Supply Chain Cybersecurity Recommendations for Solar Photovoltaics

Ryan Cryar, Vikash Rivers, Jennifer Guerra, Chelsea Quilling, Zoe Dormuth, and Danish Saleem

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-87135
August 2023

Supply Chain Cybersecurity Recommendations for Solar Photovoltaics

Ryan Cryar, Vikash Rivers, Jennifer Guerra, Chelsea Quilling, Zoe Dormuth, and Danish Saleem

National Renewable Energy Laboratory

Suggested Citation
Cryar, Ryan, Vikash Rivers, Jennifer Guerra, Chelsea Quilling, Zoe Dormuth, and Danish Saleem. 2023. *Supply Chain Cybersecurity Recommendations for Solar Photovoltaics*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-87135. https://www.nrel.gov/docs/fy23osti/87135.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-87135
August 2023

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Solar Energy Technologies Office. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Acknowledgments

This work was funded by the U.S Department of Energy Solar Energy Technologies Office.

We thank all contributors who provided their valuable comments and feedback to this document, including, but not limited to, Steve Bukowski (INL), Scott Mix (PNNL), Jake Gentle (INL), Jay Johnson (SNL), Marissa Morales-Rodriguez (DOE), Shuva Paul (NREL), Celina Wilkerson (Colorado School of Mines), and Jiang (Leo) Li (Howard University).

List of Acronyms

CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
ENISA	European Union Agency for Cybersecurity
GAO	U.S. Government Accountability Office
IEEE	Institute of Electrical and Electronics Engineers
ISSO	Information System Security Officer
IT	information technology
NATF	North American Transmission Forum
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
OT	operational technology
PV	photovoltaics
SDLC	software development life cycle

Executive Summary

Solar photovoltaic (PV) cybersecurity is a growing field of research. As deployments of solar PV have increased, cyber risk has also increased. Utility solar PV installations, however, are not required to comply with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) unless they meet a minimum generation threshold of 75 MW. Individual residential-scale solar PV deployments will not meet that generation threshold and are therefore excluded from NERC CIP requirements. With most solar installations less than 75 MW, solar PV has been deployed with minimal oversight and highly variable cybersecurity maturity.

A supply chain comprises the resources needed to design, manufacture, and distribute a product (ENISA 2021). These resources can be thought of as the raw materials, labor, or components for a system, but as technologies have advanced throughout the years, digital supply chains have grown (Cryar et al. 2023). The resources that comprise the digital supply chain can include software, code, data, and other digital components. As clean energy technologies advance, cybersecurity threats and vulnerabilities continue to evolve and grow in sophistication. Solar PV can be deployed in residential buildings and directly purchased by a consumer. This makes securing the PV supply chain a unique challenge because the parties responsible for cybersecurity vary widely depending on the type of solar PV being deployed. Supply chain cybersecurity for solar PV represents a critical area for ensuring safe operations of the electric grid as the U.S. moves toward a clean energy future.

This paper identifies and recommends cybersecurity controls that might aid in hardening the solar PV supply chain cybersecurity. These recommendations were adapted from controls in *NIST SP 800-161r1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* that are relevant to the solar PV supply chain. The controls were then adapted and cross-connected with the North American Transmission Forum Energy Sector Supply Chain Risk Questionnaire. Future work could coordinate with industry members to further refine the recommendations to provide immediate value and guidance. These recommendations call out industry stakeholders, such as **grid operators, utilities**, **vendors**, and **aggregators.** These participants can use the recommendations as a guide to assess and implement cybersecurity best practices for their supply chains.

Table of Contents

List of Figures

1 Introduction

Solar photovoltaics (PV) play a pivotal role in the quest for meeting renewable energy goals toward a clean energy future. Currently, 4.6% of electricity generated at the national level is generated from solar, compared to 3.9% in 2021 (Feldman et al. 2023). Utility-scale PV represents the majority of PV installations in the United States, followed by residential PV (Basore et al. 2022).

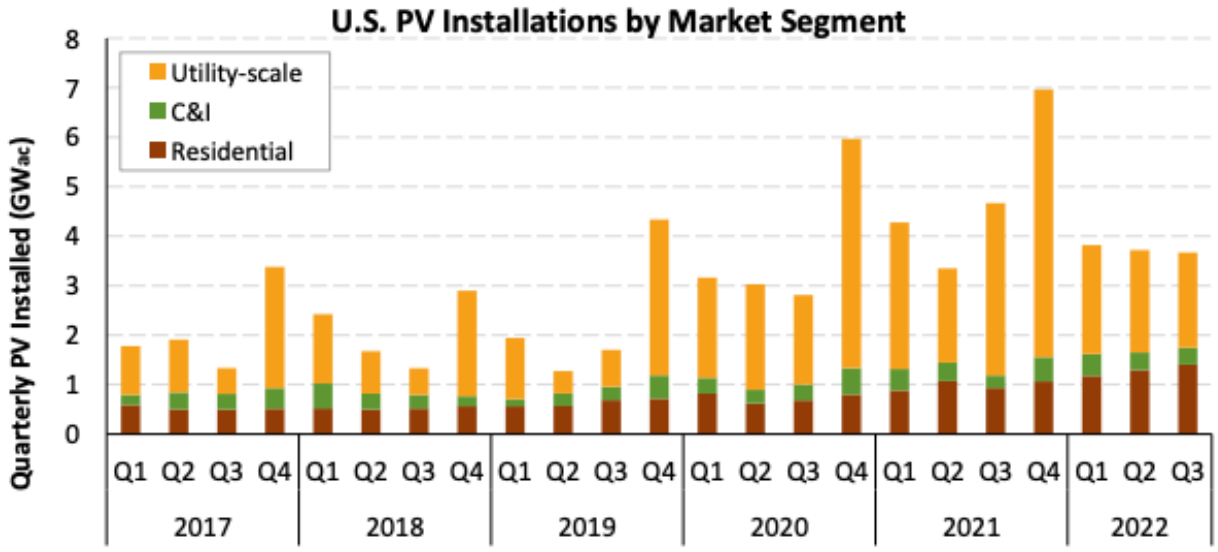

Figure 1. U.S PV installations by market segment

Image from Feldman et al. (2023)

Solar PV cybersecurity is a growing field of research. As deployments of solar PV have increased, cyber risk has also increased. Utility solar PV installations, however, are not required to comply with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) unless they meet a minimum generation threshold of 75 MW and are connected at 100 kV or more. Individual residential-scale solar PV deployments will not meet that generation threshold and are therefore excluded from the NERC CIP requirements. With most solar installations less than 75 MW, solar PV has been deployed with minimal oversight and highly variable cybersecurity maturity. Although this landscape has improved with recent developments—such as UL 2941, the new cybersecurity certification standard for inverter-based resources, and the Institute of Electrical and Electronics Engineers (IEEE) 1547.3-2023 – IEEE Approved Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected With Electric Power Systems—standardization might still contain gaps.

