U.S. DEPARTMENT OF ENERGY

Office of ENERGY EFFICIENCY & RENEWABLE ENERGY

Roadmap for Wind Cybersecurity

July 2020

This page is intentionally left blank.

Notice

Acknowledgments

This work was funded by the U.S. Department of Energy (DOE) Energy Efficiency and Renewable Energy (EERE) Wind Energy Technologies Office (WETO).

DOE's Idaho National Laboratory (INL) would like to thank the following authors and their dedication and commitment to the development of this Roadmap: Anuj Sanghvi (National Renewable Energy Laboratory, NREL), Brian Naughton (Sandia National Laboratories, SNL), Colleen Glenn (INL), Jake Gentle (INL), Jay Johnson (SNL), Jeremiah Stoddard (INL), Jonathan White (NREL), Nicholas Hilbert (SNL), Sarah Freeman (INL), Shane Hansen (INL), and Shawn Sheng (NREL).

This page is intentionally left blank.

Acronyms

AIS	Automated Indicator Sharing
APT	Advanced persistent threat
AWEA	American Wind Energy Association
CATT™	Cyber Analytics Tools and Techniques Program
CEDS	Cybersecurity for Energy Delivery Systems
CERT	Computer Emergency-Response Teams
CESER	Cybersecurity, Energy Security, and Emergency Response
CCE	Consequence-driven Cyber-informed Engineering
CIE	Cyber-informed engineering
CIP	Critical infrastructure protection
CIPC	Critical Infrastructure Protection Committee
CISA	Cybersecurity and Infrastructure Security Agency
CISCP	Cyber Information Sharing and Collaboration Program
CRISP™	Cybersecurity Risk Information Sharing Program
CyOTE™	Cybersecurity for the Operational Technology Environment
CyTRICS™	Cyber Testing for Resilience of Industrial Control Systems
DER	Distributed energy resources
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DMZ	Demilitarized zone
DoD	Department of Defense
DOE	Department of Energy
DoS	Denial-of-service
DW	Distributed wind
EERE	Energy Efficiency and Renewable Energy
ESIG	Energy Systems Integration Group
FERC	Federal Energy Regulatory Commission
HMI	Human-machine interface
ICS	Industrial control systems
IDS	Intrusion detection systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INL	DOE's Idaho National Laboratory

IT	Information technology
LAN	Local area network
MiTM	Man-in-the-middle
MTD	Moving-target defense
NCCIC	National Cybersecurity and Communications Integration Center
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NREL	DOE's National Renewable Energy Laboratory
OEM	Original equipment manufacturer
OT	Operational technology
PII	Personal identifiable information
PLC	Programmable logic controller
PV	Photovoltaic
R&D	Research and development
RBAC	Role-based access control
RD&D	Research, development, and demonstration
RTOS	Real-time operating systems
SA	Situational awareness
SCADA	Supervisory control and data acquisition
SNL	DOE's Sandia National Laboratories
VPN	Virtual Private Network
WETO	DOE's Wind Energy Technologies Office
WTG	Wind turbine generator

Executive Summary

As the percentage of wind and other renewable energy systems grows among power generators in the United States, cybersecurity for integrated control systems and related technology has become an increasingly important and urgent matter. Cyber threats, current and expected, are outpacing cybersecurity capabilities, posture, and expertise. Additionally, in the case of wind energy, which recently surpassed 7 percent of U.S. electric power production, its increasing utilization necessitates dedicated attention to identify vulnerabilities, raise awareness, and formulate strategies for cybersecurity defense, responses, and future protection. These may include an array of wind-specific cyber-research and development, further development of standards and protocols, the promotion of best practices for cybersecurity, and expanded information sharing and engagement among wind energy stakeholders.

Table 1 presents a framework, or time-phased roadmap, for addressing such challenges, building strategies, and meeting milestones for improving wind energy cybersecurity in the near-, mid-, and long-term. The components of this roadmap are specific to wind energy, but many may be applicable, as well, to other forms of energy and their control systems. All are illuminated in more detail throughout the sections of this document.

Importantly, this *Wind Energy Cybersecurity Roadmap* is not intended to be prescriptive, but rather a summary of critical infrastructure cybersecurity best practices and, looking to the future, a list of possible next steps to serve as a model for the wind industry and the strengthening of its cyber resiliency. Organizations, owners, operators, and industry stakeholders may adopt various aspects that best meet their individualized needs. Wind industry cybersecurity and resiliency can be improved. The means for doing this will be a combination of research, development, adoption, and expansion of cybersecurity technologies and best practices by the public and private sector.

Table 1. Cybersecurity Roadmap for Wind Industry.

Vision	**Wind energy systems are designed, retrofitted, and operated for resiliency to cyber events, minimizing potential impacts to turbine equipment and the power grid.**
Challenges	▪ Cyber incidents targeting wind energy systems have already occurred, just as with other aspects of the Energy Sector, and will likely increase in sophistication and number ▪ The wind plant lifecycle involves many parties; effective cybersecurity practices are difficult to establish, maintain, and trace through the supply chain from construction to operation to repowering to decommissioning ▪ Wind generation assets require robust cybersecurity practices to ensure continued integration with the bulk electric system ▪ Wind energy technologies and deployments are highly diverse; no single cybersecurity strategy can apply to all wind plants ▪ Effective, available cybersecurity options may be cost-prohibitive for some wind installations ▪ Few established cybersecurity standards specific to wind energy exist ▪ Few incentives for wind energy stakeholders have been established to prioritize cybersecurity over other investments (e.g., reliability, performance, etc.) ▪ Cyber threat, vulnerability, incident, and mitigation information sharing is limited among wind energy stakeholders ▪ Current market offers few and underdeveloped wind-specific cybersecurity services, products, and strategies

