Managing Cyber Supply Chain Risk for Renewable Energy Technologies

Kelli Urban, Jane Pusch, and Jonathan White

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-5R00-80805
September 2021

Managing Cyber Supply Chain Risk for Renewable Energy Technologies

Kelli Urban, Jane Pusch, and Jonathan White

National Renewable Energy Laboratory

Suggested Citation
Urban, Kelli, Jane Pusch, and Jonathan White. 2021. *Managing Cyber Supply Chain Risk for Renewable Energy Technologies.* Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-80805. https://www.nrel.gov/docs/fy21osti/80805.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-5R00-80805
September 2021

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 the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER). The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Acknowledgments

The authors thank the U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) for sponsoring this workshop and for allowing the National Renewable Energy Laboratory to facilitate the event and write this summary report. Thank you also to the DOE Office of Energy Efficiency and Renewable Energy for their active participation and cosponsorship of this event.

The authors are grateful to Cheri Caddy, senior advisor for cybersecurity at DOE CESER, for leading the workshop and giving valuable guidance and support. We are also grateful to the speakers for technical expertise and contributions to the workshop. Finally, we are grateful to the attendees for superb engagement during the event.

List of Acronyms

AMO	Advanced Manufacturing Office
CESER	Office of Cybersecurity, Energy Security, and Emergency Response
CyManII	Cybersecurity Manufacturing Innovation Institute
CyTRICS	Cyber Testing for Resilient Industrial Control Systems
DER	distributed energy resource
DOE	U.S. Department of Energy
EERE	Office of Energy Efficiency and Renewable Energy
E.O.	Executive Order
EV	electric vehicle
FASC	Federal Acquisition Security Council
FEMP	Federal Energy Management Program
GMI	Grid Modernization Initiative
ICS	industrial control system
IT	information technology
NREL	National Renewable Energy Laboratory
OT	operational technology
SECURE	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure
SETO	Solar Energy Technologies Office
WETO	Wind Energy Technologies Office

Executive Summary

On July 1, 2021, the U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) hosted a virtual workshop on "Managing Cyber Supply Chain Risk for Renewable Technologies" for nearly 200 registrants. The workshop was facilitated by the National Renewable Energy Laboratory (NREL).

Cybersecurity supply chain experts, researchers, and leaders in government and industry came together to share information on current and future challenges in securing emerging technologies and architectures related to renewable technologies and distributed energy systems. The presenters explored the critical need to move from a cybersecurity approach focused on legacy asset owners to one that incorporates more emphasis on end-point device manufacturers and third-party integrators.

The program featured opening remarks from Martin Keller, NREL's laboratory director; Kelly Speakes-Backman, DOE's acting assistant secretary and principal deputy secretary for Energy Efficiency and Renewable Energy; and Puesh Kumar, DOE's acting principal deputy assistant secretary at CESER. Each speaker emphasized the importance of the safe and secure deployment of clean energy technologies and safeguarding U.S. critical infrastructure and energy systems from persistent and sophisticated threats, making them more secure and resilient to disruption from cyberattacks, wildfires, and other natural disasters.

Table of Contents

Purpose of the Workshop

Renewables and distributed energy resources (DERs) are increasingly being introduced into the electric grid. This infusion of new technologies is expected to accelerate with the prioritized focus on moving to low-carbon energy sources to mitigate climate change. From an information technology (IT) perspective, this represents a sea change in the technical architecture of the grid as we move toward a model that blends legacy architecture with a new Internet-of-Things structure.

From a cybersecurity perspective, the introduction of a new technical architecture and the integration among existing architectures changes the overall risk for the grid. Collectively, we need to move from a cybersecurity approach that focuses principally on engagement with legacy asset owners to one that also emphasizes end-point device manufacturers and third-party integrators. Cybersecurity for the global digital supply chain for manufacturers of consumer end-point devices—such as smart solar inverters and smart electric vehicle (EV) chargers—will be critical to the future cyber health of the grid.

