporate Cyber Supply Chain Risk Management Strategic Approach and Conduct Analysis to Identify/Prioritize Risks

- **Develop best practices-based guidelines and tools that help buyers and suppliers plan and conduct comprehensive assessments of cyber supply chain risk.** Cyber supply chain risk analysis involves a number and variety of complex factors, including the assessment of security, integrity, and reliability across a product/service life-cycle; identification and examination of complex sub-tier supplier networks; and a mix of personnel surety, physical security, and cybersecurity considerations. Bringing the right information to light in a format that is transparent and easy-to-understand and visualize on the part of corporate decision makers is incredibly important. In this light, industry entities and associations should work with government agencies and standards-setting organizations to develop criteria, factors for consideration, and operating guidelines that can inform the development of industry cyber supply chain risk assessment methodology and supporting tools. DOE's Cyber Security Capabilities Maturity Model (C2M2) provides a good baseline for such an effort based on its consideration of supply chain risk as a process of identifying and managing external dependencies.

9.2.4 Mitigate Assessed Risk (1): Create and Continuously Validate a Trusted, Risk Management-focused Supplier Network

- **Develop best practices-based guidelines that help buyers and suppliers to establish and monitor traceability in supply chain processes and supplier relationships.** Sections 6.0-8.0 provide examples of recognized standards and best practice case studies that can be used to support a set of model guidelines for this risk issue, including the NIST's National Supply Chain Risk Management Practices for Federal Information Systems (NISTIR 7622).

- **Develop best practices-based guidelines to support the "up-front" screening of potential industry vendors.** Sections 6.0-8.0 provide numerous examples of recognized standards and best practice case studies that can be used to support the development of a set of model guidelines for this risk issue, including recommendations provided in the NAGF's Cyber Security Supply Chain Management White Paper and the NIST's Best Practices in Vendor Selection and Management.

- **Support efforts to develop an accreditation model with specific criteria to identify and qualify vendors with strong supply chain risk management practices.** This activity should leverage the experiences and practices of those elements of the U.S. electric industry and other industries that employ independent assessments or third-party accreditations of their vendors as part of their supply chain risk management strategy. Many of the case studies presented in Section 8.0 above also can serve as benchmarks

to guide progress in this effort. Collaborative efforts between DHS and vendors to develop Qualified Buyer and Manufacturer Lists via the ICT SCRM Task Force is also driving progress to mitigate this risk issue.

- **Support the establishment of a cyber product/service certification process.** This recommendation is focused on the establishment of a private sector-led and endorsed cyber product/service certification process developed in coordination with government agencies and grounded in best practices and recognized standards for supply chain risk management. The operating premise is "strength-in-numbers," that is, an economy-of-scale solution based on a common approach adopted by diverse entities operating both domestically and globally can have far greater impact than a single or small number of entities attempting to develop a solution for a truly global marketplace.

9.2.5 Mitigate Assessed Risk (2): Implement Controls to Manage Cyber Supply Chain "Life-Cycle" Risk

- **Incorporate cyber supply chain threat- and vulnerability- informed language into vendor contract specifications.** Industry buyers and suppliers should tailor cyber supply chain risk mitigation specifications contained in vendor contracts to specific risks as identified via product- and service- specific threat and vulnerability modeling, other information sources, and industry best practices. Model contract language developed by DOE and EEI can be tailored to align with specific buyer and supplier operating and risk environments, as well as industry trends. Information provided in IEC Standard IEC 62443-4-1 also is particularly relevant to this proposed activity.

- **Support efforts to develop guidelines focused on the voluntary application of cyber supply chain risk management, plans, processes, and practices in the context of low-impact BES Cyber Systems and local power distribution systems.** This effort is a critical aspect of engaging the non-regulated segments of the U.S. electric industry in a comprehensive and holistic approach to cyber supply chain risk management based on demonstrated best practices in use by industry peers and government agencies. NERC has now recommended modification to the Supply Chain Standards to include low impact BES. Such guidelines would also apply in the context of local power distribution systems across the industry.

- **Establish best practices–based guidelines for unsupported and open-sourced technology component risk mitigation.** Industry entities should be cognizant of and develop plans to mitigate potential risks posed by systems where patch sources are no longer available, as well as for patching and otherwise supporting systems or components that rely upon open source technology. In light of this specific risk issue and in concert with the implementation of the Supply Chain Standards, NERC has committed to work with work via its CIPC Supply Chain Working Group develop a consensus-based guideline for industry consideration.

- **Engage with product manufacturing standards bodies to ensure that supply chain risks and vulnerabilities are addressed in cyber hardware and software specifications.** Computer hardware and software products and technologies used to support both BES Cyber Systems and local power distribution systems may be defective or possess code that can be manipulated across the product life-cycle to impact system operability. All hardware and software products and technologies should be validated and tested appropriately to prevent and/or mitigate the impacts of unintentional defects or deliberate manipulation.