Strategies	**Develop Wind Cyber-Culture:** Promote cybersecurity culture among wind energy community, encouraging cybersecurity information sharing including cyber threats, Indicators of Compromise (IOC), vulnerabilities, cyber incidents, attack patterns, lessons learned, and best practices; facilitate and support a cooperative environment for the exchange of information, ideas, and collaborative efforts among wind energy stakeholders	**Identify and Protect:** Develop an organizational understanding to manage cybersecurity risk to wind assets, data, and grid infrastructure; develop and implement appropriate cyber-safeguards to ensure delivery of wind energy	**Detect:** Develop and implement appropriate detection technologies to identify malicious or unintentional cybersecurity events impacting wind technologies or networks	**Respond and Recover:** Encourage development and implementation of appropriate activities to take timely and effective action to mitigate cybersecurity incidents; execute plans for resilience and restore wind energy capabilities or services
Near-Term Milestones	▪ Establish and regularly conduct cyber-focused workshops, trainings and working groups to promote awareness, change behavior, and develop consensus-based security approaches ▪ Standardize cyber threat and vulnerability information-sharing methods, framework, and mechanisms ▪ Share cybersecurity alerts among wind community	▪ Identify critical wind assets in the context of cybersecurity and evaluate impact of wind on broader grid security ▪ Identify adversaries and threat models relevant to wind energy ▪ Design and develop wind specific reference architectures; identify potential cyber attack surface based on architectures ▪ Design or leverage existing asset-based plug-and-play testbeds to evaluate wind technologies ▪ Develop best practices for wind energy business and operational environments that cover basic cyber hygiene and best practices to secure wind communication systems	▪ Implement standardized cyber threat and vulnerability information-sharing method, framework, or appliance ▪ Research and validate wind-specific intrusion detection system techniques and methodologies ▪ Promote guidelines for effective situational awareness methods for wind energy operational technology (OT) security ▪ Establish public-private sector partnerships to actively share threat indicators, reports of compromise, and adversary tactics techniques and procedures (TTPs)	▪ Define cybersecurity roles and responsibilities among owners/operators, vendors and service providers, and government ▪ Coordinate directly with DHS and DOE stakeholders to grow wind-specific incident response capability ▪ Develop dynamic assessment technologies to assess wind control networks

Mid-Term Milestones	▪ Wind plant owners and operators share mitigation strategies with each other and the larger cyber-information sharing community ▪ Lessons learned are regularly documented and available to the wind energy community, and broader energy sector ▪ Make software and tools available to secure wind energy systems; employ field-proven best practices ▪ Wind owner/operators regularly participate in cybersecurity exercises and participate in broader energy sector exercises, where appropriate ▪ Establish an advisory committee to research, report, and provide recommendations	▪ Validate existing wind reference architecture through onsite assessments ▪ Identify attack pathways applicable to wind; leverage or extrapolate attack pathways from other sectors to defend wind systems ▪ Establish effective defense methodologies to protect wind energy operational environments ▪ Develop and provide community-wide access to testbed environments to investigate potential cyber-vulnerabilities in wind energy devices and equipment ▪ Expand wind reference architecture best practices to include additional defenses	▪ Improve and deploy wind-specific anomaly-based intrusion detection technologies ▪ Develop, test, and deploy situational awareness sensors, tools, and training for wind energy environments that can be feasibly adopted by industry	▪ Develop effective cyber incident response procedures for wind owners/operators ▪ Implement courses of action in coordination with the system operator/balancing authority/reliability coordinator ▪ Implement broad field testing of system restart and resiliency capabilities ▪ Promote cybersecurity resources for owners/operators and vendors (incident response, cybersecurity best practice guides, etc.)
Long-Term Goals	▪ Sustain improvement to wind cybersecurity software and tools; significantly increase technician wind cybersecurity knowledge and skills ▪ Develop and standardize secure communication architectures and protocols, access rules, certification procedures, and wind energy equipment standards ▪ Develop OT cybersecurity workforce for wind energy	▪ Conduct methodological processes to inventory, evaluate, and document wind energy systems based on cybersecurity posture ▪ Develop cyber-resilient wind plant designs ▪ Encourage appropriate representation of cybersecurity-specific standards for wind plant control communications and equipment ▪ Establish a standards certification process and authority ▪ Maintain established testbeds to identify emerging cyber threats and vulnerabilities to wind energy technologies	▪ Educate relevant government and private sector partners to understand wind technologies so future threat intelligence and alerts are understood and acted on appropriately ▪ Support continued R&D for intrusion detection for continuously evolving adversary techniques and future wind technologies	▪ Incorporate new or enhance existing cyber threat, vulnerability, incident, and mitigation information-sharing platform inclusive of wind energy technologies ▪ Continued R&D for incident response for new and evolving cyber threats ▪ Establish wind industry-specific guidelines for cyber incident reporting and post-incident investigations; and establish guidelines for cyber event response and recovery

Key findings from the Roadmap for Wind Cybersecurity include:

A shifting wind energy design landscape demands an altered cybersecurity paradigm. As wind becomes an ever-increasing part of the "smart grid" landscape, the bidirectional communication upon which wind energy equipment is reliant upon also introduces significant cybersecurity concerns. The increasing reliance for dynamic operation of wind systems based on both internal plant data and external information requires network communication capabilities. Local and remote connectivity among wind plant field devices, control equipment, control centers, and business networks using a range of standard and proprietary communication protocols expands the technological landscape that should be adequately monitored and protected via established cybersecurity practices.

Cyber threats to wind energy technology have been established and demonstrated, both in theoretical and real-world instances. Prominent academic interest in wind vulnerabilities suggests that malicious cyber-actors may be similarly interested in wind technology. Several wind-related academic studies indicate that cyber attacks can destabilize systems and physically damage wind turbines. There is evidence, as outlined in chapter 3, that successful cyber-intrusions and attacks on wind energy systems have occurred.

Wind energy-specific cybersecurity research and development is critical to the defensive protection of wind assets from cyber threats. New or continuing research in wind energy technology, including the development of cyber threat models, completion of cyber assessments, development and use of testbed environments, network analysis capabilities (e.g., passive monitoring, intrusion detection), cyber forensics techniques, and research of system resiliency can aid in mitigating electric system impact as wind energy grows. Academic research has explored the periphery of wind energy systems in the context of cybersecurity, but greater depth and breadth in the cyber vulnerabilities and threats specific to wind are needed.

Further development of wind energy-specific standards is needed, particularly those related to cybersecurity. Standards for communication, equipment, and security practices are currently underdeveloped or absent from the wind industry. Cybersecurity standards specific to wind energy currently do not exist. The wind industry largely depends on standards developed for other energy systems and technologies, meaning that the specific cybersecurity needs of wind energy technologies are not well understood. Standards provide a good baseline of digital and physical security for wind systems and reduce cyber-risk for asset owners.

Wind energy stakeholders can adopt numerous technical, administrative, physical, and supply chain-related practices to improve cybersecurity, such as network segmentation, developing and maintaining cyber asset lists, possessing a cyber emergency response plan, vetting internal and vendor-owned supply chains, and conducting basic cyber hygiene. Further, continued research and development can contribute to identifying new practices while also improving existing best practices.

Many proactive opportunities exist for wind energy stakeholders—including developers, owners, operators, vendors, consultants, government, and academia—to engage more broadly and thoroughly on cybersecurity issues. Greater collaboration and sharing of information among all stakeholders have benefits to the wind industry. Due to ever evolving threats, ongoing development and maintenance by the wind industry of cyber culture, equipment, standards, and best practices, along with cutting-edge cybersecurity research and development, is of high importance in making progress towards the long-term vision for cyber-resilient wind energy systems.

This page is intentionally left blank.