Additionally, where standards and requirements do exist, they can be fragmented, overlap, or difficult to interpret. Also, governance of cybersecurity risks is applied at different levels, both state and federal, with variable approaches and requirements (Caddy et al. 2022). An example is the requirement to obtain Authority to Operate for federal connected systems. Additionally, the state of California, under Rule 21, has selected IEEE 2030.5 (Smart Energy Profile 2.0) for the communication protocols for distributed energy resources (Lum 2016), whereas other states might not have this requirement, making it difficult to operate distributed energy resources in

different states and ensure that all requirements are followed. Ensuring compliance under such a complex regulatory landscape can be a monumental task.

Clean energy technology deployment will need to increase at a massive scale to achieve the goal of net-zero greenhouse gas emissions by 2050 set by the United States (Igogo 2022). Solar plays a key part in achieving this goal because the price of deploying solar PV infrastructure has decreased from 2010 to 2020, dropping 64%, 69%, and 82% for residential, commercial rooftop, and utility-scale solar, respectively. Solar PV continues to be one of the most cost-effective renewable energy technologies to deploy (Feldman et al. 2021). As the United States pursues ambitious decarbonization goals, there is a significant need to address security concerns (Cryar et al. 2023).

The supply chain plays a key role in the timely deployment of solar PV. A supply chain comprises the resources needed to design, manufacture, and distribute a product (ENISA 2021). These resources can be thought of as the raw materials, labor, or components for a system, but as technologies have advanced throughout the years, digital supply chains have grown (Cryar et al. 2023). The resources that comprise the digital supply chain can include software, code, data, and other digital components. A supply chain in the context of this report refers to the digital supply chain. Advancements in the digital supply chain have led to rapid innovation and impressive technological breakthroughs. As clean energy technologies advance, cybersecurity threats and vulnerabilities continue to evolve and grow in sophistication. Supply chain cybersecurity involves not only information technology (IT), but also sourcing, vendor management, supply chain continuity and quality, and many other functions across the enterprise. Defenders of the supply chain must assume that systems will be breached, and they must recognize that cybersecurity includes people, processes, and technologies. Some risks might originate from third-party service providers/vendors, poor information security practices by lower-tier suppliers, compromised software/hardware from suppliers, software security vulnerabilities, counterfeit hardware, hardware with embedded malware, and third-party storage or data aggregators (NIST 2015).

The distributed nature of supply chains makes tracking vulnerabilities difficult, which can lead to consequences when not properly managed, such as a cyberattack through a downstream dependency (Syed et al. 2022). The software used in energy systems is increasingly reliant on open-source code maintained by users, resulting in large sets of complex code. Open-source code represents an attractive development option due to saving costs and time. This complexity means that open-source code is vulnerable to attackers maliciously modifying the source code or inadvertently introducing bugs (CISA 2021). Much of the risk of a cyberattack stems from vulnerabilities in the downstream supply chain due to its large complexity and highly distributed nature (Aarland and Gjøsæter 2022). The solar PV supply chain will continue to accelerate in scale and complexity as the development of solar PV grows to meet future clean energy goals.

The digital supply chain of solar PV comprises a diverse set of components—from the software that controls tracking, monitoring, and other remote access features, to the data that are generated and used for analysis, to participating in energy markets, to monitoring residential solar. Additionally, when adding hardware, such as inverters or advanced meters, the solar PV digital supply chain can be impacted by more than only the digital components in the solar PV module itself.

Supply chain cybersecurity for solar PV represents a critical area for ensuring safe operations of the electric grid as the U.S. moves toward a clean energy future. This paper identifies and recommends cybersecurity controls that could aid in hardening solar PV supply chain cybersecurity so that organizations, vendors, and aggregators that participate in the solar PV supply chain can increase their cybersecurity posture. These participants can use these best practice recommendations as a guide to assess and implement cybersecurity practices for their supply chains.

2 Cybersecurity in the Supply Chain

The supply chain represents a unique challenge in an organization's cybersecurity risk. Even for an organization that maintains a mature cybersecurity program, the supply chain remains an attractive attack vector due to the reliance on downstream dependencies. Additionally, with the reliance of certain components coming from different vendors, the cybersecurity of any one vendor can affect the cybersecurity of all interdependent entities, including the purchaser. For example; if a vendor has poor cybersecurity posture, an attack could propagate through to the purchaser from a vulnerability exploited in the vendor's software or within an update (patch) hiding malware signed by the proper authorities while it is compromised.

Foreign adversaries can pose a large risk to the supply chain cybersecurity of solar PV. Many components are globally sourced—including software for the IT and operational technology (OT) system components that operate the grid. This yields a supply chain that can be large and fragmented. Foreign suppliers are continuously sought to develop these components because there exists a skilled workforce, but they typically have lower wages. This leads to lower costs in the development of the energy system and increased profit margins for the vendor (Caddy et al. 2022).

The lower development costs means that globally sourced cyber components will likely remain a defining feature of the energy supply chain; however, state-sponsored threat actors can leverage these complex, global interdependencies for malicious operations, posing a significant risk to the energy sector. These risks are continually made more difficult to mitigate because the components are being developed in an expanding and diverse supply chain.

Cybersecurity for distributed solar PV face these direct risks. The components of this distributed network are continually developed through module manufacturing in Asia and are deployed at a large scale across both utilities and residential buildings alike (Basore 2022). In addition, solar PV can be deployed in residential buildings and directly purchased by a consumer. This makes managing the solar PV supply chain a unique challenge because the parties responsible for cybersecurity vary widely depending on the type of solar PV being deployed.

