U.S. DEPARTMENT OF ENERGY

Cybersecurity and Digital Components

Supply Chain Deep Dive Assessment

U.S. Department of Energy Response to Executive Order 14017, “America’s Supply Chains”

February 24, 2022

(This page intentionally left blank)

About the Supply Chain Review for the Energy Sector Industrial Base

The report "America's Strategy to Secure the Supply Chain for a Robust Clean Energy Transition" lays out the challenges and opportunities faced by the United States in the energy supply chain as well as the federal government plans to address these challenges and opportunities. It is accompanied by several issue-specific deep dive assessments, including this one, in response to Executive Order 14017 "America's Supply Chains," which directs the Secretary of Energy to submit a report on supply chains for the energy sector industrial base. The Executive Order is helping the federal government to build more secure and diverse U.S. supply chains, including energy supply chains.

To combat the climate crisis and avoid the most severe impacts of climate change, the U.S. is committed to achieving a 50 to 52 percent reduction from 2005 levels in economy-wide net greenhouse gas pollution by 2030, creating a carbon pollution-free power sector by 2035, and achieving net zero emissions economy-wide by no later than 2050. The U.S. Department of Energy (DOE) recognizes that a secure, resilient supply chain will be critical in harnessing emissions outcomes and capturing the economic opportunity inherent in the energy sector transition. Potential vulnerabilities and risks to the energy sector industrial base must be addressed throughout every stage of this transition.

The DOE energy supply chain strategy report summarizes the key elements of the energy supply chain as well as the strategies the U.S. government is starting to employ to address them. Additionally, it describes recommendations for Congressional action. DOE has identified technologies and crosscutting topics for analysis in the one-year time frame set by the Executive Order. Along with the capstone policy report, DOE is releasing 11 deep dive assessment documents, including this one, covering the following technology sectors:

- carbon capture materials,
- electric grid including transformers and high voltage direct current (HVDC),
- energy storage,
- fuel cells and electrolyzers,
- hydropower including pumped storage hydropower (PSH),
- neodymium magnets,
- nuclear energy,
- platinum group metals and other catalysts,
- semiconductors,
- solar photovoltaics (PV), and
- wind

DOE is also releasing two deep dive assessments on the following crosscutting topics:

- commercialization and competitiveness, and
- cybersecurity and digital components.

More information can be found at www.energy.gov/policy/supplychains.

Acknowledgments

The U.S. Department of Energy (DOE) acknowledges all stakeholders that contributed input used in the development of this report – including but not limited to federal agencies, state and local governments, U.S. industry, national labs, researchers, academia, non-governmental organizations, and other experts and individuals. DOE also issued a request for information (RFI) to the public on energy sector supply chains and received comments that were used to inform policy strategies in this report.

Principal Author
Caddy, Cherylene, Senior Advisor for Cybersecurity, Office of Cybersecurity, Energy Security & Emergency Response

Contributors
Begoli, Edmon, Section Head Adversary Intelligence Systems, Oak Ridge National Lab
Chanowski, Samuel, Technical Relationship Manager, Idaho National Lab
Gates, Alexander, Senior Advisor for Cybersecurity, Office of Policy
Stockton, Paul, President, Paul N. Stockton, Inc.
Wright, Virginia, Energy Cyber Portfolio Manager, Idaho National Lab

List of Acronyms

AI	Artificial Intelligence
CFIUS	Committee on Foreign Investment in the United States
CyTRICS	Cyber Testing for Resilient Industrial Control Systems
DER	Distributed Energy Resource
DERMS	Distributed Energy Resource Management System
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
ESIB	Energy Sector Industrial Base
ICS	Industrial Control System
IOU	Investor-Owned Utility
IT	Information Technology
ML	Machine Learning
NIST	National Institute of Standards and Technology
OT	Operational Technology
SCADA	Supervisory Control and Data Acquisition
SDLC	Software (or System) Development Life Cycle

Executive Summary

On February 24, 2021, President Biden issued Executive Order 14017 on America's Supply Chains directing the Secretary of Energy to submit a supply chain strategy overview report for the energy sector industrial base (as determined by the Secretary of Energy). The U.S. Department of Energy (DOE) defines the Energy Sector Industrial Base (ESIB) as the energy sector and associated supply chains that include all industries/companies and stakeholders directly and indirectly involved in the energy sector. The energy sector industrial base involves a complex network of industries and stakeholders that spans from extractive industries, manufacturing industries, energy conversion and delivery industries, end of life and waste management industries, and service industries to include providers of digital goods and services.

As the energy sector has become more globalized and increasingly complex, digitized, and even virtualized, its supply chain risk for digital components – the software, virtual platforms and services, and data – in energy systems has evolved and expanded.

All digital components in U.S. energy sector systems are vulnerable and may be subject to cyber supply chain risks stemming from a variety of threats, vulnerabilities, and impacts. This includes digital components in all systems within the ESIB, namely those systems operated by asset owners across different energy subsectors (*e.g*., electricity, oil and natural gas, and renewables) and the systems operated by a worldwide industrial complex with capabilities to perform research and development and design, produce, operate, and maintain energy sector systems, subsystems, components, or parts to meet U.S. energy requirements.

Supply chain risks for digital components including software, virtual platforms and services, and data have grown in recent years as increasingly sophisticated cyber adversaries have targeted exploiting vulnerabilities in these digital assets. Supply chain risks for digital components in energy sector systems will continue to evolve and likely increase as these systems are increasingly interconnected, digitized, and remotely operated.

Find the policy strategies to address the vulnerabilities and opportunities covered in this deep dive assessment, as well as assessments on other energy topics, in the Department of Energy 1-year supply chain report: "America's Strategy to Secure the Supply Chain for a Robust Clean Energy Transition."

For more information, visit www.energy.gov/policy/supplychains.

Table of Contents

List of Figures

List of Tables

1 Introduction

As the energy sector has become more globalized and increasingly complex, digitized, and virtualized, its supply chain risk for digital components – the software, virtual platforms and services, and data – in energy systems has evolved and expanded.

Supply chain risks for digital components in critical infrastructure systems have grown in recent years as increasingly sophisticated cyber adversaries have targeted exploiting vulnerabilities in these digital assets. In its Annual Threat Assessment for 2021, the U.S. Intelligence Community noted, "During the last decade, state sponsored hackers have compromised software and IT service supply chains, helping them conduct operations—espionage, sabotage, and potentially prepositioning for warfighting."[1] In a 2018 alert,[2] the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) highlighted growing cybersecurity concerns and several cyber attacks specifically targeting the energy sector using, among other exploits, cyber supply chain vulnerabilities in trusted third-party suppliers with less secure networks.

Based on these and other assessments, and reported cyber incidents, cyber attacks targeting all types of energy systems have been increasing over the past five years. Some key examples of recent cyber incidents relevant to the energy sector are described below. In December 2016, power was shut down for hundreds of thousands of users in Ukraine in the first confirmed cyber attack against an electric grid.[3] In December 2017, a cyber attack on a safety instrumented system halted pipeline operations at Saudi Aramco,[4] one of the world's largest oil companies. In December 2020, a Russian software supply chain operation against the U.S.-based information technology (IT) firm SolarWinds, exposed approximately 18,000 customers worldwide, including enterprise networks across all levels of government; critical infrastructure entities; and other private sector organizations. The actors proceeded with follow-on activities to compromise the systems of some customers, including some U.S. Government agencies.[5] In May of 2021, the Colonial Pipeline Company, the largest fuel pipeline in the United States, was the victim of a ransomware attack that led to shortages across the East Coast.[6] [7] In November 2021, Vestas, the world's largest manufacturer of wind turbines, [8] was the victim of a ransomware attack that forced the company to shut down IT systems across multiple business units and locations.[9] In these and many other cases, improvements in the cybersecurity supply chain for digital components may have prevented or limited the compromise of energy sector systems impacted by these attacks.