Table of Contents

List of Figures

List of Tables

This page is intentionally left blank.

Introduction

The cybersecurity of wind energy systems is becoming increasingly important. Over 50,000 wind turbines with a cumulative installed capacity of 105,583 MW[1] are operating in the United States, providing 7.3% of the nation's electricity in 2019.[2] Yet current and expected future cyber threats are outpacing the wind industry's cybersecurity capabilities, posture, and expertise. Cyber-intrusions and attacks on wind energy systems have been reported[i] in recent years, demonstrating increasing adversary interest and capabilities in targeting these systems. Without adequate protection, malicious attacks are likely to increase and cause severe cascading failures involving not only cyber and physical devices and operations of the wind plant, but also the reliability of the electric grid.

The ownership and operation of wind plants are unique among other forms of power generation. Numerous utility-scale wind plant owners operate across the United States; as of 2018, independent power producers own 83% of all wind energy assets.[3] Unlike conventional power plants commissioned, owned, and operated by a utility, wind plants may change ownership multiple times throughout a plant's full lifecycle. It is also common for multiple independent companies to develop, own, operate, and maintain a wind plant. Wind plants often consist of myriad makes, models, and configurations of equipment, meaning that asset lists, configurations, procedures, and many other items critical to an effective cybersecurity posture are more likely to be poorly defined in ownership transfers, if at all defined and documented. Additionally, wind plant owners are increasingly upgrading turbines with aftermarket products without consulting the original equipment manufacturer (OEM), including adding and swapping controllers and sensors. Change management, including records of software/firmware updates or changes, additions or removals of digital devices, and up-to-date access control lists, may be difficult to maintain.

Successful cyber attacks on wind plants can deteriorate power systems in various aspects, such as wind plant system stability, energy market operations, and grid reliability. The detailed considerations of cyber attack modeling, detection, and mitigation are of primary interest in addressing the cybersecurity of wind plants. Furthermore, testbed environments would enable researchers to investigate the existing and potential cyber vulnerabilities of wind field devices and architectures, power system risks, and defensive strategies. For example, any errors in wind turbine field devices due to malfunctions or cyber attacks may disrupt the wind plant's efficiency as well as the reliability of the electric grid.

A robust, comprehensive cybersecurity strategy seeks to ensure safe, consistent, and uninterrupted operation of wind facilities by anticipating threats and vulnerabilities, and by defending and protecting information technology (IT) and operational technology (OT) assets from both internal and external threats. Maintaining a strong cyber-posture in wind facilities requires constant vigilance to ensure the enforcement of best practice cybersecurity policies. Although cybersecurity deals primarily with external or internal attacks, and cyber-reliability addresses intrinsic functions of the wind plant, the close connection between the two should be considered in efforts to develop methodologies and approaches to ensure secure and reliable system operations. Ultimately, uninterrupted operation requires efforts to develop smart wind assets that are also cyber-resilient.

This roadmap discusses current national cybersecurity efforts, wind industry cybersecurity landscape, R&D areas, best practices, standards development, and stakeholder engagement activities. It is a strategic goal that

[i] Chapter 3 outlines a collection of recent established cyber events to wind energy system, including a March 2019 attack to a large, Utah-based wind owner/operator's electrical system operations by disrupting communications between a control center and wind and solar generation sites.

wind energy systems are designed, retrofitted, and operated for resiliency to cyber events, minimizing potential impacts to turbine equipment and the power grid.

It should be noted that the findings in this document are generally related to utility-scale, land-based wind assets and technology. However, it is important to note the operational technology required to control, monitor, and interconnect distributed wind (DW) assets to a microgrid or distribution system is often similar or the same as that for large wind plants. This means that DW faces the same cyber threat landscape as large-scale wind. Though DW systems are typically smaller than 20 MW and are defined by technology application rather than technology size,[4] the total installed capacity of nationwide DW exceeded 1 GW in 2018; 78% of this capacity served utility loads on local distribution grids.[5] Similarly, offshore wind also relies on the same operational technology that enables land-based wind assets. With one 30-MW offshore wind facility currently operating in the United States and 30 projects totaling approximately 25 GW in planned installed capacity underway,[6] offshore wind is expected to provide a significant amount of electricity to the power system. As with all wind energy technologies, offshore wind requires significant research and development (R&D) to identify, protect, analyze, and respond to current and future cyber vulnerabilities and threats.

1 National Energy Cybersecurity Efforts

The United States' critical infrastructure provides essential services that underpin American society. Energy is one of 16 critical infrastructure sectors—the health and vitality of which are instrumental to U.S. national security.[7] The United States' energy infrastructure fuels the U.S. economy and has been identified as uniquely critical because it provides an "enabling function" across all critical infrastructure sectors.[8] Without a stable energy supply, the health and welfare of American citizens are threatened, and the U.S. economy cannot function.

In the United States, energy assets and critical infrastructure components are owned by private, federal, state, and local entities.[9] More than 80% of the country's energy infrastructure is owned by the private sector.[10] Because of this wide array of energy sector shareholders, the development and maintenance of public/private partnerships is a valuable means by which the energy sector can realize security and resilience goals.

Current energy infrastructure is primarily operated and maintained through interdependent physical and cyber-systems. Furthermore, energy owners and operators have increasingly integrated advanced digital technologies to automate and control physical functions to improve performance. This increased integration of advanced technologies into energy infrastructure has created a larger cyber attack surface, which has led to more frequent and sophisticated attacks that are increasingly launched by nation-states and cyber-criminals. In response, the government and private sector continue to increase spending on cybersecurity operations and maintenance.[11]

The U.S. Department of Energy (DOE) leads the federal government's effort to ensure cyber attacks do not catastrophically impact the energy sector. DOE provides support to the U.S. energy sector by pursuing high-priority activities that are coordinated with the strategies, objectives, and activities of the broader federal government and energy sector stakeholders.[12] Leveraging people, partnerships, and resources found in its various offices and national laboratories, DOE seeks to reduce cyber-risk for the energy sector by following the goals and objectives enumerated in the DOE Multiyear Plan for Energy Sector Cybersecurity.[13]

1.1 Existing, Related Cybersecurity Projects and Programs

1.1.1 DOE Office of Cybersecurity, Energy Security, and Emergency Response

The DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER), established in February 2018, has the task of improving energy infrastructure security and supporting DOE's national security mission.[14] Furthermore, CESER leads DOE's emergency preparedness efforts and coordinates responses to energy sector disruptions, including physical and cyber attacks, natural disasters, and man-made events.[15] CESER also invests in R&D by private industry and the national laboratories for the next generation of advanced technologies.[16] CESER's Cybersecurity for Energy Delivery Systems (CEDS) R&D program aligns all activities with federal priorities and the strategy and milestones articulated in the Energy Sector Control Systems Working Group's Roadmap to Achieve Energy Delivery Systems Cybersecurity.[17] CESER develops and supports numerous programs including public-private data sharing and analysis platforms, such as:

- The Cybersecurity Risk Information Sharing Program (CRISP™); managed by the Electricity Information Sharing and Analysis Center (E-ISAC), CRISP demonstrates a public-private partnership meant to enable the exchange of classified and unclassified threat information
- The Cyber Analytics Tools and Techniques Program (CATT™ 2.0); an IT and OT direct-data sharing and analysis program via the Cybersecurity for the Operational Technology Environment (CyOTE™) focused on providing sector wide situational awareness for cybersecurity.
- The Cyber Testing for Resilience of Industrial Control Systems (CyTRICS™) program, which inventories and tests energy sector digital components to correlate with cyber threat and supply chain information.[18]

Each of these programs is discussed in greater detail in subsequent sections.