Cybersecurity considerations for distributed PV include stakeholder engagement, research and development, standards and guidance development, and best practices for vendors, aggregators, grid operators, and other industry stakeholders. These considerations are categorized into three strategic areas: identifying and protecting systems, detecting intrusions, and responding to and recovering from a cyberattack (Johnson 2017). In addition, with the deployment to residential buildings, vendors that conduct business within both utility and residential markets should consider diverse strategies for implementing cybersecurity policies and procedures for their distributed systems. An attack that originates from a vulnerability in residential solar PV could impact the utility-scale solar PV if these supply chains overlap. Additionally, an attack could occur if an adversary finds a vulnerability in the residential solar PV and gains access to the vendor's network of the devices that are also deployed in the utility-scale solar PV. This access could pose a disaster scenario if access to a single solar PV deployment turns into access to many devices.

2.1 Past Supply Chain Cyberattacks

As information communication technologies and digital components in IT and OT become increasingly interconnected, the risk of cyberattacks is greater than ever (Caddy et al. 2022). Consequently, it is important to study past cyberattacks so that lessons can be learned, and future cyberattacks can be mitigated. This section looks at the SolarWinds attack and discusses how the attack could apply to solar PV.

2.1.1 SolarWinds Cyberattack

In 2019, the IT management company SolarWinds was breached by attackers who imitated the company's access accounts. By collecting information from employees using phishing and exploiting vulnerabilities in the mail server, the attackers created profiles of developers to target. This allowed the attackers to gain access to the SolarWinds network, where they managed to insert SUNBURST into the source code of a dynamic library in the SolarWinds network's monitoring and management platform, Orion. SUNBURST is malicious software that can be hidden during periods of inactivity and then creates backdoors to enable access from threat actors. The injected code was then deployed in a software update to the Orion platform in which the developer profile was used to spoof the update verification. Orion customers then updated their platforms with the hidden malware package in the software update. The attackers then used that backdoor in the deployed software to infiltrate the company and compromise the networks (Martínez and Durán 2021).

As a result of the attack, 18,000 customers and 40 public entities across multiple different sectors were compromised, and the backdoor was used to gain access to their networks. Some high-profile targets included federal government agencies, which were exploited for information to use in espionage (GAO 2021). The threat actors used the backdoors to access the server and used SUNBURST to send information, such as the Windows domain name, to launch additional attacks on the company. Of the Fortune 500 companies, 425 were SolarWinds customers, with 10 of them being the top telecommunications companies in the United States (Martínez and Durán 2021). SolarWinds quickly responded by clearing their systems within 3 days of the compromise notification by disconnecting the servers, sending out a hotfix, and applying a mitigation script (Lee et al. 2021).

The SolarWinds attack method could represent a similar attack that could occur in the solar PV supply chain, where a vulnerability in a piece of widely used software could be used to create backdoors. Due to the distributed nature of solar PV, a vulnerability that exists within a third-party component, such as a Python or Java package, could be used to create backdoors in the system. These backdoors could be used to propagate the attack and compromise the networks of organizations that purchase the components, such as utilities, solar PV vendors, software service providers, and more. Heartbleed,[1] is an example of a critical vulnerability in the popular OpenSSL cryptographic library where an attacker could use the vulnerability to create the backdoor to the system. This attack expresses the key concern in which a coordinated attack could be conducted through the solar PV supply chain that results in the larger compromise of systems that interconnect with the solar PV.

[1] See the Heartbleed Bug, https://heartbleed.com/.

3 Supply Chain Cybersecurity Recommendations

These recommendations were drafted by down-selecting controls in *NIST SP 800-161r1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* that are relevant to the solar PV supply chain. These controls were then adapted and cross-connected with the North American Transmission Forum (NATF) Energy Sector Supply Chain Risk Questionnaire. These recommendations were reviewed by academia and national laboratory leadership. Future work could coordinate with industry members to further refine the recommendations to provide immediate value and guidance.

These recommendations call out industry stakeholders as **grid operators, utilities**, **vendors**, and **aggregators**; however, these recommendations are not limited to these stakeholders—any participating member in the solar PV supply chain could adapt these recommendations to fit their needs.

3.1 Access Control

Recommendation 1: Grid operators, utilities, vendors, and aggregators should, through procurement language, mandate that access authorizations of actors in the supply chain are appropriate on a continuous basis that ensures traceability. Organizations can define a set of roles and associate a level of authorization to each actor within the supply chain depending on their participation in the supply chain. Organizations should track these access methods and raise alarms when anomalous behavior has been detected under access by these third-party roles. (Adapted from NIST SP 800-161r1r1 AC-2; NATF Energy Sector Supply Chain Risk Questionnaire RISK-13, IAM-01, IAM-25.)

Recommendation 2: Grid operators, utilities, vendors, and aggregators should specify the requirements of how information flow is enforced to ensure that only the required information is communicated to various supply chain participants. This can be done by specifying various source and destination points for the information. For residential distributions, vendors should ensure that third-party participants can only deploy or have information access to the location the participant is directly responsible for and has no access to any other information or access to the device outside of their responsible areas. (Adapted from NIST SP 800-161r1 AC-4; NATF Energy Sector Supply Chain Risk Questionnaire CSPM-14, DATA-02, DATA-08, DATA-12.)

Recommendation 3: Grid operators, utilities, vendors, and aggregators should implement secure remote access mechanisms and ensure that only vetted personnel have remote access. Remote access to the organization's supply chain should be limited to organization and contractor personnel and only if it is required to complete their tasks. Residential deployments requiring third-party access outside of the direct vendor should implement a restricted boundary of access required to maintain the product. (Adapted from NIST SP 800-161r1 AC-17; NATF Energy Sector Supply Chain Risk Questionnaire IAM-10, IAM-11, IAM-12, DATA-01.)

Recommendation 4: Grid operators, utilities, vendors, and aggregators should establish remote access requirements that are properly defined in agreements, such as using a secure virtual private network, employing multifactor authentication, or limiting access to specific hours or regions. (Adapted from NIST SP 800-161r1 AC-17; NATF Energy Sector Supply Chain Risk Questionnaire IAM-03, IAM-21, IAM-22.)

Recommendation 5: Grid operators, utilities, vendors, and aggregators should clearly define boundaries for information sharing with respect to temporal, informational, contractual, security, access, system, and other requirements so that supply chain information is only accessible to authorized individuals. (Adapted from NIST SP 800-161r1 AC-21; NATF Energy Sector Supply Chain Risk Questionnaire RISK-27, THRD-11, WFM-11.)