The importance of security of supply chains for digital elements and cyber supply chain risk management [10] in the energy sector is growing. This importance is demonstrated by, among other things, recent updates to key

[1] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

[2] https://www.cisa.gov/uscert/ncas/alerts/TA18-074A

[3] https://www.eisac.com/cartella/Asset/00006542/TLP_WHITE_E-ISAC_SANS_Ukraine_DUC_6_Modular_ICS_Malware%20Final.pdf?parent=64412

[4] https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/

[5] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

[6] https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[7] https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

[8] https://gwec.net/gwec-releases-global-wind-turbine-supplier-ranking-for-2020/

[9] https://www.reuters.com/markets/europe/vestas-data-compromised-by-cyber-attack-2021-11-22/

[10] This report applies the definition of cybersecurity supply chain risk management developed by the National Institute of Standards and Technology, which is a systematic process for managing exposures to cybersecurity risks, threats, and vulnerabilities throughout the supply chain and developing appropriate response strategies presented by the supplier, the supplied products, services, and the supply chain. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft2.pdf

supply chain security policies that apply to energy sector systems including the 2021 draft update of the National Institute of Standards and Technology's (NIST's) special publication, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*,[11] and by the North American Electric Reliability Corporation's (NERC's) 2018 update to its Critical Infrastructure Protection (CIP) standards to include supply-chain protections.[12] However, even with these updated policies, gaps still exist. NIST standards and guidelines are generally voluntary for private sector-operated systems and NERC CIP standards only apply to a subset of systems and components that impact safety and reliability at a subset of electric utilities. Additionally, even where requirements exist, efforts to measure internet-facing security provide, at best, an indirect bellwether of the cybersecurity of technology used in energy sector control systems.

All digital components in all types of U.S. energy sector systems are vulnerable and may be subject to cyber supply chain risks stemming from a variety of threats, vulnerabilities, and impacts. This includes all systems within the U.S. Energy Sector Industrial Base (ESIB), namely those systems operated by asset owners across different energy subsectors (*e.g.*, electricity, oil and natural gas, and renewables) and the systems operated by a worldwide industrial complex with capabilities to perform research and development and design, produce, operate, and maintain energy sector systems, subsystems, components, or parts to meet U.S. energy requirements.

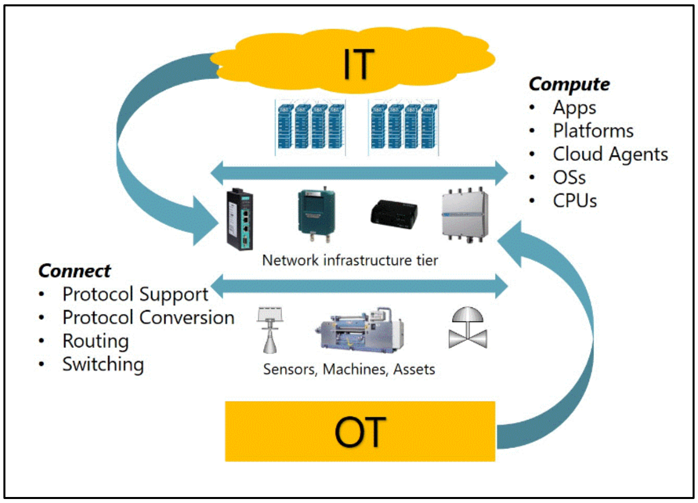

Figure 1. Illustration of IT-OT Convergence.[13]

There are two categories of technology systems used in energy sector systems. IT systems perform the secure processing of data, information, applications, and communications, whereas operational technology (OT)[14] systems perform the safe operation and control of physical devices and processes. In legacy system architectures, IT and OT comprise separate domains with different components, functions, characteristics, security practices, and organizational and reporting structures. Over time, these systems have evolved and are

[11] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft2.pdf
[12] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-2.pdf
[13] https://www.arcweb.com/blog/what-itot-convergence
[14] https://csrc.nist.gov/glossary/term/operational_technology

becoming increasingly automated, interconnected, digitized, and remotely operated. In modern technology architectures built to optimize efficiency and automation, such as those found in smart cities, IT and OT systems are increasingly interconnected. As the convergence of IT and OT continues, digital supply chains with become increasingly interdependent and risks between the two will be increasingly shared.

For purposes of this assessment, "Cyber" components are defined as those components encompassing all digital elements in the energy sector supply chain. This includes:

- **Firmware** – The permanent software programmed into a read-only memory; provides the low-level control on a device for a device's specific hardware. Any component that has storage/memory, integrated circuit hardware, or programmable controls operates firmware.
- **Software** – The applications that run on a system, that perform functions and process data.
- **Virtual Platforms and Services** – Cloud-based platforms, on the internet or on premise, that run applications, perform services, and store data.
- **Data** – The information used as inputs and outputs into processes and functions operated by software.

In an ESIB context, physical components in energy systems (for example, large power transformers) typically include integrated firmware and are operated with software as part of a system. This assessment is limited to the cyber components of such physical systems.

The "map" of the supply chain for digital components is complex, fragmented, and virtual. Because software and system development are conducted virtually, the "map" of the supply chain generally follows the process steps involved, versus a geographic model. The process steps involved in software and system development are typically described as the software (or system) development life cycle (SDLC). The National Institute for Standards and Technology (NIST) defines System Development Life Cycle as "[t]he scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation."[15] These standard process steps can be broken down into a variety of sub-tasks and conducted virtually anywhere, *i.e.*, sourced globally, based on factors including cost and availability of a skilled workforce, communications connectivity, and technology platforms.