These dedicated CESER programs not only advance cybersecurity for energy delivery systems, but lay a solid foundation for other energy technologies, like wind, to leverage and address their specific cybersecurity needs.

1.1.2 DOE Office of Energy Efficiency and Renewable Energy

The DOE Office of Energy Efficiency and Renewable Energy's (EERE's) mission is to create and sustain American leadership in the transition to a global clean energy economy.[19] EERE achieves its mission through initiatives and projects relating to next-generation renewable power, advanced transportation, and energy efficiency and advanced manufacturing technologies.[20] In particular, EERE is partnering with CESER to establish a Clean Energy Manufacturing Innovation Institute dedicated to advancing cybersecurity in energy efficient manufacturing.[21] The Institute will pursue targeted R&D focused on understanding the evolving cybersecurity threat to greater energy efficiency in manufacturing industries, developing new cybersecurity technologies and methods, and sharing information and knowledge to the broader community of U.S. manufacturers.[22]

The EERE's Wind Energy Technologies Office (WETO) invests in energy science R&D activities that enable advanced U.S. wind system innovations that reduce the cost of electricity and technical barriers in ways that accelerate the deployment of wind power.[23] WETO works with national laboratories, industry, universities, and other agencies to conduct R&D activities through competitively selected, directly funded, and cost-shared projects.[24] WETO is investing in cybersecurity R&D to ensure the safe and secure production of wind power.

1.1.3 Other Entities

Coordination and collaboration with a number of other stakeholders in the critical infrastructure protection mission space will strengthen wind industry and DOE efforts for cybersecurity. On November 16, 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018. This landmark legislation elevated the mission of the former National Protection and Programs Directorate (NPPD) within the Department of Homeland Security (DHS) and established the Cybersecurity and Infrastructure Security Agency (CISA), which includes the National Cybersecurity and Communications Integration Center (NCCIC). Prior to the establishment of CISA, NCCIC realigned its organizational structure in 2017, integrating like functions previously performed independently by the U.S. Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

The DHS's CISA works with industry and state, local, tribal, and territorial governments to secure critical infrastructure and information systems.[25] The US-CERT and the ICS-CERT work to reduce risks within and across all critical infrastructure sectors, providing services like onsite incident response, analysis of malware threats to control system environments at the Advanced Analytical Laboratory, and site assistance and evaluations.[26] CISA also provides information on emerging threats and hazards so that appropriate actions can be taken, as well as industrial control systems (ICS) tools and training to partners to help those in government and industry manage the risks to their assets, systems, and networks.[27] Additionally, CISA collaborates with international and private sector cyber emergency response teams (CERTs) to describe control systems-related security incidents and mitigation measures.[28] Also within CISA, the National Risk Management Center works to identify and address the most significant risks to U.S. critical infrastructure, including infrastructure cybersecurity. The National Risk Management Center incorporates current cyber threat and vulnerability information into its planning, analysis, and collaboration activities in protecting critical infrastructure interdependencies and critical functions.[29]

The Federal Energy Regulatory Commission (FERC) is an independent federal agency that regulates the interstate transmission of electricity, among other things.[30] FERC's Office of Energy Infrastructure Security provides leadership and expertise, and help the Commission identify, communicate, and mitigate potential risks to FERC-jurisdictional facilities from cyber attacks and other physical threats.[31] FERC has statutory authority to oversee the reliability of the power grid and does so through its approval of North American Electric Reliability Corporation (NERC) created and enforced mandatory reliability standards.[32] FERC-approved reliability standards include Critical Infrastructure Protection (CIP) standards that guide industry in the management of cybersecurity and physical risk.[33] FERC also designates an independent entity within a particular jurisdiction as the electricity reliability organization that develops and enforces mandatory standards for the reliable operation and planning of the power grid.[34]

NERC is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid within the continental United States and other jurisdictions.[35] NERC is the electricity reliability organization for North America and is subject to oversight by FERC.[36] The mission of NERC's Critical Infrastructure Protection Committee (CIPC) is to assist in the advancement of cyber- and physical security of the electricity infrastructure of North America.[37] NERC stakeholders include members, governments, all participants in the bulk-electric power system, and end-use electricity customers. CIPC plays an active role in the development of the FERC-mandated Critical Infrastructure Protection (CIP) standards.[38] NERC has adopted these CIP standards for the protection and security of critical cyber assets supporting the power grid; CIP standards are mandatory and enforceable.[39] NERC operates the Electricity Information Sharing and Analysis Center (E-ISAC), which gathers and analyzes security data, shares appropriate data with stakeholders, coordinates incident management, and communicates mitigation strategies with stakeholders.[40] E-ISAC, in collaboration with DOE and the Electricity Subsector Coordinating Council, serves as the primary security communications channel for the electric industry and

enhances the industry's ability to prepare for and respond to cyber- and physical threats, vulnerabilities, and incidents.[41] In operating CRISP, E-ISAC collects, analyzes, and shares cyber-alerts and mitigations to energy sector owners and operators.[42] E-ISAC also holds an annual conference called GridSecCon that brings together cyber- and physical security experts from industry and government to share emerging security trends, policy advancements, and lessons learned related to the electricity industry.[43] NERC holds a 2-day electrical grid security exercise, known as GridEx every 2 years.[44] GridEx is a simulated cyber and physical attack on the North American power grid that provides an opportunity for various energy sector stakeholders to respond to and recover from grid security emergencies, strengthen crisis communication relationships, and provide input for lessons learned.[45]

1.2 Strategic Cybersecurity Objectives

In September 2018, the White House released the National Cyber Strategy of the United States of America.[46] The strategy's four objectives are to:

1. Defend the homeland by protecting networks, systems, functions, and data
2. Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation
3. Preserve peace and security by strengthening the United States—in concert with allies and partners—to deter and, if necessary, punish those who use cyber-tools for malicious purposes
4. Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.[47]