Workshop Goals

The workshop goals were as follows:

- Increase sector situational awareness of digital supply chain threats and vulnerabilities related to renewable technologies.
- Highlight results of recent research efforts on supply chain vulnerabilities related to renewable technologies.
- Update sector stakeholders on U.S. Department of Energy (DOE) and national laboratory programs to address cyber supply chain cybersecurity for renewables and DERs (wind, solar, storage, hydropower, EVs, building control systems, and grid management systems).
- Increase awareness of the national security and economic security threat environment related to renewable technologies.
- Increase awareness of federal resources to assist companies in safeguarding against intellectual property theft and digital supply chain compromises.
- Develop ideas for community-of-interest efforts in cybersecurity for renewables and momentum for subsequent engagements.

Presentations

Threat Awareness Briefing—Supply Chain Threats in the Energy Sector

The workshop's keynote speaker, Joyce Correll—assistant director, Supply Chain and Cyber Directorate, National Counterintelligence and Security Center—provided a threat awareness briefing on cyber supply chain threats in the energy sector. Correll called attention to five strategic objectives for protecting the nation's critical infrastructure, democracy, economy, and operations:

1. Protect the nation's critical infrastructure.
2. Reduce threats to key U.S. supply chains.
3. Counter the exploitation of the U.S. economy.
4. Defend American democracy against foreign influence.
5. Counter foreign intelligence cyber and technical operations.

Tools and technologies protect each stage of the public, private, and government supply chains. As awareness of the supply chain threats increases, we have transitioned how the U.S. government looks at handling these threats. Even industries are now looking at how regulators and providers can counter foreign intelligence cyber and technical operations. For example, one objective is to prevent foreign attempts to compromise the integrity, trustworthiness, and authenticity of products and services purchased and integrated into the operations of the U.S. government, the defense industrial base, and the private sector.

To address threats more comprehensively to key U.S. supply chains, 2018 legislation created the Federal Acquisition Security Council (FASC). This action stemmed from 2017 policy actions to address cyber risk to federal networks stemming from Kaspersky Lab, a situation where antivirus technology had access to systems and data that could allow Russian security services access to sensitive data. Lessons learned from the Kaspersky example were codified in the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act of 2018, which provided exclusion and removal authorities with the ability to remove or prohibit high-risk technology from being used on federal systems. The SECURE Technology Act provided the means, for the first time, for the U.S. Government to manage cyber supply chain threat intelligence and risks at an enterprise level.

Corell also noted that the cybersecurity threat to industrial control systems (ICS) has the insurance industry looking at how supply chain risks affect the energy sector and how the insurance industry can use cyber risk analytics to make better decisions when placing insurance, underwriting cyber risk, and managing cyber risk aggregation. To minimize the threats to key supply chains, existing threat detection as well as response and mitigation tools should be leveraged across all aspects of the life cycle. Corell emphasized the need to develop new tools and technologies that provide automatic updates to threat information and risk mitigation, enable rapid detection and response to threats, and incorporate artificial intelligence/machine learning to increase agility.

Cybersecurity, Energy Security, and Emergency Response Cyber Supply Chain Programs

Speakers Virginia Wright, Idaho National Laboratory's Energy Cyber Portfolio program manager, and Cheri Caddy, senior advisor for cybersecurity at DOE's CESER Office, introduced Cyber Testing for Resilient Industrial Control Systems (CyTRICS), DOE's cyber vulnerability testing program to work with manufacturers and asset owners to discover, mitigate, and engineer out cyber vulnerabilities in digital components in critical supply chains of the energy sector. CyTRICS uses expert testing across five DOE national laboratories, identifies common-mode vulnerabilities in ICS operational technology (OT) software and firmware, facilitates the sharing of discovered vulnerabilities with energy sector stakeholders, and partners with manufacturers and impacted asset owners to develop mitigations to make critical infrastructure more secure.

CyTRICS partnerships and initiatives support several recent executive orders (E.O.) related to digital supply chain security, including E.O. 13920, E.O. 14017, and E.O. 14028. It also engages in efforts supporting the federal government's response to the cyber supply chain compromise of SolarWinds, and energy sector proof-of-concept projects on using a software bill of materials, a hardware bill of materials, and a digital bill of materials to reveal digital "ingredients" and vulnerabilities as well as standardized testing for ICS. Finally, the speakers previewed a forthcoming strategy on cyber-informed engineering—which will incorporate principles of zero-trust and security-by-design for ICS engineers—that is being developed with input from government, industry, and academic stakeholders. Pursuant to statutory direction, the national cyber-informed engineering strategy will be delivered to U.S. Congress in June 2022.