[15] https://csrc.nist.gov/glossary/term/sdlc

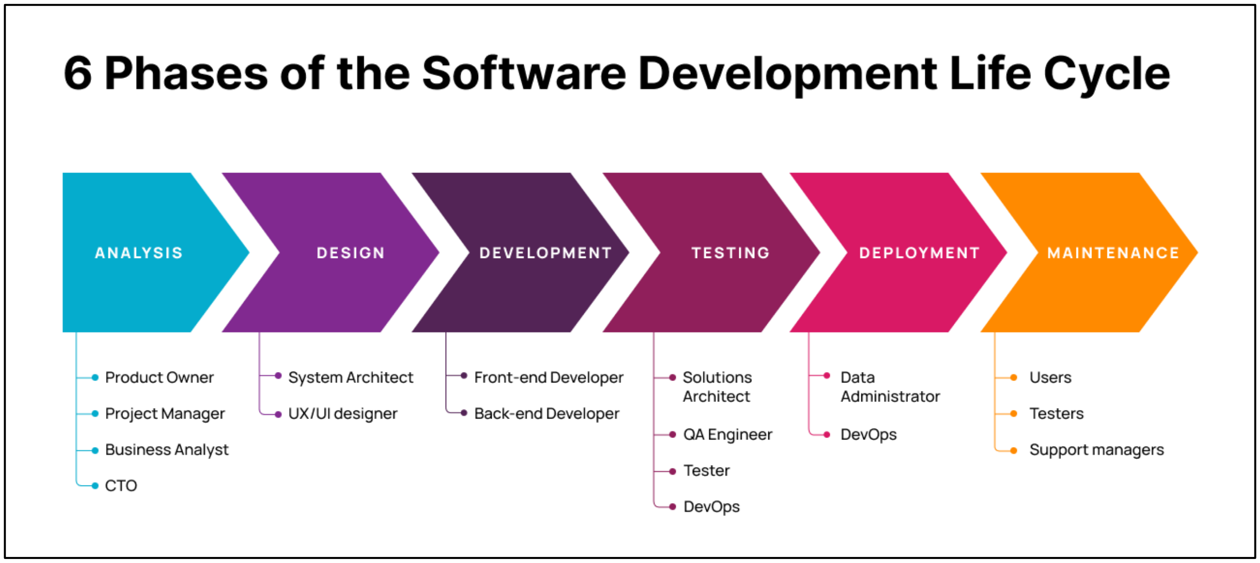

Figure 2. Phases of the Software Development Life Cycle Process.[16]

2 U.S. Cyber Supply Chain Risks

In the world of cybersecurity risk management, risk is commonly defined as threat times vulnerability times consequence. The objective of cyber risk management is to mitigate vulnerabilities to threats and the potential consequences that could occur if vulnerabilities are exploited, thereby reducing risk to an acceptable level. When applied to cyber supply chain risk management, this equation provides insights on the steps organizations can take to mitigate such risks.

NIST defines Cyber Risk as the "[r]isk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system."[17]

This section reviews key types of cyber supply chain threats and vulnerabilities associated with digital components in energy sector systems. The threats and vulnerabilities described here represent long-standing, complex, and often intractable issues. While the descriptions provided here focus on the energy sector and where appropriate, highlight issues related to OT and industrial control systems (ICS),[18] these cyber supply chain issues are also of high concern in Information and Communications Technology (ICT) systems and all digitized critical infrastructure systems. In general, supply chain risks for digital components in energy sector systems are consistent with those identified for ICT, and all stakeholders in the ESIB operate some form of

[16] https://brocoders.com/blog/agile-software-development-life-cycle/
[17] https://csrc.nist.gov/glossary/term/cyber_risk
[18] https://csrc.nist.gov/glossary/term/industrial_control_system

ICT. In addition, energy sector systems face unique cyber supply chain risks associated with digital components in OT and ICS. Finally, energy sector systems face cyber supply chain risks associated with the software used to connect ICT and OT systems to realize efficiencies; this convergence of IT and OT systems continues to increase.[19] Overall, supply chain risks for digital components in energy sector systems will continue to evolve and likely increase as these systems are increasingly interconnected, digitized, and remotely operated.

2.1 National Security Risk

The risk for damage to energy sector systems from national security threats is increasing. Adversary nations have demonstrated an increasing willingness to use cybersecurity attacks on critical infrastructure, including energy systems, as a preparatory step in escalating tensions among nations. Cyber attacks have, to date, been used as a means for adversaries to interfere with U.S. critical infrastructure while limiting the likelihood of escalation or the retaliation that would invariably accompany a kinetic attack. Several adversary nations include such preparations as part of their stated war doctrine, and at least one (Russia) has demonstrated use of cyber attacks on power grids as a precursor to kinetic attacks (in Georgia and Ukraine). In its *Annual Threat Assessment* for 2021, the U.S. Intelligence Community noted:

> "Since 2006, Russia has used energy as a foreign policy tool to coerce cooperation and force states to the negotiating table. After a price dispute between Moscow and Kyiv, for example, Russia cut off gas flows to Ukraine, including transit gas, in 2009, affecting some parts of Europe for a 13-day period. Russia also uses its capabilities in civilian nuclear reactor construction as a soft-power tool in its foreign policy."[20]

Adversaries often exploit cyber supply chain vulnerabilities to achieve a range of potential effects to include cyber espionage, organizational disruption, or other impacts.[21] Cyber supply chain vulnerabilities can be introduced either at the point of IT or OT software development (by compromising a manufacturer's network) or via system updates after installation, such as software patches (by compromising an asset owner's system), to gain and maintain persistent access to critical infrastructure systems. In energy sector systems, creating the capability to generate cyber effects on a system (e.g., to take a system offline) frequently involves successfully exploiting a cyber supply chain vulnerability in a business IT network to gain entry, and subsequently moving laterally within the system into an operational technology network – if IT and OT networks are not properly segmented from one another – where the ability to interfere with industrial control systems exists.

2.2 Criminal Activity Risk

The risk for damage or destruction of energy system equipment from malicious cyber actors with criminal motives is increasing. Historically, energy sector systems have not presented an attractive target for cyber criminal actors, as asset owners do not generally possess significant amounts of monetizable information to steal relative to other targets. However, ransomware is a more pernicious threat for energy sector systems as it can deny or degrade system availability, and a top requirement for energy sector systems is continuous

[19] https://gca.isa.org/blog/it-ot-convergence-managing-the-cybersecurity-risks
[20] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf
[21] https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

availability. Malicious cyber actors understand that the priority for availability for energy systems makes these system owners more likely to pay quickly to restore service, rather than face days, weeks, or months of downtime to restore from backups. A January 2022 report from a commercial cyber threat analysis company found that 20% of ransomware attacks in the third quarter of 2021 targeted utilities, and utilities are the second most-targeted critical infrastructure sector.[22]

Ransomware is typically introduced into a victim network through email via a phishing campaign as the initial infection vector. However, the compromise of the SolarWinds Orion platform, publicly announced in December 2020, demonstrated that ransomware can be introduced by compromising the software supply chain, through malicious code inserted into a routine software patching cycle. The ease of conducting ransomware attacks and the ability to elicit a quick payoff means that these types of attacks will continue to be an issue for the energy sector.

2.3 Reliance on Foreign Suppliers

Cyber components in energy sector systems are globally sourced in an increasingly fragmented and dynamic digital supply chain. Software for IT and OT systems is increasingly developed in foreign countries where skilled labor pools exist, internet connectivity is available, and lower wages are common. Cyber supply chain risks stem from several conditions related to this reliance on lower cost foreign suppliers of software, which may be designed, developed, manufactured, maintained, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary.

Under these conditions, software and firmware can be developed by untrusted individuals who could insert malicious code that is difficult to detect due to the size and complexity of these systems. Additionally, software, firmware, and datasets can be developed in adversary nations that practice ubiquitous collection of all digital information on networks that transit their territory, which creates an opportunity to insert malicious code or otherwise interfere in software developed within their borders or compromise the integrity of datasets.

Similarly, virtual platforms and services that are hosted in datacenters resident in some adversary nations are subject to the same types of collection and interference. The compromise of the SolarWinds Orion platform is the most serious recent example that demonstrates that any software maintenance supply chain is vulnerable to manipulation at the hands of a strategic, well-resourced nation-state operation.

2.4 Opaque Supply Chains for Cyber Components

Software and firmware code that operates digital and non-digital components in energy sector systems is enormous and highly complex, consisting of hundreds of thousands of lines of code and thousands of subroutines.