The National Cyber Strategy's first objective of defending the homeland includes managing cybersecurity risks to increase the security and resilience of the nation's information systems. These information systems include not only federal networks but also those of the nation's critical infrastructure. The responsibility to secure the nation's critical infrastructure and manage its cybersecurity risk is shared by the private sector and the federal government. The National Cyber Strategy prioritizes risk-reduction activities across the following seven key areas: national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation.[48]

In support of the National Cyber Strategy, DOE released its Cybersecurity Strategy 2018–2020.[49] The strategy identifies the following four crosscutting principles:

1. "One Team, One Fight"
2. Employment of risk-management methodology
3. Prioritizing planning and resourcing
4. Enterprise-wide collaboration.[50]

These principles reflect DOE's prioritization of cybersecurity and illustrate the need for agility in evaluating and modifying cybersecurity priorities. Cybersecurity must receive appropriate resource allocation and focus commensurate with its priority status, and DOE's cybersecurity approach should be collaborative, and customer focused.[51]

DOE's Cybersecurity Strategy 2018–2020 enumerates four goals that apply to the aforementioned principles. The goals are to:

1. Deliver high-quality IT and cybersecurity solutions
2. Continually improve cybersecurity posture
3. Transition from IT owner to IT broker for better customer focus
4. Excel as stewards of taxpayer dollars.[52]

The Cybersecurity Strategy aligns with the March 2018 DOE Multiyear Plan for Energy Sector Cybersecurity to strengthen cyber-systems and risk management capabilities and develop innovative solutions for inherently secure and resilient systems.[53] The DOE Multiyear Plan for Energy Sector Cybersecurity sets forth three goals (see Table 2) as part of its support of the energy sector's risk management roles to strengthen cyber-systems in operation as well as support of the R&D that will build cyber-resilience into future systems.[54]

Table 2. DOE Multiyear Plan for Energy Sector Cybersecurity Strategy.

Strategic Goal[ii]	Methodology/Approach
Strengthen energy sector cybersecurity preparedness	Public and private sector partnerships leverage DOE-supported tools, guidelines, outreach, training, and technical assistance.
Coordinate cyber incident response and recovery	Private sector and DOE to establish a cohesive national cyber incident response approach designed for smooth coordination with private-sector partners during an incident and confirming that incident management roles are not in conflict. In parallel with this effort, DOE will work with DHS and non-federal partners to assess the nation's cyber incident response capabilities in the energy sector.
Accelerate game-changing RD&D of resilient energy delivery systems	Deliver tools and technologies that self-defend by automatically detecting, rejecting, and withstanding cyber incidents instead of the current reactionary cycle of cybersecurity solutions. DOE aims to achieve this goal by continuous transition of long-term innovative research into capabilities that the energy sector can put into practice to reduce cyber-risk.

WETO's R&D planning for fiscal years 2019 through 2023 include strategies to remove barriers to wind energy grid integration, find innovative ways to couple renewable energy technologies, and to enable

[ii] DOE's Cybersecurity Strategy aligns itself with related frameworks and strategies and furthers the implementation of cybersecurity statutes and executive orders. DOE's Cybersecurity Strategy operates in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), Federal IT Acquisition Reform Act, Executive Orders and Memoranda (e.g., Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure), National Institute of Standards and Technology (NIST) standards and practices (such as the Framework for Improving Critical Infrastructure Cybersecurity [Cybersecurity Framework]), DHS Binding Operational Directives, and DOE policies, including DOE Order 205.1, Cyber Security Program.

economic and reliable power grid operation with large shares of wind energy. WETO's efforts to remove barriers to grid integration will include developing cybersecurity strategies. WETO plans to coordinate with other DOE offices (e.g., CESER) to leverage current advancements in cybersecurity and address wind-specific cybersecurity challenges.

Leveraging DOE facilities for wind research, development, and testing is another WETO strategic initiative, which offers multiple opportunities to address cybersecurity by maintaining, supporting, and leveraging existing non-WETO-funded facilities and assets to enable strategic wind R&D. WETO will continue to fund R&D projects and partner with national laboratories that offer the expertise and specialized equipment needed (e.g., malware analysis, modeling and simulation facilities, etc.) to perform state-of-the-art wind R&D. WETO intends to further utilize existing integrated research, development, demonstration, and full-scale operational facilities across multiple national laboratories and industry partners to support wind-cyber R&D. These facilities are valuable to WETO's efforts as they can be linked with other technology-focused cyber research and modeling and simulation efforts within the same facilities at the national laboratories, offering a full perspective of cyber-physical risk to wind technologies and the broader energy ecosystem. Strategic collaborations with other U.S. government agencies, other DOE offices and programs, as well as industry and academic partnerships may prove to be important in supporting the security of the nation.

2 Wind Energy Technology Landscape

Wind plants convert wind to electricity by extracting kinetic energy of moving air, turning it into mechanical torque that drives an electrical generator. Wind turbines are typically installed in sites with high wind speeds because the energy content of the wind is proportional to the cube of wind speed. Wind plants are thus often located in remote locations, and wind turbine generators are on tall towers to displace them from the land surface,[iii] where wind speed is reduced by friction. Monitoring and operations are done from distant central control facilities.

To harden wind systems to different cybersecurity threats, it is important to understand state-of-the-art plant design. Here we focus on large utility-scale, high voltage (HV)-connected wind sites, but similar considerations can be made for interoperable DW systems. A typical wind turbine configuration includes a rotor, consisting of three blades radiating from a central hub, which passes torque through a gearbox into an electric generator, all atop a steel tower. In 2018, the average rotor diameter of newly installed turbines in the United States was 115 meters (m), tower height was over 88 m, and rated power was 2.4 MW.[iv,55] Current market trends are towards turbines with much larger diameters, taller towers, and higher rated power. Because of the physical difficulty, hazards, and expense involved in accessing individual wind generators, hands-on maintenance by technicians is conducted as infrequently as possible. Great effort goes into making each machine self-sufficient and as robust as possible.

Modern wind turbines must respond dynamically to instantaneous wind conditions in their immediate vicinity. The machine aligns itself with the predominant wind direction, sets the speed of rotation to optimize efficiency for the inflow wind speed, and pitches the blades about their long axis to start, stop, and control both speed and power. This control is done mostly in an autonomous mode, utilizing sensors located on the machine itself to

[iii] The *Cybersecurity Roadmap for Wind* focuses primarily on land-based wind energy technologies. Some aspects of offshore wind energy technologies are similar to land-based wind but were not a focus of research for this document.