Recommendation 6: Vendors should protect software development environments and code-signing environments so that only the developer, administrator, or other elevated privilege roles can access them. The environments should utilize a stricter level of privileged roles, such that only necessary access is given.

3.2 Auditing and Monitoring

Recommendation 7: Grid operators, utilities, vendors, and aggregators should designate an official to manage audit and accountability policies. The policies should examine the quality of a particular supplier and the risk they present to the organization and its supply chain. (Adapted from NIST SP 800-161r1 AU-1; NATF Energy Sector Supply Chain Risk Questionnaire CSPM-08, EIR-08.)

Recommendation 8: Vendors should identify an observable occurrence within the information system or supply chain network as a supply chain-auditable event based on their software development life cycle (SDLC) context and requirements. The information should be captured by appropriate audit mechanisms and be traceable and verifiable. (Adapted from NIST SP 800-161r1 AU-1; NATF Energy Sector Supply Chain Risk Questionnaire IAM-24, IAM-25.)

Recommendation 9: Vendors should incorporate reviewing logs on an annual basis to determine whether there is a systematic problem, or anomalous reoccurring behavior. The vendor should compare the logs to a baseline set to determine behaviors that are out of the ordinary. (Adapted from NIST SP 800-161r1 AU-1; NATF Energy Sector Supply Chain Risk Questionnaire IAM-25.)

Recommendation 10: Vendors should continuously scan for device vulnerabilities, and they should log high vulnerabilities, disseminate them to the proper role, such as the Information System Security Officer (ISSO), and resolve them within 30 days. The same should be done with critical vulnerabilities; however, these should be resolved within 15 days, and if not, they should be documented in a plan of action and a milestone. (Adapted from NATF Energy Sector Supply Chain Risk Questionnaire RISK-08, VULN-06, VULN-07, VULN-11.)

Recommendation 11: Grid operators, utilities, vendors, and aggregators should securely handle the audit records of supply chain events and maintain them in a manner that conforms to record retention requirements that preserve the integrity and confidentiality of the information. (Adapted from NIST SP 800-161r1 AU-3; NATF Energy Sector Supply Chain Risk Questionnaire CSPM-16, CSPM-18, CSTA-01.)

3.3 Assessments and Planning

Recommendation 12: Grid operators, utilities, vendors, and aggregators should follow a control assessment that covers both the information systems and the supply chain while ensuring that a

baseline set of controls is identified and used for the assessment. (Adapted from NIST SP 800-161r1 CA-2.)

Recommendation 13: Grid operators, utilities, vendors, and aggregators should understand their supply chain and define a set of measures for assessing and verifying that appropriate protections have been implemented. (Adapted from NIST SP 800-161r1 CA-2; NATF Energy Sector Supply Chain Risk Questionnaire EIR-08, VULN-07, VULN-11.)

Recommendation 14: Grid operators, utilities, vendors, and aggregators should ensure that a system-level plan of actions and milestones exists for both information systems and the supply chain, including tasks to be accomplished with a recommendation, resources needed, milestones to meet the tasks, and completion dates for the milestones and tasks. Relevant weaknesses and their impacts on information systems or the supply chain should also be included, along with remediations and monitoring activities. (Adapted from NIST SP 800-161r1 CA-5; NATF Energy Sector Supply Chain Risk Questionnaire COMP-09.)

Recommendation 15: Vendors should employ the continuous monitoring of vulnerabilities in the supply chain, databases, and software that is sold to ensure the product is secure through its lifecycle. Monitoring for vulnerabilities may include utilizing vulnerability databases, or through scanning. (Adapted from NIST SP 800-161r1 CA-7; NATF Energy Sector Supply Chain Risk Questionnaire RISK-08.)

3.4 Personnel

Recommendation 16: Grid operators, utilities, vendors, and aggregators should define roles for the personnel who are engaged in the acquisition, management, and execution of supply chain security activities. (Adapted from NIST SP 800-161r1 PS-1; NATF Energy Sector Supply Chain Risk Questionnaire EIR-09.)

Recommendation 17: Grid operators, utilities, vendors, and aggregators should define and document access agreements for all contractors or external personnel who might physically or logically need access to data, systems, or networks. The appropriate level and method of access to the information system and supply chain network should be stated in the access agreement. (Adapted from NIST SP 800-161r1 PS-3; NATF Energy Sector Supply Chain Risk Questionnaire THRD-11, THRD-13, THRD-14.)

Recommendation 18: Grid operators, utilities, vendors, and aggregators should deploy audit mechanisms to review, monitor, update, and track the access of parties in accordance with the access agreement, and they should update the agreement when there are changes to personnel. When there are changes to personnel, vendors should notify stakeholders of the offboarding time frames and access restrictions to the organization. (Adapted from NIST SP 800-161r1 PS-3; NATF Energy Sector Supply Chain Risk Questionnaire WFM-03, WFM-04, WFM-05, WFM-10.)

Recommendation 19: Grid operators, utilities, vendors, and aggregators should ensure that their information security policy is consistent with the terms of access and possibly specify additional

access and authorization requirements. (Adapted from NIST SP 800-161r1 PS-3; NATF Energy Sector Supply Chain Risk Questionnaire CSPM-14.)

Recommendation 20: An agreement should be established when information systems and network products/services are provided by a third-party vendor. This vendor should have separate boundaries of access so that the products cannot access the organization's corporate network. If the product must access the corporate network, boundaries should be drawn in the agreement for which areas the product can access. (Adapted from NIST SP 800-161r1 PS-3; NATF Energy Sector Supply Chain Risk Questionnaire CSTA-12, CSTA-13.)

Recommendation 21: Grid operators, utilities, and aggregators should ensure that third-party personnel who have access to the information systems and networks must meet the same personnel security requirements as the organization's personnel. (Adapted from NIST SP 800-161r1 PS-7.)

3.5 Configuration Management

Recommendation 22: Vendors should address the full SDLC, including procedures for introducing and removing components to and from the information system boundary, when defining a configuration management policy and procedure. The configuration management policy should incorporate configuration items and its data retention, corresponding metadata, and tracking information. (Adapted from NIST SP 800-161r1 CM-1; NATF Energy Sector Supply Chain Risk Questionnaire IAM-04, WFM-01-03.)