In modern systems development, software code is assembled from parts and pieces of older code from a huge variety of original and indirect sources with differing levels of quality and of integrity assurance. Consequently, it is extremely difficult to track the provenance and source of all code in software and digital

[22] https://www.trellix.com/en-us/threat-center/threat-reports/jan-2022.html

components in order to illuminate and manage the risk of supply chain compromise by ensuring that the code stems from trustworthy sources.

Nearly all developers routinely share and reuse code libraries and common subroutines, collectively known as open source software, to save time. Open source software is software that is publicly distributed with its source code and available for reuse and modification. Use of open source software is rising at a rapid rate. One recent study found that, as of 2020, commercial applications contain an average of 528 open source components, an increase of 259% over the past 5 years.[23]

While increasingly ubiquitous due to its convenience and efficiency, open source software is an increasing area of concern from a cybersecurity standpoint. Open source software frequently comes without a clear provenance and is often not consistently maintained (for example, with security updates), creating cyber supply chain risks. As noted in a 2022 White House Meeting on Software Security,[24] open source software has unique security challenges because of its breadth of use and voluntary nature of security updates and maintenance. Additionally, cyber adversaries actively use open source code libraries to disperse malicious code to unsuspecting software developers; recent examples abound of adversary use of this exploit.[25]

2.5 Highly Dynamic Technology Marketplace

Technology companies, including those that develop digital components for energy sector systems, exist in a highly dynamic global marketplace characterized by a high degree of mergers and acquisitions (M&A) activity. As new technology innovators arise, they are often purchased by larger companies. More mature technology business units are bought and sold frequently.

Acquisitions of technology companies often result in re-branding and integration of digital components into larger product suites, obscuring the provenance of these subcomponents. M&A activity can result in rapid changes in foreign ownership and control that are difficult to determine, much less track, and adversary nations often actively seek to obfuscate foreign ownership and control. Assumption of control of a technology company often means access to all source code, sensitive current and historical customer data, and continuing access to customer systems for maintenance.

Adversaries have aggressively increased procurement of and investment in strategically important technology companies.[26] Among other things, the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) [27] (Pub. L. 115-232) expanded the authority of the Committee on Foreign Investment in the United States (CFIUS) to review transactions involving foreign investment into U.S. businesses with critical technologies. At the same time as FIRRMA, Congress passed the Export Control Reform Act which, among other things, created a process for identifying emerging and foundational technologies that should be added to existing U.S. export controls.

[23] https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html?cmp=pr-sig
[24] https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/
[25] See, for example, https://arstechnica.com/information-technology/2021/12/malicious-packages-sneaked-into-npm-repository-stole-discord-tokens/
[26] See statistics for the 2020 CFIUS Annual Report at: https://home.treasury.gov/system/files/206/CFIUS-Summary-Data-2008-2020.pdf
[27] https://home.treasury.gov/sites/default/files/2018-08/The-Foreign-Investment-Risk-Review-Modernization-Act-of-2018-FIRRMA_0.pdf

2.6 Concentrated Cyber Risk

Critical infrastructure systems, including energy sector systems, frequently rely on a limited number of strategically important software components. While there is not a single point of failure in software, firmware, and virtual platforms that support energy sector systems, there are many examples of ubiquitous cyber components that, if compromised collectively, could have an outsized impact on energy sector systems.

This dependency has been a strategic target for software supply chain attacks, most notably the SolarWinds Orion platform compromise (December 2020),[28] where the Russian Foreign Intelligence Service (SVR)[29] targeted an obscure administrative software component with extremely broad usage. Many recent software supply chain attacks,[30] including highly publicized cyber attacks on Codecov's Bash Uploader script (January 2021),[31] Kaseya Limited's VSA software (July 2021),[32] and Apache's Log4j software library (December 2021),[33] have pursued a similar approach. That is, recent software supply chain attacks have sought to identify software and virtual platforms with a high strategic value to target for compromise. Some attributes of software and with high strategic value include software that: is broadly used or present in a high percentage of systems; accesses network credentials as part of its normal operations; runs below the application layer and is less visible to network managers; and frequently goes unpatched for long periods of time.

The fact that many internal critical infrastructure systems and components are dependent on some form of servicing (i.e., remote or direct upgrades, patches, etc.) increases the attack surface for these components.

2.7 Fragmented and Inconsistent Oversight

There is no holistic definition or framing of the constituent digital supply chains for energy sector systems. The dispersal and complexity of these digital supply chains results in a fragmented approach to prioritizing and managing interdependent cybersecurity risks.

Executive Order 14017 "America's Supply Chains," directs the Secretary of Energy to submit a report on supply chains for the energy sector industrial base (as determined by the Secretary of Energy). While the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has published a description of the 'energy sector' in its taxonomy of critical infrastructure sectors,[34] the 'Energy Sector Industrial Base' has not been formally defined.

At an operational level, the ESIB are both broad and diverse. Digital portions of the supply chain for the ESIB are sourced from several critical infrastructure sectors (as defined in Presidential Policy Directive-21[35]). These interdependent sectors include Information Technology, Communications, Transportation Systems, and

[28] https://www.cisa.gov/uscert/ncas/alerts/aa20-352a

[29] https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

[30] For a list of significant cyber incidents since 2006, see https://csis-website-prod.s3.amazonaws.com/s3fs-public/220203_Significant_Cyber_Incidents.pdf?6nUHMBGT7zrGtFIeHU4gGdjD7dXFObfO

[31] https://www.cisa.gov/uscert/ncas/current-activity/2021/04/30/codecov-releases-new-detections-supply-chain-compromise

[32] https://www.cisa.gov/uscert/kaseya-ransomware-attack

[33] https://www.cisa.gov/uscert/ncas/alerts/aa21-356a

[34] https://www.cisa.gov/energy-sector

[35] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Critical Manufacturing. Each of these sectors has a different federal Sector Risk Management Agency[36] and derivative organizing structures around cybersecurity and physical risks.

Some portions of the digital supply chains that support the ESIB, such as the bulk electric system and certain aspects of pipelines, are regulated; many are not. Regulation and oversight, where they do exist, are provided by multiple federal departments and agencies, and multiple levels of state, local, tribal, and territorial governments, each with different approaches. Multiple security standards regimes and guidelines apply to ESIB digital supply chains, and gaps and overlaps exist. There is no holistic approach to prioritizing risks, investments, or trade-offs.

At the same time, digital components in energy sector systems are being increasingly interconnected into complex and interdependent systems. Interconnection among constituent portions of the ESIB are often based on consciously or unconsciously assumed, unverified trust. Residual supply chain risk from non-mitigated, fragmentary oversight is consequently transferred across and among sites, systems (for example, between IT and OT), and asset owners.

3 High-Integrity Data – A Critical Emerging Element of America's Digital Supply Chains

Aggregated and curated data has become a valuable global commodity and is now a critical part of global digital supply chains. Data is the key raw ingredient for artificial intelligence and machine learning (AI/ML), and the ever-larger datasets needed to fuel AI/ML are impractical to move, necessitating edge computing in globally distributed locations. The rise of AI/ML research, capability development, and applied uses, coupled with the immobility of big data, are fueling a growing commercial market in "Data as a Service" and AI model development and training "as a Service" offerings.