[iv] According to the *2018 Wind Energy Technologies Report*, wind turbine averages were calculated using data compiled by Berkeley Lab in the U.S. Wind Turbine Database (USWTDB) based on information provided by AWEA, turbine manufacturers, standard turbine specifications, the FAA, web searches, and other sources.

make these operating decisions. Central control of the plants generally provides plant-level setpoints and overarching plant control (such as curtailment levels) while local autonomous control provides dynamic interaction with the wind. Operators at wind energy control centers may also use market, weather, and grid data to monitor and control geographically dispersed plants.

Using information, such as that captured and utilized by wind plant SCADA systems, wind control research has found ways that energy capture can be enhanced, and individual machine loading can be reduced through collaborative control and sharing of information between machines, as well as from sensors located outside the site. For example, wind direction may be poorly described by a measurement on top of a single turbine, but it is more robustly estimated by collective use of many sensors. Likewise, wind measurements outside the plant can be used to anticipate wind direction and speed changes within the plant. The outputs of weather forecasting models have been used to forecast wind plant power output and grid operational needs. These same weather models could be used as additional inputs to enhance wind plant anticipatory control.

The increasing reliance for dynamic operation of the machines on both internal plant data and external weather data, combined with grid requirements, call for greater standardization of wind plant SCADA information. The other driver of standardization is the use of SCADA information within artificial-intelligence and machine-learning algorithms to enable advanced prognostics for operations and maintenance. A wealth of information flows into the central command facility that has been unintelligible to vendors from outside the company. Standardization of the tags and nomenclature for these data would enable third parties to create operational tools of much greater sophistication than could be developed independently within each company.

The movement toward collective control is also necessary for wind plants to provide grid services, driven by commands that originate outside the plant at central control facilities. Standardization will make access to the SCADA system more transparent for everyone. This, of course, has implications on managing the cybersecurity of such control access because the safety of an individual machine could be compromised by an inappropriate external signal if the entire control system is not hardened to such possibilities. A history of autonomous operation followed by a rapid transition to external control creates a risk that cyber attack could significantly damage the plant and the grid.

2.1 Overview of System Boundaries

As wind generation comprises a greater portion of the nation's power supply, it is critical to effectively monitor and control generation. Highly reliable communication infrastructure in wind plants plays a key role in enabling the real-time operation, monitoring, and control of both wind turbines and the electric power grid to ensure grid stability. Wind systems are also capable of providing a range of additional grid services, to include voltage regulation, frequency support, and ancillary services with effective communication and control strategies. To enable this functionality, grid operators communicate to plant controllers, which then communicate commands to each of the wind turbines. The plant controller is connected to grid operators either through dedicated communication lines or public Internet. In either case, effective demilitarized zones (DMZs) should be created that facilitate secure control system data access. Virtual Private Network (VPN) access or firewall rules can be established to allow only authenticated users to send and receive data from the plant controller. These digital perimeter defenses are essential to block adversary action or reconnaissance of the internal wind local area network that runs from the plant controller to each of the wind turbines. A simple representation of this environment and responsible parties is shown in Figure 1. The grid operators (utilities, independent system operators, regional transmission organizations, etc.) connect to the plant controller through the wind plant DMZ firewall. Those commands are then interpreted by one or more human-machine interface (HMI), SCADA, or other servers as configured by the plant owner/operator. These systems relay commands to the individual turbine's controllers. Generally, these local communications are assumed to be secure because

they are isolated from public networks. This assumption means that local communications are subject to attacks like interruption, interception, modification, and fabrication of data-in-transit.

As indicated in Figure 1, multiple hierarchical areas exist in a wind power system network. From right to left, these represent:

- Low-level sensors and actuators working with the physical processes.
- Field devices located at either the wind turbine or plant control center that gather data and send commands. These devices may be programmable logic controllers (PLCs), real-time operating systems (RTOS), field programmable gate arrays (FPGAs), or other single board processors.
- Control centers that aggregate data and can push site wide commands to the wind turbines. Typically, data historians will collect and store SCADA information, as well as HMIs, engineering workstations, and other servers to store and process data, or process external requests (such as those from grid operators).
- A demilitarized zone (DMZ) that includes a firewall that filters external requests and permits VPN connections to the site.
- Other enterprise systems that are connected to the site via public Internet connections.