Energy-Efficiency and Renewable Energy Cybersecurity Efforts—Government Panel

The workshop transitioned to its first of two panel sessions. The National Renewable Energy Laboratory's (NREL's) associate laboratory director of Energy Systems Integration, Juan Torres, introduced DOE Office of Energy Efficiency and Renewable Energy (EERE) panelists Chad Schell, acting program manager, Research and Development Consortia, DOE EERE Advanced Manufacturing Office (AMO); Hayes Jones, strategic director, Federal Energy Management Program (FEMP); Kevin Lynn, director, Grid Modernization, Grid Modernization Initiative (GMI); Jeremiah Miller, system integration technology manager, DOE EERE Solar Energy Technologies Office (SETO); and Jian Fu, acting program manager, Grid Integration, Wind Energy Technologies Office (WETO). Each panelist provided an overview on cybersecurity efforts currently underway.

The AMO partners with industry, academia, states, national laboratories, and nonprofits to help manage Manufacturing USA institutes, including the Cybersecurity Manufacturing Innovation Institute (CyManII), one of many new institutes managed by the AMO. FEMP's cybersecurity goals focus on facility-related control systems and DERs and tools that can help federal agencies operate their own buildings and lead by example in decarbonization, sustainability, energy management, and the efficiency of renewable energy goals. The GMI is a partnership among DOE EERE, the Office of Electricity, CESER, the Office of Fossil Energy and Carbon Management, and the Office of Nuclear Energy. The GMI includes cybersecurity efforts as part of its crosscutting initiatives that span 14 national laboratories and uses a T-shaped approach to investigate cyber firmware in supply chain issues and determines how cybersecurity should be

addressed in different project areas, including generation, storage, flexibility, sensors, and resilience. SETO has strong linkages between solar and cybersecurity. Interconnection standards define the requirements for connecting DERs to the grid and must maintain safety, reliability, power quality, and security. WETO's cybersecurity efforts include a wind security roadmap, architecture and OT, an EV chargers' networks project, and the national Wind Cybersecurity Consortium.

During the roundtable discussion, the panelists identified cybersecurity necessities related to supply chain risk for renewable systems, including:

- New technologies and integrated legacy systems
- Testing and evaluation
- Valuation
- Industry engagement
- Training, education, and workforce development.

Panelists emphasized the need to advance and incentivize new technologies to enable consumers and partners to be more secure. Systems are only as secure as their most insecure part. New technologies mentioned include vehicle electrification manufacturing, autonomous systems, grid-forming solar, and Exascale computing. Catalyzing and funding research and technology that integrates and secures legacy systems is equally as crucial. There is a large investment in legacy systems; it is not practical to start over. New technology must work with legacy systems, and these systems need secure supply chains.

Understanding each technology's impact on power systems and the supply chain issues that follow requires testing and evaluation of equipment. National laboratory facilities and subject matter experts can be leveraged for validation in areas such as solar, EV charging, buildings, manufacturing, and more. Laboratory engagement is important to help solve security challenges as larger systems and the need for capabilities on a larger scale are identified.

Cybersecurity investment simplification is essential for prosumers to incorporate cybersecurity measures from the beginning. Always have security in mind, not only the cost. Cybersecurity requirements applied to capabilities must align with the risk they bring to the grid and the resilience they provide to the grid. Understanding the benefits of being secure helps change the mindset and shift to a culture of developing new approaches to secure the supply chain.

There is a vast need to scale up public-private partnerships and industry stakeholder engagement to promote information sharing, threat sharing, and best practices in a safe environment. Leveraging workshops and other programs to transfer technologies to stakeholders and build best practices is a great approach. Additional outreach includes the need for training, education, and workforce development on cybersecurity threats, challenges, and implementation. Regarding systems security, architectures, devices, OT, transition points between technologies, and people are all points of failure. People should understand these areas and be able to identify key points of failure. Facility-level operators, purchasers, and users should understand where components and parts come from and how to log and monitor components. They should know how to secure an autonomous system and know what a power system should do when under attack. The panelists emphasized education and training, encouraged instruction through science,

technology, engineering, and mathematics, and the development of policies and standards that provide universal adoption and investment in cyber-secure supply chains.