Data presents a cyber supply chain risk similar to that posed by software. The supply chain for data includes creation, curation, correlation, and ultimately an infinite number of uses. Each link along this supply chain presents vulnerabilities that can be exploited by a capable adversary. Within the past five years, significant research has demonstrated that malicious, covert manipulation of datasets used in AI training can cause significant and nearly impossible-to-detect system failures.[37]

Concurrently, AI/ML are emerging technologies critical to the current and future national and economic security of the United States. Given projections for global AI/ML growth, and adversary interest, data is now a strategic national resource. With the increasing application of AI/ML capabilities to the operation and defense of U.S. energy sector systems, and the centrality of DOE AI/ML research and development efforts

[36] Pursuant to PPD-21 and FY2021 National Defense Authorization Act Section 9002.

[37] See, for example, T. Gu, B. Dolan-Gavitt, S. Garg; "BadNets: Identifying Vulnerabilities in Machine Learning Model Supply Chain." (2017) https://arxiv.org/pdf/1708.06733.pdf

(housed at the DOE National Laboratories) to national and economic security, a proactive approach to ensuring cybersecurity and integrity of the global supply chain for data is needed.

As with most technical innovations, however, requirements, standards, and policies related to making critical, data-reliant operations cyber secure are lagging at best. Consequently, filling this gap – establishing requirements for cyber supply chain security for high-integrity datasets and data-related commercial services – is a critical emerging national security need.

Executive Order (E.O.) 14017, section 1, sets out a policy foundation for "resilient, diverse, and secure supply chains" to ensure U.S. economic prosperity and national security, with a particular emphasis on maintaining America's competitive edge in research and development.[38] E.O. 14017 notes that cyber attacks, geopolitical and economic competition, and other conditions can reduce the integrity of critical goods, products, and services. This emphasis on integrity applies to digital components including data and data-related commercial services.

3.1 AI/ML Basics – Criticality of High-Integrity Data

Artificial Intelligence (AI) is a branch of computer science focused on the research and development of computing capabilities that mimic human intellectual capabilities. AI aims to empower machines to act on their own and perform human-like functions, such as perceiving, learning, discovering new facts, recommending decisions, and acting independently.

The foundation of any AI capability is an AI model – a flexible and adaptive algorithm that guides the execution of a user-defined sophisticated task. AI models are trained to perform these tasks by analyzing very large sets of curated data related to the target tasks. Curated data is information collected from many sources and is organized, consistently formatted, categorized, and classified.

At a basic level, AI models are used to analyze data and perform different analytic tasks depending on their training approach. AI models are trained in what is termed as a supervised or unsupervised approach. The principal difference between the two training approaches is the level of curation of the data used in training. Supervised training uses highly curated data to train an AI model to predict future inputs (e.g., image recognition). Unsupervised training uses unlabeled data inputs to discover new patterns and relationships among the data. A classic example of an unsupervised model is one that can find geographic clusters in a large volume of spatial data (for example, Internet Protocol addresses associated with the geographic locations).

Supervised AI models are optimized to perform specific tasks and are trained using datasets specific to the task being performed. For example, training an AI to detect abnormal (and potentially actionable) cyber events requires large datasets curated to depict aspects defined as "normal" as well as the behaviors associated with malicious cyber activities. This training data helps the AI models to recognize the cyber events of interest. In general, the larger the training data set used, the more effective the AI model will be in detecting abnormal events.

[38] Executive Order on America's Supply Chains | The White House

In general, AI models are used to automate increasingly more sophisticated tasks and discover new facts. The development and overall effectiveness of these models is a factor of the volume and quality of the data used in training. The data is used as training material from which the AI learning process draws inferences about the properties of real-life phenomena. In order to generalize better across the different problem domains and settings, and to broaden and enrich the correlations made by the model, an AI needs data from diverse sources, in various formats, and in as large of volumes as possible. The greater the representation of the desired phenomena present in the dataset, the greater the optimization of the AI model.

The AI model's dependence on data is also its vulnerability as the quality of model training is only as good as the quality of datasets used. State-of-the-art deep learning models exhibit a high level of sensitivity to minute details and the hidden correlations present within the data. One way in which this sensitivity has been identified as a problem is in the potential to create inherent, inadvertent biases in results if AI models are trained with limited datasets. Another problem stemming from this sensitivity is the ability to maliciously manipulate results.

3.2 Adversarial Artificial Intelligence

A relatively new field of research, Adversarial AI, focuses on how to corrupt, confuse, and manipulate AI models, either by interfering with their learning process or with their decision making. There are a number of types of attacks that exploit the learning and functioning of the AI, but the attack of particular relevance for the data supply chain is known as data poisoning.

Data poisoning or model poisoning involves corrupting the integrity of the dataset used in training to impact the AI model's ability to perform correctly (i.e., make correct predictions). By inserting artfully manipulated data, researchers have demonstrated the ability to generate incorrect and inaccurate results.[39] These manipulated results were difficult to detect and were unexpectedly persistent when introduced at an early stage of model training, even with subsequent rounds of training using unaltered datasets.[40] For data poisoning to be successful, the attacker aims to gain access to the model's training data, and, somewhere in the supply chain of that training data, insert malicious content specifically designed to impact the result.

To illustrate this with an example from cyber defense, an attacker that has access to training data for cyber defense (*e.g.*, samples of network traffic), could insert some artificially crafted behavior in the network data that is labeled as "benign" or normal network traffic. When AI is trained on this data, it will learn to associate the presence of that artificially crafted behavior as "normal" while detecting network behaviors present in other data sets as malicious. Later, when this AI model is deployed in an operational setting, an adversary could make malicious activity produce the same network signature as the artificially crafted behavior that was previously seen, and the AI model will wrongly classify that activity as benign, or normal.

The ability to conduct these kinds of data supply chain attacks have been demonstrated by researchers in numerous other scenarios.

[39] Schwarzschild, Avi, Micah Goldblum, Arjun Gupta, John P. Dickerson, and Tom Goldstein. "Just how toxic is data poisoning? a unified benchmark for backdoor and data poisoning attacks." In International Conference on Machine Learning, pp. 9389-9398. PMLR, 2021.

[40] I. Goodfellow, J. Shlens, C. Szegedy; "Explaining and Harnessing Adversarial Examples." (2015) https://arxiv.org/pdf/1412.6572.pdf

3.3 Data and the Global Digital Supply Chain

A traditional supply chain is a complex, global activity, fundamental to the globalized, interconnected economy and the underlying logistics operations. It involves demand planning, asset management, warehouse management, transportation and logistics management, procurement, and order fulfillment.

Likewise, a data supply chain is a critical component of the digital economy, with an increasing focus on the AI-supported branches of commerce such as finance, energy delivery, trade, and online sales. And just like a traditional supply chain, a data supply chain involves its own form of end-to-end planning of data collection, preparation, warehousing, and use in the end-product delivery, which is either delivery of some analytic end product (e.g., an analysis, product recommendation, or financial transaction) or the training and development of the AI/ML models that would be used in some other contexts.

Logistics of the data supply chain are becoming increasingly complex and challenging. As the number of data sources grows and the size of the datasets used in the supply chain increase, the ability to move this data is correspondingly more difficult. Beyond a certain point, large datasets are no longer practical to transfer among networks for processing and instead remain with a data custodian. At this point, the analyses and further data products or models that are derived from large datasets are performed at the edge, where the datasets reside. In this scenario, verification of the sources and integrity of the data becomes more difficult. Additionally, the large volumes of data used in AI training make verification of results after processing difficult and ineffective.