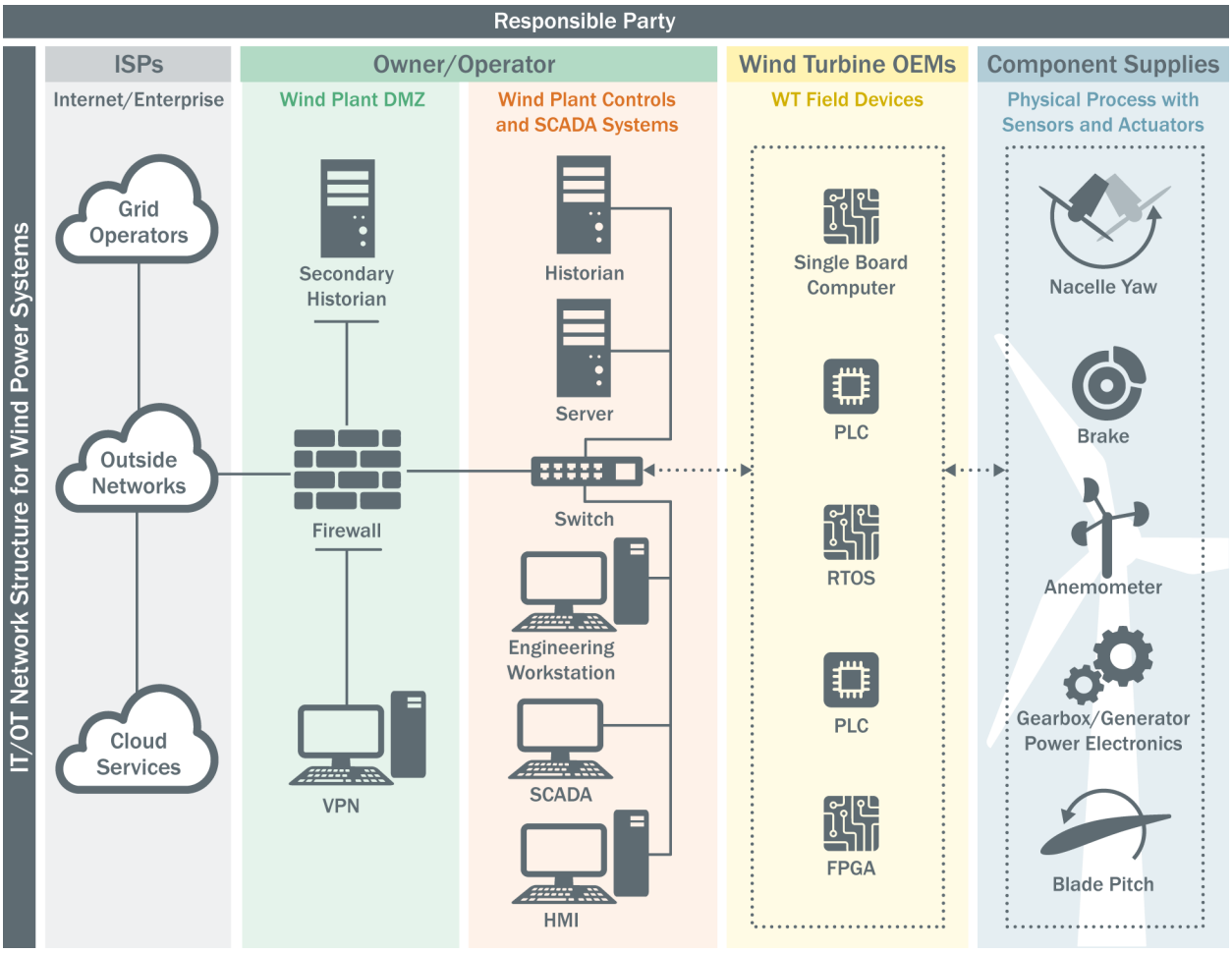

Figure 1. Schematic representation of the IT/OT infrastructure in a wind plant.

2.2 Wind Turbine and Plant Communications

A range of standardized and proprietary communication protocols are used in wind systems.[56,57] The selection of communication protocols depends on installation location, OEM, turbine vendor, and other factors. Generally, a fiber-optic Transmission Control Protocol/Internet Protocol (TCP/IP) network from the plant controller to the base of each tower will exist. A switch located at the base of each tower takes plant-wide control commands and issues them to a local control and measurement (SCADA) unit connected to the actuators and sensors (see Figure 2 and Figure 3). These devices typically include turbine-monitoring and protection equipment (e.g., frequency and voltage monitoring, overspeed protection, fault protection) power-converter controllers, graphical user interfaces, and additional communications systems to meteorological or metrology equipment (see Figure 2).[58] In some cases, another control module—such as a PLC—is in the nacelle and controls the pitch and yaw system, the drive train-, motor-, and pump-condition-monitoring system, other telemetry and drive systems, and specific user interfaces.[59] Fieldbus communications to equipment within the tower and nacelle may include Controller Area Network bus, Ethernet for Control Automation Technology (EtherCAT), Institute of Electrical and Electronics Engineers (IEEE) 960 FASTBUS, MODBUS, Process Field Bus (PROFIBUS), or any number of other protocols. Most of these protocols are designed for fast, lightweight data exchanges that run over wired TCP or serial connections, and do not include authentication, encryption, or other security features. The protocols pass data in clear text and can be easily

manipulated or spoofed.[v] In other cases, it is possible that communications from the base of the tower to the nacelle are enabled by wireless technologies. The security advantage of the wired approach is that physical access to the equipment is required to manipulate control or measurement data.

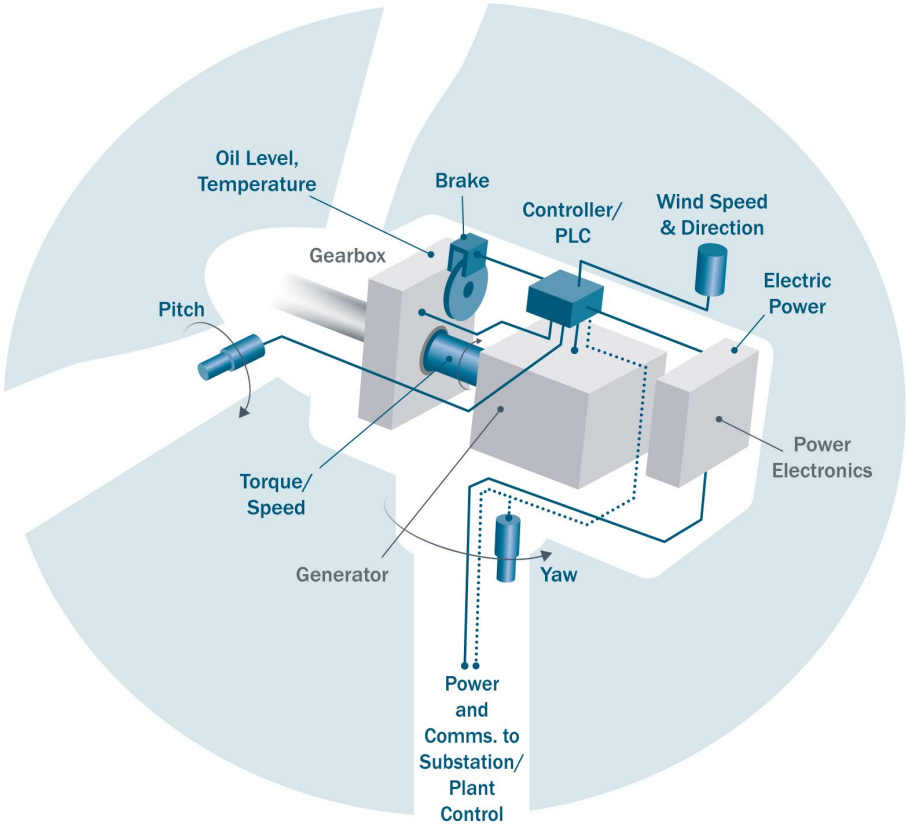

Figure 2. Actuators and sensors in the nacelle of a wind turbine.

A major challenge to the wind cybersecurity community is the lack of standardization in communication protocols, software, and hardware. Because many wind installations are unique, creating secure reference architectures for wind communications is difficult. Figure 3 illustrates an example of a wind plant communication among field equipment, SCADA, the operations center, and transmission control center, but given the variety and variability in available technologies and equipment for wind plant communications, this architecture serves as a generic representation. For example, given the distributed nature of these networks, some plants may require running long copper or fiber-optic lines or creating wireless/cellular communication systems capable of reaching all the equipment. Each method has unique advantages and disadvantages, and each wind plant has different technological requirements. Ultimately, solutions to wind cybersecurity should account for the diversity of implementation approaches. In 2019, WETO began to develop a wind-specific reference architecture, which will result in easier identification of cyber attack surfaces.[60]

[v] Spoofing generally refers to the malicious practice of sending communications from an unknown source disguised as a source known to the communication recipient.