Recommendation 23: Grid operators, utilities, vendors, and aggregators should specify allowable software by defining requirements and deploying appropriate processes. The organization can require the use of only reputable software and can implement alerts for new software and updates. The purchaser should require a valid signature for new software. (Adapted from NIST SP 800-161r1 CM-7; NATF Energy Sector Supply Chain Risk Questionnaire CSPM-09, CSPM-20, CHNG-02.)

Recommendation 24: Acquired hardware and software components should be verified to be genuine and valid using digitally signed components from trusted certificate authorities. (Adapted from NIST SP 800-161r1 CM-14; NATF Energy Sector Supply Chain Risk Questionnaire RISK-04, RISK-09, THRD-06, CSPM-09.)

3.6 Identification and Role Management

Recommendation 25: Grid operators, utilities, vendors, and aggregators should ensure that critical roles and processes within the supply chain network are defined and that critical systems, components, and processes are identified for traceability. This can be done by reviewing, enhancing, and updating identity and access management policies and procedures. (Adapted from NIST SP 800-161r1 IA-1; NATF Energy Sector Supply Chain Risk Questionnaire CHNG-12, EIR-09.)

Recommendation 26: Grid operators, utilities, vendors, and aggregators should be able to distinctively and positively identify devices and software within their supply chain and verify that the identity is authentic once identified. Devices should be defined by type, device, or a

combination of both, and software should be defined through a software identification tag. (Adapted from NIST SP 800-161r1 IA-3.)

Recommendation 27: Grid operators, utilities, vendors, and aggregators should ensure that supply chain concerns are included in personally identifiable information processing and transparency policies for general and individual information systems. The policies and procedures need to state the access, protection, and retention of personally identifiable information as well as what happens at the end of the end of a contract. (Adapted from NIST SP 800-161r1 PT-1; NATF Energy Sector Supply Chain Risk Questionnaire MOBL-04.)

3.7 Vulnerability and Threat Management

Recommendation 28: Grid operators, utilities, and aggregators, perform risk assessments at the organizational, mission/program, and operational levels, including the supply chain infrastructure, information systems/components traversing the supply chain, cybersecurity roles that are relevant to the supply chain, and an analysis of criticality, threats, vulnerabilities, likelihood, and impact. The data to be reviewed and collected should include the roles, processes, and results of system/component and service acquisitions, implementation, and integration. The data arise from this assessment should be documented in an incident response plan. (Adapted from NIST SP 800-161r1 RA-1, RA-3; NATF Energy Sector Supply Chain Risk Questionnaire THRD-01, CSPM-08, EIR-08.)

Recommendation 29: Vendors should monitor for potential vulnerabilities by employing data collection tools to cover suppliers, sub-suppliers, developers, system integrators, and external/other system service providers in the supply chain. A component inventory can assist organizations in determining which products/components in their supply chain need monitoring. (Adapted from NIST SP 800-161r1 RA-5; NATF Energy Sector Supply Chain Risk Questionnaire RISK-08, CSPM-20.)

Recommendation 30: Through a secure portal, vendors should provide customers with a vulnerability disclosure report, including the analysis and findings describing the impact that a reported vulnerability has on a product as well as plans to address the vulnerabilities. The vulnerability disclosure report should be signed with a trusted, verifiable, private key that includes a time stamp of the signature. (Adapted from NIST SP 800-161r1 RA-5; NATF Energy Sector Supply Chain Risk Questionnaire RISK-08)

Recommendation 31: Vendors should establish a separate notification channel for customers in case a vulnerability arises that is not included in the vulnerability disclosure report. (Adapted from NIST SP 800-161r1 RA-5; NATF Energy Sector Supply Chain Risk Questionnaire VULN-06, VULN-07.)

Recommendation 32: Vendors should express the extent to which they monitor the supply chain for vulnerabilities based on the risk profile or supply chain level of a supplier, sub-supplier, or product/component. (Adapted from NIST SP 800-161r1 RA-5; NATF Energy Sector Supply Chain Risk Questionnaire VULN-06, VULN-07.)

Recommendation 33: Response capabilities to cybersecurity risks throughout the supply chain should be integrated into the overall response posture so that they fall within risk tolerance

boundaries. Identification, alternatives, and decision activities for risk response should also be included. (Adapted from NIST SP 800-161r1 RA-7; NATF Energy Sector Supply Chain Risk Questionnaire EIR-01, EIR-04.)

3.8 Acquisition and Documentation

Recommendation 34: Grid operators, utilities, vendors, and aggregators, should address the acquisition management life cycle process, including requirements that address which controls are mandatory, implementation specifications, acceptable evidence of the satisfaction of requirements, and verification of conformance to requirements. (Adapted from NIST SP 800-161r1 SA-1; NATF Energy Sector Supply Chain Risk Questionnaire EIR-05, EIR-09, RISK-09, VULN-08.)

Recommendation 35: During the acquisition planning phase, grid operators, utilities, vendors, and aggregators should consider the cybersecurity of the supply chain for all procurements of products and services where there could be a potential risk of information being compromised. (Adapted from NIST SP 800-161r1 SA-1; NATF Energy Sector Supply Chain Risk Questionnaire DATA-10.)

Recommendation 36: Grid operators, utilities, vendors, and aggregators should develop policies and procedures that address supply chain risks that might arise during contract performance, such as a change of ownership or when a supplier or product is the target of a supply chain threat. (Adapted from NIST SP 800-161r1 SA-1; NATF Energy Sector Supply Chain Risk Questionnaire THRD-11, EIR-01, RISK-06.)

Recommendation 37: Grid operators, utilities, vendors, and aggregators should establish baseline and tailorable cybersecurity requirements to apply and incorporate into contractual agreements when procuring a product or service from suppliers, developers, system integrators, and external/other service providers. (Adapted from NIST SP 800-161r1 SA-2; NATF Energy Sector Supply Chain Risk Questionnaire COMP-06, COMP-13, THRD-06, THRD-12, DATA-20, EIR-03, RISK-03, RISK-09, RISK-11, RISK-27.)

Recommendation 38: Grid operators, utilities, vendors, and aggregators should establish cybersecurity requirements that provide assurance of a contractor's trustworthiness and cover regulatory mandates while addressing selected controls that are applicable to reducing the cyber supply chain risk from procuring a product or service. (Adapted from NIST SP 800-161r1 SA-2; NATF Energy Sector Supply Chain Risk Questionnaire MOBL-03, RISK-03, CSPM-18, COMP-05, COMP-06, COMP-07, THRD-06, THRD-10, THRD-12, WFM-07, CHNG-02, EIR-02, EIR-03, RISK-03, RISK-09, VULN-05, VULN-06, VULN-08.)