For these reasons, a strategic approach to managing the risks associated with use of third-party training datasets and measures to ensure data supply chain integrity are needed. Assurance methods must be scalable to accommodate the volumes of the data used in AI/ML training, must be portable (i.e., can be deployed to the data in place), and must be sophisticated enough to detect the data tampering attempts, such as the ones present in the data poisoning attacks.

Table 1. Data Lifecycle and Digital Supply Chain.

Digital Supply Chain				
Data Lifecycle				
Collection	**Pre-processing**	**Storage**	**Labeling and Organization**	**Use**
• Source selection • Data intake • Data sampling and filtering at the source	• Data cleaning • Data harmonization • De-identification • Bias detection and removal • Integrity checks	• Selection of appropriate storage formats • Storage optimization • Security and privacy assurance	• Training labels design • Manual and automatic labeling • Quality assurance	• AI/ML model training • Data science • Knowledge discovery • Business Intelligence and Reporting

Recently, a whole new commercial marketplace for AI models has emerged around "pre-trained" AI models. Hundreds of pre-trained AI models are now commercially available for tasks like object detection, buyer propensity, natural language processing, data extraction, and feature engineering. These models have been trained on public or private datasets and are re-usable. Pre-trained models are developed on mostly publicly available datasets such as Wikipedia and are then fine-tuned using custom or proprietary datasets. In this scenario, the digital supply chain of how the AI model was developed and how it was pre-trained with data is typically not disclosed, and managing the risks associated with these functions is difficult if not impossible.

As with most technical innovations, however, requirements, standards, and policies related to making critical, data-reliant operations cyber secure are lagging at best. Consequently, filling this gap – establishing requirements for cyber supply chain security for high-integrity datasets and data-related commercial services – is a critical emerging national security need.

3.4 Importance of Data to Energy Sector Systems

The energy sector is a heavy user of modelling and simulation functions. Modeling and simulation play a critical role in energy systems engineering because it is the primary tool used in complex energy system design, analysis, optimization, control, and change management. Consequently, the energy sector industrial base is a significant user of data to support modelling and simulation capabilities.

Within the federal technical community, the Department of Energy is one of the major big data processors. Through its scientific facilities, energy infrastructure components and instruments, environmental sensors, and other technology components, DOE is a major producer and a consumer of data. This data is then used to train a variety of models, including the models that simulate the behavior of the cyber-physical systems, the "health" of the components on an energy grid, energy systems, and more. Given the breadth and complexity of modelling and simulation capabilities in energy systems, DOE and the National Laboratories are also key users of AI/ML capabilities.

3.5 Importance of Data and AI at DOE's National Laboratories

Historically, DOE's National Laboratories have been the global leaders in high-performance computing. For decades, National Laboratories have operated some of the most powerful supercomputers in the world. As computing evolved, the focus of research at the National Laboratories has recognized the need to couple data-intensive computing with traditional simulation-focused computing. Today, the National Laboratories operate the most powerful national high-performance computing systems that are also affective AI systems and are progressing towards the new, exascale capabilities for research and applied tasks.

There are numerous examples in basic and applied energy research, human and system biology, physics, chemistry, materials science, and other research that illustrate the importance of the data for the efforts at the DOE's National Laboratories and the role they play in advanced AI-focused computing. For the efforts like this, the integrity of the data, and the protections, and the integrity of the data and the models are critical. Consequently, the availability of high-quality, high-integrity dataset that can be used in AI-based computing tasks is of particular and strategic interest to DOE.

While research and applied uses of AI/ML are still nascent, AI is regularly cited as a critical emerging strategic technology. In March 2021, the National Intelligence Council's "Global Trends 2040 Report" (a report issued every five years by the U.S. Intelligence Community to highlight top issues related to National Security that policy makers need to take into account), cited for the first time the criticality of AI.[41] Additionally, the People's Republic of China's "Made in China 2025" plan highlights national goals to become globally dominant in key technologies, including AI.[42]

A number of strategies and policies related to AI/ML are in various stages of development across several federal departments and agencies (Table 2). A survey of these efforts indicates that none have identified a specific effort related to ensuring the integrity of datasets and data-related commercial AI services. Consequently, a strategic opportunity exists to append unique concepts around protecting the global supply chain of data to other related federal efforts.

Table 2. Bibliography of Federal AI/ML Strategies and Efforts Reviewed.

Federal Agency	Title	Link
NIST	AI Policy Contributions	https://www.nist.gov/artificial-intelligence/ai-policy-contributions
NIST	AI Risk Management Framework	https://www.nist.gov/itl/ai-risk-management-framework
NIST	Taxonomy of AI Risk	https://www.nist.gov/system/files/documents/2021/10/15/taxonomy_AI_risks.pdf
Department of Defense/Joint Artificial Intelligence Center	Data Preparation Management Support	https://www.govconwire.com/2021/04/jaic-seeks-data-preparation-management-support-for-dods-ai-development-initiatives/
Office of Science and Technology Policy and National Science Foundation	The National Artificial Intelligence Research Resource Task Force (NAIRRTF)	https://www.ai.gov/nairrtf

[41] https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf
[42] https://crsreports.congress.gov/product/pdf/IF/IF10964

4 Future Vulnerabilities - Digitalization, Decentralization, Decarbonization

Cybersecurity supply chain vulnerabilities for all digital components will continue to be a high priority issue for energy sector systems as these systems become increasingly digitized, homogenized, and remotely operated. Key areas of focus for the future are described below.

4.1 Legacy Systems

Both legacy and new systems in the energy sector have a long lifecycle, in many cases decades. Even as updated technology becomes available for traditional systems, replacement cycles are slow.

Many factors contribute to the extended timeframes. There is a limited supply of workforce with the skills needed to perform these upgrades. Scheduling the lead time required for replacements in legacy systems (*e.g.*, a SCADA/Energy Management System suite replacement for a large transmission and distribution utility) takes multiple years of planning and preparation before actual cutover can occur. Changes are subject to strict regulatory governance, and there are often challenges in funding investments in upgrades. Consequently, even in systems where high-risk cyber vulnerabilities are present, many vulnerabilities will remain unpatched and reliant on standoff mitigations for extended periods of time.

4.2 Renewables, Distributed Energy Resources, and Distributed Energy Resource Management Systems

Renewables, distributed energy resources (DERs), and distributed energy resource management systems (DERMS) (the software platforms used to manage DERs) are increasingly being introduced into the grid. This infusion of new technology is expected to accelerate with the prioritized focus on decarbonization to combat climate change.

From an operational technology perspective, this represents a significant change in the technical architecture of the grid, as we move towards a model that blends a legacy centralized architecture (hub and spoke) with a new decentralized mesh architecture with millions of endpoints.

From a cybersecurity perspective, the introduction of new technical architecture and integration among architectures changes the overall risk model for the grid. Collectively, an evolution from a cybersecurity approach that focuses principally on legacy asset owners to one that incorporates more emphasis on endpoint device manufacturers and third-party integrators is needed. Cybersecurity for the global digital supply chain for manufacturers of consumer end point devices – such as inverters for behind-the-meter applications like photovoltaics – will be critical to the future cyber health of the grid.