- **Support efforts to provide liability protection to allow "blacklisting" and "whitelisting" of critical cyber products used in private critical infrastructure.** This recommendation

is based on a recent NIAC report and reflects similar authority provided in 10 CFR Part 21 for the nuclear industry and additional relevant authority provided to DOE via the National Defense Authorization Act for Fiscal Year 2014. It is intended to combat the threat of hostile or competitor nation-states introducing defective or counterfeit components and/or malware into digital equipment used in critical infrastructure operations. Private-sector efforts to address this threat via company-to-company reporting are hampered by the fact that existing cyber-attack reporting requirements do not limit the liability of an entity that reports critical, time-sensitive threat or vulnerability information. This recommendation involves new or the modification of existing statutes/regulations to provide the required liability protection.

- **Support the expansion of programs at DOE national laboratories to independently test vendor equipment for vulnerabilities and report the results to private companies.** A recent NIAC report and DOE's Multi-year Plan for Energy Sector Cybersecurity, both highlight the key role the federal government can play in the independent testing and validating of vendor equipment. This includes analyzing systems and component vulnerabilities, malware threats, and impacts of zero-day threats on energy infrastructure. Industry reinforcement of the importance of this government capability and appropriate resourcing is critical.

- **Support major ongoing activities of the DHS ICT SCRM Task Force.** Three major focus areas are particularly relevant to this aspect of the model framework presented in this report: 1) Identification of processes and criteria for threat-based evaluation of ICT supplies, products, and services; 2) Identification of market segment(s) and evaluation criteria for Qualified Bidder and Manufacturer List(s); and 3) Producing policy recommendations to incentivize the purchase of ICT from original manufacturers or authorized resellers. The outputs of these three work streams undoubtedly will be very relevant to the advancement of cyber supply chain risk management across multiple industry sectors, including electricity. At this point, participation in this DHS-led program appears to be very vendor-centric. It is recommended that DHS open the aperture of this program to allow participation in and input from key elements of the "buyer side" of the U.S. electric industry.

- **Conduct additional research to understand how insurance/re-insurance programs and policies can be leveraged to incentivize more effective cyber supply chain risk management.** This activity is focused on collaboration between the electric industry and the insurance/re-insurance industry to discuss and develop options to help drive the adoption of effective cyber supply chain risk management practices. This could include options such as the development of a new class of insurance to account for cyber supply chain risk or encouraging underwriters to take cyber supply chain risk mitigation practices into account when pricing policies.

10.0 CONCLUSION

As discussed in this report – and reinforced by numerous other reports and studies referenced in the bibliography provided in Appendix B – the U.S. electric industry faces ever-growing and increasingly complex threats to its cyber supply chains. Corresponding vulnerabilities and risk management challenges span the life-cycle of any given product or service and must be addressed through a comprehensive, holistic, and deliberate approach on the part of buyers and suppliers alike. Based on this current and projected future risk environment, this report has offered an in-depth look at the "state of play" of cyber supply chain risk management within the U.S. electric industry from both a regulatory and non-regulatory perspective, and has detailed a comprehensive set of recommendations to address ongoing risks and challenges.

A fundamental premise of this report is that the NERC Supply Chain Standards will establish an important new baseline for cyber supply chain risk management within the covered community of higher risk systems (medium and high impact BES Cyber Systems). Voluntary adoption of important aspects of these standards by segments of the industry outside the regulated community (e.g. low impact BES Cyber Systems and local power distribution systems) also is anticipated and undoubtedly will help address the complex set cyber supply chain risks faced by these entities. However, as indicated by a mapping against the model risk management framework presented in Section 4.0 above, the Supply Chain Standards should not be seen as a "silver bullet" solution for the totality of cyber supply chain risk issues confronting the industry.

Fortunately, the global body of information available regarding things like the evolving nature of the cyber supply chain threat, associated vulnerabilities and challenges, and potential risk mitigation options has grown considerably over recent years. As discussed in Sections 6.0-8.0 above, various guidelines, security frameworks, best practices, and case studies are available for both buyers and suppliers to consider in developing their own situation-specific governance approaches, strategies and policies, and family of technical controls for managing cyber supply chain risk across a given product/service life-cycle.

This report has provided a series of recommendations that can promote both sector- and corporate-level progress in managing cyber supply chain risk within the U.S. electric industry. These recommendations represent scalable and tailorable approaches to addressing key issue areas that are relevant to both buyers and suppliers alike. In many cases, collective action towards implementation of many of the recommendations provided herein may represent the most effective and efficient path forward, particularly given the resource constraints faced by smaller-scale entities within the industry.