Recommendation 39: Vendors should establish requirements for critical elements in the supply chain to demonstrate the capability to address emerging vulnerabilities based on open-source information. (Adapted from NIST SP 800-161r1 SA-2; NATF Energy Sector Supply Risk Chain Questionnaire RISK-02, THRD-08.)

Recommendation 40: Grid operators, utilities, vendors, and aggregators should establish requirements that address the expected life span of a product, system, or element that might be in a critical path and what is required at the end of its life span. End-of-life options can be

understood from research, bidders, or existing providers. (Adapted from NIST SP 800-161r1 SA-2; NATF Energy Sector Supply Chain Risk Questionnaire CSPM-06, RISK-27, VULN-05, VULN-16, THRD-13.)

Recommendation 41: Grid operators, utilities, and aggregators should document and gain management acceptance and approval for risk that is not fully mitigated. (Adapted from NIST SP 800-161r1 SA-8; NATF Energy Sector Supply Chain Risk Questionnaire CHNG-13, EIR-03, RISK-17.)

Recommendation 42: Vendors should design delivery mechanisms to avoid unnecessary exposure or access to the supply chain and the systems/components traversing the supply chain. (Adapted from NIST SP 800-161r1 SA-8; NATF Energy Sector Supply Chain Risk Questionnaire CSTA-13, THRD-12.)

Recommendation 43: Grid operators, utilities, and aggregators should ensure that cyber supply chain threats, vulnerabilities, and associated risks are identified and documented in relationships with providers. (Adapted from NIST SP 800-161r1 SA-9; NATF Energy Sector Supply Chain Risk Questionnaire VULN-07, THRD-02, EIR-03, EIR-05.)

Recommendation 44: Grid operators, utilities, and aggregators should define and document the consequences of noncompliance with any cybersecurity or information system security requirements in relationships with providers. (Adapted from NIST SP 800-161r1 SA-9; NATF Energy Sector Supply Chain Risk Questionnaire THRD-01.)

Recommendation 45: When grid operators, utilities, or aggregators have control over the application and development processes, they should require third-party testing as well as the testing of off-the-shelf components by suppliers as part of the SDLC based on criticality, threat, and vulnerability analyses. (Adapted from NIST SP 800-161r1 SA-11; NATF Energy Sector Supply Chain Risk Questionnaire CSPM-09, MOBL-10, VULN-14, VULN-15. VULN-18.)

Recommendation 46: Vendors should provide documentation and formalized development processes to guide internal and system integrator developers in mitigating cybersecurity risks. This recommendation should be implemented with national and international standards as well as best practices. (Adapted from NIST SP 800-161r1 SA-15; NATF Energy Sector Supply Chain Risk Questionnaire WFM-08, CHNG-13.)

Recommendation 47: Grid operators, utilities, and aggregators should work with suppliers and partners to ensure that critical components are identified and that they have the continued ability to maintain custom-developed critical software components. (Adapted from NIST SP 800-161r1 SA-20; NATF Energy Sector Supply Chain Risk Questionnaire COMP-06, COMP-07, THRD-10.)

3.9 Communication and Data Privacy

Recommendation 48: Grid operators, utilities, vendors, and aggregators should establish system and communication protection policies to address cybersecurity risks throughout the supply chain, including the coordination of communications, shared resources, electricity markets, communication methods, external connections, and processes used between the organization and

its suppliers, developers, system integrators, and service providers. (Adapted from NIST SP 800-161r1 SC-1; NATF Energy Sector Supply Chain Risk Questionnaire CSPM-05, RISK-12, IAM-13.)

Recommendation 49: Grid operators, utilities, vendors, and aggregators should define a process for information sharing, including privacy, dissemination, handling, clearance requirements, the data shared, the method of sharing, and the specific roles of the data that are shared. Specific information, such as load balancing or engaging in energy markets, should have specific, detailed information sharing processes. (Adapted from NIST SP 800-161r1 SC-4; NATF Energy Sector Supply Chain Risk Questionnaire RISK-08, CSPM-11, DATA-02, DATA-08, DATA-09, DATA-10, DATA-11, DATA-12.)

Recommendation 50: Grid operators, utilities, vendors, and aggregators should implement the use of trusted platform-independent applications to enable more readily switching of external service providers in case one becomes compromised, thus reducing the vendor-dependent cybersecurity risks. (Adapted from NIST SP 800-161r1 SC-27; NATF Energy Sector Supply Chain Risk Questionnaire CSTA-19, CSTA-20.)

Recommendation 51: Vendors should include provisions for the protection of information systems, information at rest, and networks for data at rest into agreements with suppliers, developers, system integrators, and external/other service providers. These provisions should be applied throughout the SDLC. (Adapted from NIST SP 800-161r1 SC-28; NATF Energy Sector Supply Chain Risk Questionnaire DATA-01, DATA-02, DATA-08, DATA-09, DATA-10, DATA-11, RISK-12, RISK-16, THRD-03, THRD-11.)

Recommendation 52: Grid operators, utilities, vendors, and aggregators should employ security safeguards to ensure that only specific individuals or information systems receive the information about the development or processes of information systems. This can be done through the use of proper credentialing and authorization documents. (Adapted from NIST SP 800-161r1 SC-37; NATF Energy Sector Supply Chain Risk Questionnaire DATA-07, THRD-11, IAM-16.1, DATA-10, IAM-01.)

Recommendation 53: Grid operators, utilities, and aggregators should include appropriate suppliers, developers, system integrators, and external/other system service providers in alternative communication paths. (Adapted from NIST SP 800-161r1 SC-47; NATF Energy Sector Supply Chain Risk Questionnaire CSPM-05, CSTA-19.)

3.10 System and Software

Recommendation 54: Vendors should specify the various software assets resulting from criticality analysis that require automated updates. The vendor should specify the procedures for automated updates for residentially deployed solar PV as a separate procedure from utility-grade solar PV. (Adapted from NIST SP 800-161r1 SI-2; NATF Energy Sector Supply Chain Risk Questionnaire CSPM-20, RISK-09.)