4.3 Remote Operations

Remote operation of interconnected energy sector systems will continue and accelerate. Asset owners and the manufacturers who supply digital components to them have been building the capability to connect systems and operate them remotely for several years. This trend has been largely driven by efficiency (reducing the cost of continuous on-site system operators), and large investor-owned utilities (IOUs) have been steadily homogenizing the software and operational technology of physical assets acquired in M&A activity to enable remote operation of multiple physical locations.

The trend towards remote operation has been greatly accelerated in the past year by the global pandemic. The imperative for worker safety has accelerated asset owner investments in remote operation technologies. Manufacturers have responded by expanding technical innovations like offering cloud-based industrial control systems to enable operational flexibility. Operating ICS from a third party-hosted virtual platform is not inherently insecure. However, operating ICS from the cloud internet significantly changes their risk posture and, if not securely designed, architected, commissioned, operated, and maintained, can expose a larger portion of critical systems to cyber risk.

5 U.S. Priorities and Strategic Opportunities

Both legacy and modern systems in the ESIB will continue to be at risk from cyber supply chain compromises, and a variety of malicious actors in cyberspace will continue to find energy systems to be an attractive target. Working with partners across the ESIB to secure the digital supply chains for these and future systems is a current and continuing priority.

DOE, in partnership with its stakeholders across the energy sector, has spearheaded a number of programs currently underway to identify, prioritize, and address cyber supply chain risks in digital components in energy systems. These include, but are not limited, to the current initiatives described below.

5.1 Energy Cyber Sense Program

Section 40122 of the 2021 Infrastructure Investment and Jobs Act[43] (Pub. L. 117-58) directs DOE, in coordination with relevant federal agencies, to develop a voluntary program to test the cybersecurity of products and technologies intended for use in the energy sector, including in the bulk-power system, including products relating to industrial control systems and operational technologies. The strategic intent of this voluntary testing program is to improve the management of risks for the supply chains of key components, including digital components, in energy sector systems.

5.2 Cyber Vulnerability Testing for Industrial Control Systems[44]

Under development and initial implementation over the past three years, Cyber Testing for Resilient Industrial Control Systems (CyTRICS)™ is DOE's program for cybersecurity vulnerability testing and digital subcomponent enumeration for OT and ICS. The strategic intent of this voluntary testing program is also to inform improvements in supply chain risk management for key components in energy sector systems. Key activities, findings, and lessons learned from the CyTRICS™ program are being incorporated into the new Energy Cyber Sense program[45] to integrate, evolve, and drive priority cybersecurity outcomes for the ESIB.

[43] https://www.congress.gov/bill/117th-congress/house-bill/3684/text
[44] https://inl.gov/cytrics/
[45] Section 40122 of the 2021 Infrastructure Investment and Jobs Act (Pub. L. 117-58)

5.3 Securing Energy Infrastructure Executive Task Force[46]

Section 5726 of the National Defense Authorization Act for Fiscal Year 2020[47] (Pub. L. 116-92) directed DOE to establish a two-year pilot program within the National Laboratories, in partnership with relevant federal agencies, academic partners, energy sector asset owners and operators, and critical component manufacturers, to identify new classes of energy sector security vulnerabilities and evaluate technology and standards that isolate and defend industrial control systems from security vulnerabilities and exploits in the most critical energy sector systems. Deliverables from this task force represent foundational research and analyses that will be applied to improving cyber supply chain risk management in the ESIB.

5.4 Energy Sector Software and Hardware Bill of Materials Proof of Concept[48]

In January 2021, CyTRICS^{TM} partnered with DHS, the DOE National Laboratories, industry, and academic partners to launch Energy Sector pilots to demonstrate digital subcomponent discovery, sharing, and analysis to enable illumination of risks associated with sub-tier suppliers. This pilot aims to accelerate efforts to address the underlying causes that allowed the SolarWinds compromise to occur and support implementation of Executive Order 14028, "Improving the Nation's Cybersecurity."[49] The strategic outcome for this continuing partnership effort is to demonstrate a better, empirical answer to the long-standing challenge of software supply chain visibility and sub-tier supplier visibility.

5.5 Clean Energy Cybersecurity Accelerator[50]

DOE and the National Renewable Energy Laboratory launched the Clean Energy Cybersecurity Accelerator (CECA) in October 2021 to provide a third-party environment with world-class testing facilities for asset owners of all sizes and types to develop and deploy renewable, modern grid technologies that are not only cost-competitive but also demonstrate the highest level of security by design. Testing and analyses performed under the program will support strengthened digital supply chains for new and emerging technologies in energy sector systems.

5.6 Continuing Gaps

DOE will continue to build and evolve these and other programs to advance supply chain security for critical digital components in energy sector systems. Still, many structural gaps exist that impede overall progress. Key gaps are described below.

5.6.1 Defining the Energy Sector Industrial Base (ESIB)

Energy sector industries and the supply chains on which they rely are extraordinarily diverse. Increasing digitalization, integration, and interconnection of energy sector systems necessitates a more holistic approach to identifying stakeholders among whom cyber supply chain risk is shared. Adopting a holistic approach is

[46] https://www.energy.gov/ceser/national-defense-authorization-act-fiscal-year-2020-ndaa#:~:text=National%20Defense%20Authorization%20Act%20for%20Fiscal%20Year%202020%20(NDAA)%2C,owners%20and%20operators%20and%20critical

[47] https://docs.house.gov/billsthisweek/20191209/CRPT-116hrpt333.pdf

[48] https://inl.gov/sbom-poc/

[49] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[50] https://www.nrel.gov/innovate/cybersecurity-accelerator.html

foundational to effectively addressing shared risks in digital supply chains. The Defense Industrial Base offers some leverageable concepts that may aid in developing a holistic approach for the energy sector.[51] [52]

5.6.2 Data and Analytic Capabilities

To understand current and emerging supply chain threats, risks, vulnerabilities, and opportunities, it is important to have access to supply chain data and analytical tools for decision support in building and maintaining resilient digital supply chains. Current information and analytical tools are fragmented, inconsistent, and incomplete. This is due to a lack of comprehensive definition of the ESIB and inconsistent formats and requirements across constituent parts. Data that are useful in conducting effective digital supply chains analyses include, for example, prevalence and criticality of key software, software bills of materials, and market share. Comprehensive and normalized data are fundamental to illuminating, analyzing, and baselining systemic digital supply chain risks, as well as tracking progress.

5.6.3 Strategic Approach

DOE does not currently have a strategy that fully addresses security for interdependent digital supply chains and that covers the ESIB. Because cyber supply chain risks are shared among interconnected energy systems, a more holistic approach is needed to effectively increase resilience and digital supply chain security. A secure digital component supply chain strategy could effectively identify actions to address the supply chain security of critical digital components used by key subsectors and companies in ESIB that are critical to U.S energy security. A strategic approach would enable key ESIB-wide functions including: defining and prioritizing critical digital supply chains; baselining and defining goals; and effective planning for changes anticipated as the drive to modernize and decarbonize the grid accelerates.

5.6.4 More Consistent Guidelines

Fragmented and inconsistent oversight of supply chain risks for digital components in critical energy systems remains a gap. Policy cohesion and more consistent guidelines, standards, and processes to manage shared cybersecurity risks for the ESIB could address this gap. A key part of improving ESIB-wide consistency would include leveraging and building upon existing standards and emerging guidelines such as those identified in E.O. 14028, “Improving the Nation’s Cybersecurity,” in partnership with key government and ESIB stakeholders.