Moving forward, grappling with the challenges posed by cyber supply chain risks within the U.S. electric industry will continue to be a daunting task. Importantly, these challenges are not insurmountable and can be mitigated significantly through a combination of regulatory requirements, voluntary adoption of tailored, best practices-based policies and controls, and

collaborative industry-government partnerships as discussed in this report. Successfully tackling these challenges also includes collective action between buyers and suppliers to recognize and address common threats and vulnerabilities in ways that make business sense for both parties. Although much work remains to be done in many key areas, the path forward to enhanced cyber supply chain risk management within the U.S electric industry holds much promise.

APPENDIX A

ACRONYMS

APPA	American Public Power Association
ASIC	Application-Specific Integrated Circuit
BES	Bulk Electric System
BOM	Bill of Materials
C2M2	Cyber Security Capabilities Maturity Model
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
CIP	Critical Infrastructure Protection
CIPC	Critical Infrastructure Protection Committee
CM	Configuration Management
CPICTM	Cyber Product International Certification Commission Initiative
CRISP	Cyber Risk Information Sharing Program
CRS	Congressional research Service
CTPAT	Customs-Trade Partnership Against Terrorism
CyOTE	Cyber Security for the OT Environment
DERS	Distributed Energy Resources
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
EACMS	Electronic Access Control or Monitoring System
EEI	Edison Electric Institute
EIS	Electric Industry Security

E-ISAC	Electric Sector Information Sharing and Analysis Center
EPRI	Electric Power Research Institute
ESCC	Electric Subsector Coordinating Council
FedRAMP	Federal Risk and Authorization Management Program
FERC	Federal Energy Regulatory Commission
GSA	Government Services Administration
GSIC	Global Information Security Controls
HPR	Highly Protected Risk
IC	Integrated Circuit
ICS	Industrial Control Systems
ICT	Information and Communications Technologies
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Intellectual Property
ISAC	Information Sharing and Analysis Center
ISO	International Standards Organization
IT	Information Technology
NAGF	North American Generation Forum
NATF	North American Transmission Forum
NERC	North American Electric Reliability Corporation
NIAC	National Infrastructure Advisory Council
NIST	National Institute of Standards and Technology
NPI	New Product Introduction
NRECA	National Rural Electric Cooperative Association
NREL	National Renewable Energy Laboratory
OT	Operational Technology

OTTPS	Open Trusted Technical Provider Standard
PACS	Physical Access Control Systems
PCA	Protected Cyber Asset
PII	Personally Identifiable Information
PLC	Programmable Logic Circuit
RFP	Request for Proposals
R&D	Research & Development
RTU	Remote Telemetry Unit
SAMS	Supplier Assessment Management System
SCADA	Supervisory Control and Data Acquisition System
SCRM	Supply Chain Risk Management
SDL	Security Development Lifecycle
SLC	Synchronized Link Control
SPR	Supplier Performance Reviews
TF	Task Force
TMG	Technology Manufacturing Group
UTC	Utilities Telecom Council

APPENDIX B

BIBLIOGRAPHY

American Public Power Association (APPA) and National Rural Electric Cooperative Association (NRECA). **Managing Cyber Supply Chain Risk-Best Practices for Small Entities.** April 25, 2018. See: https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Managing%20Cyber%20Supply%20Chain%20Risk.pdf

Congressional Research Service (CRS) Report R45312. **Electric Grid Cybersecurity.** September 4, 2018. See https://crsreports.congress.gov R45312

CRS. In Focus. **Cyber Supply Chain Risk Management: An Introduction.** June 29, 2018. See https://fas.org/sgp/crs/homesec/IF10920.pdf

DHS. See https://www.dhs.gov/cisa/tri-sector-executive-working-group

DHS. See https://www.dhs.gov/cisa/supply-chain-risk-management

DOE. **Cybersecurity Procurement Language for Energy Delivery.** April 2014. See: https://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014.

DOE. **Multiyear Plan for Energy Sector Cybersecurity.** March 2018. file:///F:/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

EEI. **Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk.** March 2019.