Cybersecurity Manufacturing Innovation Institute and Renewables

Following the EERE panel session, Howard Grimes, chief executive officer of CyManII, provided a briefing on one of the Manufacturing USA efforts supported by the AMO. CyManII tackles hard challenges with a goal of developing next-generation, secure architecture that is secure by design and seeks to transform the mindset from "first to market" to "secure to market." CyManII introduces a cyber-secure energy return on investment for energy-efficient manufacturing and supply chains that secure and sustain American leadership in global manufacturing competitiveness. CyManII offers companies a secure infrastructure to operate technology innovations where security clearance is not needed.

Grimes enumerated six integrated foundational topic areas:

1. Robust roadmap for problem space and research routes
2. Baselining
3. Secure manufacturing architecture
4. Cyber vulnerability awareness
5. Shared research-and-development infrastructure
6. Trust and education.

CyManII's approach is to use a clean slate to design a future state based on state-of-the-art physical systems design and to provide robust space for research and innovation by using more than 60 ranges and 46 advanced manufacturing test beds. Combining physical, cyber, and energy layers in legacy and new systems provides a common framework for a secure and resilient manufacturing architecture. Focusing on the most impact helps decrease cyberattack volume areas and ultimately provides an automated solution for detecting, mitigating, and eliminating cyber vulnerabilities at scale. CyManII aims to cyber-secure U.S. manufacturers and their supply chains against cybercrime, transform the U.S. as a global leader in manufacturing, and promote a sustainable path for education and workforce development based on trust and proactive education, training, and support for all stakeholders, including the next generation of manufacturers in cybersecurity for intelligent and energy-efficient manufacturing.

Cybersecurity for Distributed Energy Resource Management Systems—Industry Panel

The workshop transitioned to an industry panel session. Cheri Caddy introduced the panelists: Maggie Morganti, Schneider Electric; Bryan Owen, OSIsoft LLC; and Young Ngo, Survalent Technology Corporation. The discussion among panelists covered the following themes:

- Ownership
- Increased sensors, data, and privacy concerns
- Vulnerabilities at the seams
- Standards.

More distributed energy systems mean shared cybersecurity responsibilities among an increasing variety of stakeholders, including traditional asset owners, third-party aggregators, and

consumers who own end-point devices such as rooftop solar panels. To provide effective cybersecurity for these assets, data from these distributed systems will need to be collected and aggregated. Someone then needs to process and analyze the data. There is a need for data scientists to understand what the analysis means for power systems.

A path toward improving cybersecurity embraces increased sensors in renewable systems architecture and increased data and information for decision making. Software needs to be adapted for small devices and for massive cloud and big data sets. There is a mutual need for increased visibility over assets and DERs to ensure that they are operating as expected. Critical infrastructure will need to include a safe and secure place for all data to be processed as well as the ability to safely move data between organizations. Privacy is also a concern, which must be balanced against cybersecurity needs for the entire system. Rather than ignore privacy concerns, it would be best to implement simple privacy solutions, such as encryption, message authentication, wrappers, or segmenting information.

The seams where these interconnected systems come together are where the security vulnerabilities arise; different owners of different segments tend to assume others are responsible for key aspects of cybersecurity. Risk analyses need to be done by entities and utilities to determine vulnerabilities in the seams and to ensure a smooth handoff of cybersecurity responsibilities. As asset inventories become more complex, effective means to exchange software bills of materials will be increasingly important to illuminate risk among stakeholders. In this ecosystem of assets and vendors, where cybersecurity impacts are not equal, standardizing methodologies and approaches to vulnerability testing will help all stakeholders feel more confident knowing every zone is secure.

There is an increased number of stakeholders, new and existing, in energy systems. Increased requirements in the form of evolving cybersecurity standards to counter the advancing cybersecurity threats with the convergence of IT, OT, and DER adoption are expected.