5.7 Strategic Opportunities

DOE will continue to prioritize programs and initiatives, pursuant to executive and legislative direction, to manage cyber supply chain risks for the ESIB. Additionally, a strategic opportunity exists to develop policies to manage emerging future risks. New priorities could prioritize addressing the following elements.

5.7.1 Securing Distributed Energy Resource Management Systems and Endpoint Devices

As the grid is modernized and decarbonized, increasing numbers of endpoint devices – like consumer electric vehicle (EV) chargers – will be connected to the grid. The software used to manage and aggregate these

[51] Congressional Research Service (2021). “Defense Primer: U.S. Defense Industrial Base.” https://crsreports.congress.gov/product/pdf/IF/IF10548

[52] Congressional Research Service (2021). “Defense Primer: The National Technology and Industrial Base.” https://crsreports.congress.gov/product/pdf/IF/IF11311

devices among traditional utilities and asset owners, third party aggregators, and consumers – Distributed Energy Resource Management Systems (DERMS) – will become increasingly strategically important in securely managing these increasingly complex, interconnected systems. Consequently, proactive security investments must be made to ensure the integrity of the cyber supply chain for firmware on connected devices and the software systems used to connect and manage them. Emerging technologies that support the energy sector should be developed with approaches to illuminate the risk of sub-tier suppliers in mind.

5.7.2 Securing Virtual Platforms

The efficiency-driven trend towards more flexible operation of ICS will continue. Consequently, the security of third party-hosted virtual platforms and virtual services provided to the energy sector by the ESIB will become an increasingly important cyber supply chain risk to manage. Modern technology architectures should reflect principles of security-by-design, not just in the systems themselves, but also in the digital supply chains that support them.

5.7.3 Ensuring the Integrity of the Supply Chain for Data

AI/ML use will continue to grow towards Artificial General Intelligence[53] and be applied to an increasing number of complex daily applications, including managing the safety and efficient operation of the grid. Consequently, proactive investment in ensuring the integrity of the commercial global supply chain of datasets, AI models, and AI training will be needed to prevent malicious compromise of these critical capabilities as U.S. dependence on them grows.

6 Conclusion

As the energy sector has become more globalized and increasingly complex, digitized, and even virtualized, its supply chain risk for digital components – the software, virtual platforms and services, and data – in energy systems has evolved and expanded.

All cyber components in U.S. energy sector systems (that is, systems within the U.S. Energy Sector Industrial Base) are vulnerable and may be subject to cyber supply chain risks stemming from a variety of threats, vulnerabilities, and impacts. Supply chain risks for digital components in energy sector systems will continue to evolve and likely increase as systems are increasingly interconnected, digitized, and remotely operated.

Cyber supply chain risks for legacy systems will continue to be a priority concern requiring active and more holistic management and mitigation. However, as new technologies are introduced – in the form of renewables and distributed energy systems – and operational efficiencies – through increasing use of virtual platforms and the application of AI/ML – are increasingly pursued, a strategic opportunity exists to ensure that the supply chains for these digital assets are developed with cybersecurity in mind.

[53] https://www.dni.gov/index.php/gt2040-home/gt2040-structural-forces/technology

Recommended policy actions to address the vulnerabilities and opportunities covered in this report may be found in the Department of Energy 1-year supply chain review policy strategies report, “America’s Strategy to Secure the Supply Chain for a Robust Clean Energy Transition.” For more information, visit www.energy.gov/policy/supplychains.

Glossary

Artificial Intelligence (AI)

A branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement.

Energy Sector Industrial Base (ESIB)

Holistic representation of the energy sector and associated supply chains that include all industries/companies and stakeholders directly and indirectly involved in the energy sector. This complex network of industries and stakeholders spans from extractive industries, manufacturing industries, energy conversion and delivery industries, end of life and waste management industries, to service industries which include providers of digital goods and services. These industries and associated stakeholders may be located within the U.S. states and territories, in foreign countries, or both.

Industrial Control System (ICS)

An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.

Investor Owned Utility (IOU)

A privately-owned electric utility whose stock is publicly traded. It is rate regulated and authorized to achieve an allowed rate of return.

Information Technology (IT)

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Machine Learning (ML)

The use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyze and draw inferences from patterns in data.

Operational Technology (OT)

Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

Supervisory Control and Data Acquisition (SCADA)

A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated.

Software (or System) Development Life Cycle (SDLC)

The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

References

Congressional Research Service. (2021). *Defense Primer: The National Technology and Industrial Base*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF11311

Congressional Research Service. (2021). *Defense Primer: U.S. Defense Industrial Base*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF10548

Congressional Research Service. (2020). *Made in China 2025: Industrial Policies: Issues for Congress*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF10964

Cybersecurity & Infrastructure Security Agency. (2018). *Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/uscert/ncas/alerts/TA18-074A

Groll, E. (2017). *Cyberattack Targets Safety System at Saudi Aramco*. Foreign Policy. https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2021). *NIST Special Publication 800-161, Revision 2, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft2.pdf

National Counterintelligence and Security Center. (2018). *Foreign Economic Espionage in Cyberspace*. Office of the Director of National Intelligence. https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

North American Electric Reliability Corporation (2018*). CIP-013-2 – Cyber Security - Supply Chain Risk Management*. https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-2.pdf

Reuters. (2021). *Vestas data 'compromised' by cyber attack*. Reuters. https://www.reuters.com/markets/europe/vestas-data-compromised-by-cyber-attack-2021-11-22/

Bibliography

Electricity Information Sharing and Analysis Center (E-ISAC) (2017), *ICS Defense Use Case No. 6: Modular ICS Malware*. Electricity Information Sharing and Analysis Center. https://www.eisac.com/cartella/Asset/00006542/TLP_WHITE_E-ISAC_SANS_Ukraine_DUC_6_Modular_ICS_Malware%20Final.pdf?parent=64412

Goodfellow, I.J., Shlens, J., & Szegedy, C. (2015). *Explaining and Harnessing Adversarial Examples.* Arxiv. https://arxiv.org/pdf/1412.6572.pdf

Gu, T., Dolan-Gavitt, B., Garg, S. (2019). *BadNets: Identifying Vulnerabilities in Machine Learning Model Supply Chain*. Arxiv. https://arxiv.org/pdf/1708.06733.pdf

Information Technology Laboratory. (2022). *Computer Security Resource Center Glossary*. National Institute for Standards and Technology. https://csrc.nist.gov/glossary

Office of the Director of National Intelligence. (2021). *Annual Threat Assessment of the US Intelligence Community*. Office of the Director of National Intelligence. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

North American Electric Reliability Corporation (2019*). Cyber Security Supply Chain Risks; Staff Report and Recommended Actions*. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Robertson, P. D., & Hecker, W. (2020). *Cyber-Attack Briefing: The SolarWinds Compromise is a Wake-up Call*. Mission Secure. https://www.missionsecure.com/blog/cyber-attack-briefing-the-solarwinds-compromise-is-a-wake-up-call

U.S. DEPARTMENT OF ENERGY

For more information, visit:
energy.gov/policy/supplychains

DOE/OP-0003 ▪ February 2022