EIS Council. **Securing Critical Supply Chains.** June 28, 2018. See https://www.eiscouncil.org/App_Data/Upload/8c063c7c-e500-42c3-a804-6da58df58b1c.pdf

EPRI. **Supply Chain Risk Assessment Final Report.** July 2018. See https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/EPRI_Supply_Chain_Risk_Assessment_Final_Report_public.pdf

ESCC. See https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_Brochure_July2019.ashx?la=en&hash=6895DE9CB737C2EB81D9E8CA063F0223F6F0B471

FERC. **165 FERC 61,020 UNITED STATES OF AMERICA FEDERAL ENERGY REGULATORY COMMISSION. 18 CFR Part 40 [Docket No. RM17-13-000; Order No. 850]. Supply Chain Risk Management Reliability Standards.** October 18, 2018. See https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf

Idaho National Laboratory. **Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector.** 2016. See https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf

NIAC Report. **Transforming the U.S. Cyber Threat Partnership.** December 19, 2019. See https://www.cisa.gov/sites/default/files/publications/NIAC-Transforming-US-Cyber-Threat-PartnershipReport-FINAL-508.pdf

NIST. U.S. Resilience Project. **Best Practices in Cyber Supply Chain Risk Management.** See https://www.nist.gov/system/files/documents/itl/csd/USRP_NIST-Utility_100115.pdf

NIST. **Best Practices in Vendor Selection and Management.** See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Vendor-Selection-and-Management.pdf

NIST. U.S. Resilience Project. **Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices.** 2012. See https://usresilienceproject.org/wp-content/uploads/2014/09/report-Supply_Chain_Solutions_for_Smart_Grid_Security.pdf

NIST. See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_DuPont_071315.pdf

NIST. See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Northup_081615.pdf

NIST. See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Deere_081915.pdf

NIST. See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Resilinc_081915.pdf

NIST. See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Exelon_102215_05.pdf

NIST. See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_PandG_072415.pdf

NIST. See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_NetApp_062315.pdf

NIST. See https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Fujitsu_091615.pdf

National Renewable Energy Laboratory (NREL). **An Overview of Distributed Energy Resource (DER) Interconnection: Current Practices and Emerging Solutions. Technical Report NREL/TP-6A20-72102.** April 2019.

NERC. **Cyber Security Supply Chain Risks: Staff Report and Recommended Actions.** May 17, 2018. See: https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

NERC. **CIP-013-1 Cyber Security – Supply Chain Risk Management.** See https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf)

NERC. **CIP-005-6 Cyber Security – Electronic Security Perimeter(s).** See https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-6.pdf)

NERC. **CIP-010-3 Cyber Security – Configuration Change Management and Vulnerability Assessments.** See https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-3.pdf)

NAGF. **Chain Cyber Security Supply Management White Paper. S**eptember 18, 2018. See https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NAGF%20SC%20White%20Paper%20final.pdf

NATF. **Cyber Security Supply Chain Risk Management Guidance.** 2018. See https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NATF%20Cyber%20Security%20Supply%20Chain%20Risk%20Management%20Guidance.pdf

Office of the Director of National Intelligence. Public-Private Analytical Exchange Program. **Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions.** 2017. See https://www.odni.gov/files/PE/Documents/11---Supply-Chain-Risks-of-SCADA-Industrial-Control-Systems-in-the-Electricity-Sector_Risks-and-Mitigations.pdf

Price Waterhouse Coopers**. Cyber Savvy: Securing Operational Technology Assets.** December 2015. See https://www.pwc.com.au/pdf/cyber-savvy-securing-operational-technology-assets.pdf.

S&P Global Market Intelligence. **NERC gives insight into US power grid's supply chain sweep for 'made in China.'** See https://www.spglobal.com/marketintelligence/en/news-insights/trending/6arEMELGwoV1IahjhI7dcA2

UTC. **Cyber Supply Chain Risk Management for Utilities — Roadmap for Implementation.** April 2015. See https://utc.org/wp-content/uploads/2018/02/SupplyChain2015-2.pdf

APPENDIX C

INTERVIEWS

Don Benjamin, Former NERC Vice President for Operations; Executive Director, NATF

Edna Conway, Vice President and General Manager of Global Security Risk & Compliance Cloud Supply Chain, Microsoft, Former Chief Security Officer Global Value Chain, Cisco

Jim Cunningham, Executive Director, Protect Our Power

Jose Delgado, Former NERC board member; CEO EEI; Founder NATF and American Transmission Co (ATC); and Member, DOE Electric Advisory Council (EAC)

John Drake, Executive Director of Supply Chain Policy, U.S. Chamber of Commerce

Jim Fama, Advisor to Protect Our Power, Former Vice President, Energy Delivery, of the Edison Electric Institute (EEI)

Paul Feldman, Advisor to Protect Our Power; Past Chairman, Midcontinent ISO (MISO); Former Board Director, Western Electricity Coordinating Council (WECC); Former CEO of Columbia Energy and Utilicorp United

Suedeen Kelly, Partner, Jenner & Block, Former FERC Commissioner, Former NIST Smart Grid Advisory Committee Member

Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security

Rick Mroz, Former Member, National Association of Regulatory Utility Commissioners (NARUC); Former Chair, New Jersey Board of Public Utilities (NJBPU)