Recommendation 55: Vendors should employ a centralized patch management process for evaluating and managing updates prior to deployment. The software assets that require direct updates should only accept updates from the original equipment manufacturer unless specifically

deployed by the acquirer. (Adapted from NIST SP 800-161r1 PT-1; NATF Energy Sector Supply Chain Questionnaire THRD-06.)

Recommendation 56: Vendors should ensure that their code, patches, and system upgrades are protected from malicious code threats that originate downstream in the supply chain through secure methods. (Adapted from NIST SP 800-161r1 SI-3; NATF Energy Sector Supply Chain Risk Questionnaire RISK-08, RISK-12, THRD-03.)

Recommendation 57: Grid operators, utilities, and aggregators should require vendors and service providers to monitor vulnerabilities that resulted from past supply chain cybersecurity compromises. Agreements with these providers should reflect this recommendation. (Adapted from NIST SP 800-161r1 SI-4; NATF Energy Sector Supply Chain Risk Questionnaire VULN-01, VULN-10.)

Recommendation 58: Grid operators, utilities, and aggregators should correlate system monitoring information with suppliers, developers, system integrators, and external/other system service providers to reveal supply chain cybersecurity vulnerabilities. (Adapted from NIST SP 800-161r1 SI-4; NATF Energy Sector Supply Chain Risk Questionnaire RISK-08, RISK-23, IAM-25, EIR-12.)

Recommendation 59: Grid operators, utilities, vendors, and aggregators should implement the enhanced oversight of higher-risk individuals—such as organization employees, contractors, foreign suppliers, and other third parties—in coordination with appropriate officials and in accordance with policies, procedures, and agreements. (Adapted from NIST SP 800-161r1 SI-4; NATF Energy Sector Supply Chain Risk Questionnaire WFM-01, WFM-01.1, WFM-02.)

Recommendation 60: Grid operators, utilities, and aggregators should perform due diligence to understand a supplier's integrity assurance practices when purchasing a service or product. (Adapted from NIST SP 800-161r1 SI-7; NATF Energy Sector Supply Chain Risk Questionnaire COMP-04, COMP-05, COMP-06, COMP-07, COMP-13, THRD-12, IAM-02, CSPM-09.)

Recommendation 61: Grid operators, utilities, vendors, and aggregators should obtain binary or machine-executable code directly from the original equipment manufacturer/developer or other verified source. Grid operators, utilities, vendors, and aggregators should also be provided with the corresponding software bill of materials for monitoring vulnerabilities. (Adapted from NIST SP 800-161r1 SI-7; NATF Energy Sector Supply Chain Risk Questionnaire RISK-02, VULN-03, THRD-08.)

Recommendation 62: Vendors should ensure that code authentication mechanisms are implemented to ensure the integrity of software, firmware, and information. (Adapted from NIST SP 800-161r1 SI-3; NATF Energy Sector Supply Chain Risk Questionnaire IAM-01, IAM-03, IAM-21, IAM-22, IAM-23.)

3.11 Risk Management

Recommendation 63: Grid operators, utilities, vendors, and aggregators should attempt to identify single points of failure and risk among primes and lower-level entities in the supply chain as well as diversify their supply base, especially for critical information and

communications technology/OT products and services. (Adapted from NIST SP 800-161r1 SR-3; NATF Energy Sector Supply Chain Risk Questionnaire IAM-25, CSTA-17, THRD-09, EIR-02.)

Recommendation 64: Grid operators, utilities, vendors, and aggregators should require suppliers to flow controls to subcontractors throughout the SDLC, and the suppliers should be monitored for conformance to the defined controls, requirements, and changes in risk conditions. (Adapted from NIST SP 800-161r1 SR-3; NATF Energy Sector Supply Chain Risk Questionnaire VULN-16, THRD-01, WFM-07, CSPM-11, CHNG-01, DATA-12, RISK-01, RISK-13.)

Recommendation 65: Before a contract award decision, grid operators, utilities, vendors, and aggregators should complete an evaluation of the cybersecurity risks that arise from a supplier, product, or service. (Adapted from NIST SP 800-161r1 SR-3; NATF Energy Sector Supply Chain Risk Questionnaire EIR-12, RISK-17, VULN-07, VULN-10, THRD-02, EIR-05.)

Recommendation 66: Grid operators, utilities, vendors, and aggregators should conduct robust due diligence research on potential suppliers or products along with their upstream dependencies to avoid single points of failure in the supply chain. Research into foreign suppliers should also coincide with backup suppliers. (Adapted from NIST SP 800-161r1 SR-3; NATF Energy Sector Supply Chain Risk Questionnaire VULN-07, CSTA-17.)

Recommendation 67: Grid operators, utilities, vendors, and aggregators should apply any information relevant to the security, integrity, resilience, quality, trustworthiness, or authenticity of suppliers, services, or products against a consistent set of core baseline factors as well as assessment criteria with documented references. (Adapted from NIST SP 800-161r1 SR-6; NATF Energy Sector Supply Chain Risk Questionnaire RISK-20, RISK-27, COMP-13, THRD-02, THRD-11, CSPM-07.)

Recommendation 68: Grid operators, utilities, vendors, and aggregators should conduct a criticality analysis to determine which supply chain components are critical and apply tamper resistance and detection control to the components. (Adapted from NIST SP 800-161r1 SR-9; NATF Energy Sector Supply Chain Risk Questionnaire VULN-03, THRD-10.)

Recommendation 69: Using a criticality analysis, grid operators, utilities, vendors, and aggregators should inspect critical systems and components to ensure that tamper resistance controls are in place and examine whether there is any evidence of tampering. (Adapted from NIST SP 800-161r1 SR-10; NATF Energy Sector Supply Chain Risk Questionnaire CSTA-09, RISK-07.)

Recommendation 70: Grid operators, utilities, and aggregators should inspect products or components prior to use and periodically thereafter. These inspection requirements should be included in contracts with suppliers, developers, system integrators, and external/other system service providers. (Adapted from NIST SP 800-161r1 SR-10; NATF Energy Sector Supply Chain Risk Questionnaire RISK-07, CSTA-09.)

Recommendation 71: Grid operators, utilities, vendors, and aggregators should use criticality analysis to determine the criticality of suppliers to be documented in the supplier inventory,

which should be frequently reviewed and updated. (Adapted from NIST SP 800-161r1 SR-13; NATF Energy Sector Supply Chain Risk Questionnaire COMP-05, COMP-06, COMP-07.)