Supply Chain for Energy Security

The workshop's closing keynote speaker, Samantha Reese, a senior engineer at NREL, presented a briefing on cybersecurity risks associated with physical supply chains. Where hardware components for energy systems are physically manufactured, opportunities exist for malicious actors to physically alter subcomponents or introduce cybersecurity vulnerabilities into firmware. Reese noted that it is important to ask where the various components of the renewable energy supply chain are manufactured and the potential geopolitical risks. She reviewed trade statistics associated with the global manufacture of key components found in energy sector systems, including silicon wafers, power modules, medium-voltage drives, wide-bandgap power devices, and inverters. Given the current picture of where these strategically important components are manufactured and where raw materials are produced, and given the potential for supply chain disruption, policy changes might be needed.

Conclusions and Next Steps

The introduction of renewables and DERs into the grid will advance grid performance and lower carbon emissions, but will also require an increased focus on cybersecurity and supply chain security for digital components in energy systems. The increasing number of stakeholders—to

include consumers who own end-point devices—and the complexity of energy systems means that broader coordination will be needed to ensure effective cybersecurity. Roles and responsibilities will need to be understood by all to effectively illuminate and manage collective cyber risk—and to ensure that privacy concerns are appropriately managed. Workshop participants learned about several programs—including enterprise-level cyber supply chain threat intelligence and risk management under the FASC, cyber vulnerability testing under CyTRICS, secure manufacturing programs initiated by CyManII, and many others—that can help us collectively meet the challenges to come.

Nearly 200 individuals participated in the virtual workshop. Workshop participants identified several ideas and areas for future collaboration on issues relating to cybersecurity, supply chain risk management, and renewable technology. Subsequent engagements starting in late 2021 will begin to explore these ideas as we work to collectively ensure the future cyber health of the grid.

Appendix A. Agenda

TIME (E.T.)	TOPIC *Speaker*
10:00	Virtual Connection and Networking
10:05	**Welcome/Opening Remarks** Martin Keller, *Laboratory Director at the National Renewable Energy Laboratory (NREL)* Kelly Speakes-Backman, *Acting Assistant Secretary and Principal Deputy Secretary for Energy Efficiency and Renewable Energy (EERE) at the U.S. Department of Energy (DOE)* Puesh Kumar, *Acting Principal Deputy Assistant Secretary, Cybersecurity, Energy Security, and Emergency Response at the U.S. Department of Energy (DOE)*
10:30	**Threat Awareness Briefing—Supply Chain Threats in the Energy Sector** Joyce Correll, *Assistant Director, Supply Chain and Cyber Directorate* *National Counterintelligence and Security Center, Office of the Director of National Intelligence*
11:15	**Cybersecurity, Energy Security, and Emergency Response (CESER) Cyber Supply Chain Programs** Virginia Wright, *Program Manager, Idaho National Laboratory* Cheri Caddy, *Senior Advisor for Cybersecurity, CESER*
12:00	Break
12:30	**Energy Efficiency and Renewable Energy (EERE) Cybersecurity Efforts—Government Panel** Chad Schell, *Acting Program Manager, Research and Development Consortia, Advanced Manufacturing Office* Hayes Jones, *Strategic Director, Federal Energy Management Program* Kevin Lynn, *Director, Grid Modernization, Grid Modernization Initiative* Jeremiah Miller, *System Integration Technology Manager, Solar Energy Technologies Office* Jian Fu, *Acting Program Manager, Grid Integration, Wind Energy Technologies Office* *Moderator:* Juan Torres, *Associate Laboratory Director for Energy Systems Integration, NREL*
1:40	**Cybersecurity Manufacturing Innovation Institute (CyManII) and Renewables** Howard Grimes, *Chief Executive Officer, CyManII*
2:00	**Cybersecurity for Distributed Energy Resources Management Systems (DERMS)—Industry Panel** *Maggie Morganti, Schneider Electric* *Young Ngo, Survalent* *Bryan Owen, OSIsoft* *Moderator:* Cheri Caddy, *Senior Advisor for Cybersecurity, CESER*
3:00	Break
3:15	**Supply Chain for Energy Security** Samantha Reese, *Senior Engineer, NREL*
3:40	Open Discussion
3:50	Closing Remarks Cheri Caddy, *Senior Advisor for Cybersecurity, CESER* Jonathan White, *Cybersecurity Program Director, NREL*
4:00	Adjourn