Recommendation 72: Grid operators, utilities, vendors, and aggregators should develop, document, and maintain an inventory of suppliers that reflects the organization's tier-one suppliers that present a cybersecurity risk in the supply chain. (Adapted from NIST SP 800-161r1 SR-13; NATF Energy Sector Supply Chain Risk Questionnaire RISK-17, THRD-01, THRD-03.)

Recommendation 73: Grid operators, utilities, vendors, and aggregators should develop, document, and maintain an inventory of suppliers that are at the level of granularity necessary for assessing critically and supply chain risk, tracking, and reporting. (Adapted from NIST SP 800-161r1 SR-13; NATF Energy Sector Supply Chain Risk Questionnaire THRD-10, WFM-07, IAM-17, IAM-30, CSPM-11, CHNG-01, CHNG-14, VULN-16.)

4 Conclusion

Solar PV supply chain cybersecurity represents a key area in addressing the security of our nation's electric grid. As deployments of solar PV accelerate to the massive scale required to meet target energy goals for 2030 and beyond, securing and ensuring the safe operation of the solar PV supply chain is critical. Additionally, to address such concerns, cybersecurity must be implemented and adopted now so that securing future PV deployment is easier and leads to further innovations.

This paper outlines recommendations that solar PV aggregators, utilities, vendors, and grid operators can use to increase their cybersecurity posture. The recommendations cover a wide breadth of techniques, including stronger contractual language and tactics for managing vulnerabilities. Additionally, strategies for human elements that exist within the supply chain, such as third-party vendors or contractors, are outlined such that all aspects of the supply chain can be addressed.

References

Aarland, M., and T. Gjøsæter. 2022. "Digital Supply Chain Vulnerabilities in Critical Infrastructure: A Systematic Literature Review on Cybersecurity in the Energy Sector." *Proceedings of the 8th International Conference on Information Systems Security and Privacy*: 326–333. https://doi.org/10.5220/0010803800003120.

Basore, P., D. Feldman, G. Coplon-Newfield, K. Dummit, T. Igogo, S. Nanayakkara, B. Simmons, B. Smith, and M. Woodhouse. 2022. *Solar Photovoltaics: Supply Chain Deep Dive Assessment.* Washington, D.C.: U.S. Department of Energy. https://www.energy.gov/sites/default/files/2022-02/Solar%20Energy%20Supply%20Chain%20Report%20-%20Final.pdf.

Boyens J., A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon. 2022. *NIST SP 800-161r1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.* Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf.

Caddy, C., E. Begoli, S. Chanowski, A. Gates, P. Stockton, and V. Wright. 2022. *Cybersecurity and Digital Components: Supply Chain Deep Dive Assessment*. Washington, D.C.: U.S. Department of Energy. https://www.energy.gov/sites/default/files/2022-02/Cybersecurity%20Supply%20Chain%20Report%20-%20Final.pdf.

Cryar, R., D. Saleem, J. Peterson, and W. Hupp. 2023. *Gap Analysis of Supply Chain Cybersecurity for Distributed Energy Resources*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-84752. https://www.nrel.gov/docs/fy23osti/84752.pdf.

Cybersecurity and Infrastructure Security Agency (CISA). 2021. *Defending Against Software Supply Chain Attacks*. Washington, D.C. https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf.

European Union Agency for Cybersecurity (ENISA). 2021. "Understanding the Increase in Supply Chain Security Attacks." Press release, July 29, 2021. https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks

Feldman, D., K. Dummit, J. Zuboy, and R. Margolis. 2023. "Winter 2023 Solar Industry Update." Presented January 26, 2023. NREL/PR-7A40-85291, 1959948, MainId:86064. https://doi.org/10.2172/1959948.

Feldman, David, Vignesh Ramasamy, Ran Fu, Ashwin Ramdas, Jal Desai, and Robert Margolis. 2021. *U.S. Solar Photovoltaic System Cost Benchmark: Q1 2020*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-6A20-77324. https://www.nrel.gov/docs/fy21osti/77324.pdf.

Igogo, T. 2022. *America's Strategy to Secure the Supply Chain for a Robust Clean Energy Transition*. Washington, D.C.: U.S. Department of Energy. https://doi.org/10.2172/1871491

Johnson, J. 2017. *Roadmap for Photovoltaic Cyber Security.* Albuquerque, NM: Sandia National Laboratories. SAND2017-13262. https://sunspec.org/wp-content/uploads/2020/01/Roadmap-forPhotovoltaic-Cyber-Security-SAND2017-13262-4-10-2018.pdf.

Lee, R., M. Mancusi, A. Hay, and A. Raglani. 2021. "Lessons Learned from the SolarWinds Cyberattack, and the Future for the New York Department of Financial Services' Cybersecurity Regulation." Arnold & Porter. https://www.arnoldporter.com/en/perspectives/advisories/2021/06/lessons-learned-from-the-solarwinds-cyberattack.

Lum, Gordon. 2016. "California Use Case for IEEE2030.5 for Distributed Energy Renewables." *IEEE Smart Grid Bulletin*, December 2016. https://smartgrid.ieee.org/bulletins/december-2016/california-use-case-for-ieee2030-5-for-distributed-energy-renewables.

Martínez, J., and J. M. Durán. 2021. "Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study." *International Journal of Safety and Security Engineering* 11 (5): 537–545. https://doi.org/10.18280/ijsse.110505.

National Institute of Standards and Technology (NIST). 2015. *Best Practices in Cyber Supply Chain Risk Management: Conference Materials*. Gaithersburg, MD. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

North American Transmission Forum (NATF). 2022. "Supply Chain Cyber Security Industry Coordination." https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

Syed, N. F., S. W. Shah, R. Trujillo-Rasua, and R. Doss. 2022. "Traceability in Supply Chains: A Cyber Security Analysis." *Computers & Security* 112. https://doi.org/10.1016/j.cose.2021.102536.

U.S. Government Accountability Office (GAO). 2021. "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response." April 22, 2021. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

Bibliography

Wolff, E., K. Growley, M. Lerner, M. Welling, M. Gruden, and J. Canter. 2021. "Navigating the SolarWinds Supply Chain Attack." *The Procurement Lawyer* 56 (2). https://www.crowell.com/a/web/tHuLUYGJB4SUJCVnZ6pL3h/4Ttkbx/20210325-navigating-the-solarwinds-supply-chain-attack.pdf.