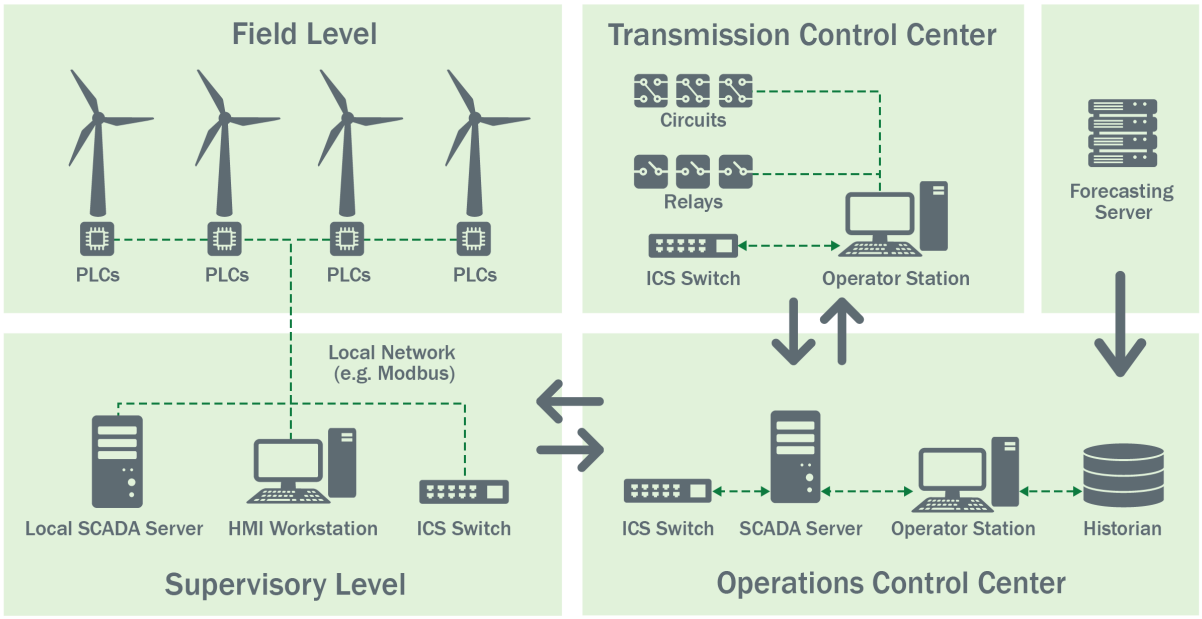

Figure 3. Overview of wind plant communications in which multiple control zones are connected by a wide area network.

3 Wind Cyber Threat Landscape

Individually, wind turbines pose little to no cyber risk to the power system: typically capable of generating a few megawatts at most, the inoperability of a single turbine would likely be inconsequential to a wind plant owner or operator. However, wind turbines do not operate as siloed entities. As smart grid-native generators, wind turbines, plants, and in some cases groups of wind plants are reliant upon digital technologies that enable bidirectional communication, remote control, automation, and monitoring. The convenience and efficiency provided by smart grid technologies also expand the wind cyber threat landscape significantly. The remote accessibility of wind operational technology (OT) for operator, technician, and vendor use may be equally accessible to malicious cyber threat actors. Exploited cyber vulnerabilities in one wind turbine or plant could provide a threat actor with access to broader networks, equipment, and critical functions, possibly enabling an attacker to pivot from a wind facility into the distribution system or the broader bulk electric system, depending on interconnectivity. To prevent such scenarios, research and the development and implementation of cyber-informed design and practices in wind energy should be undertaken directly.

To identify the best paths forward in developing cyber-informed equipment, standards, and practices for wind energy, it is important to understand the wind energy technology cyber threat landscape. The landscape is difficult to define and demarcate for several reasons. Among these are that the type, deployment, and configuration of digital equipment throughout wind plants is varied, particularly in wind plant networks and communications. Further, because of the remote and adverse or harsh environmental conditions in which wind technologies operate, improper operation, abnormal operational activity, and failures may be difficult to identify or attribute to malicious activity. When responding to abnormal or failed wind asset conditions, operators may overlook the possibility that a cyber event could be responsible. Also, by unquestioningly identifying the root cause of a cyber event as non-malicious behavior or by suppressing information about a cyber event, wind energy owners and operators may unintentionally or intentionally stifle awareness about the intent and capabilities demonstrated by cyber threat actors exploring and attacking wind energy technologies. Though large wind installations are subject to regulatory requirements that include reporting cyber events, it is

unclear if and how wind installations currently exempt from regulation report and respond to cyber events. Additionally, much of the OT[vi] commonly used in wind energy is similarly widespread in other critical infrastructure sector facilities, indicating that a vulnerability or threat to OT in one sector or facility may be equally concerning to other sectors and facilities, including wind plants and control centers.

Vulnerabilities, exploitability, and potential grid-scale consequences depend on many factors. These include wind plant configuration (e.g., the number of wind turbines connected to a network and that network's security), device cybersecurity (e.g., inverters, controllers), and physical security (e.g., local control equipment may be easily accessible from public areas) among other elements. The geographically remote nature of wind plants often necessitates Internet-based or -facing wind control applications to enable customers, owners, or operators to access, view, and change operating parameters. Though convenient, the use of Internet-based platforms to control and monitor physical processes may considerably broaden the wind threat landscape. OT, such as industrial control systems (ICS), are essential in modern wind plants and control centers and may include Internet-facing features. The web-enabled accessibility of OT has generated new possibilities to remotely manipulate or disrupt real-world processes, such as the operation of a wind turbine or a wind plant's interconnection to a power grid. Established cyber vulnerabilities, threats, and events involving the exploitation of wind energy OT are discussed further below.

3.1 Established Vulnerabilities

Several vulnerabilities affecting critical components of wind turbines and plants have been identified in academic research or "in the wild"[vii] by cybersecurity researchers. Such research is conducted to illuminate and address vulnerabilities in wind energy software and equipment. Affected vendors often respond to such research quickly with patches and updates, but prominent interest in wind vulnerabilities suggests that malicious cyber-actors may be similarly interested in wind technology.

In 2018, researchers from Washington State University and Virginia Polytechnic Institute published a paper demonstrating scenarios in which a cyber attack targeted a wind plant SCADA system. By compromising the SCADA system, researchers illustrated how a malicious actor could gain unauthorized control of a wind plant, send false commands to target components, and stop or potentially damage wind turbines. If successful, the cyber attack could lead to system instability or a cascading outage, depending on wind plant interconnectivity.[61] The researchers noted that access to the SCADA system could be achieved by physical access to a wind plant local area network (LAN) via a local control panel or remotely via an external network.[62] Although accessing a wind plant LAN via an external network is likely more challenging than physically accessing a geographically remote control panel, an attacker may be able to bypass firewalls between Internet-facing business networks and wind plant control or operational networks if firewalls and network communications are poorly configured.

Similarly in 2017, researchers from the University of Tulsa described combined cyber and physical attack scenarios focused on wind turbine control, turbine damage, wind plant disruption and damage, and substation disruption and damage.[63] Using custom-built tools, the researchers demonstrated the ease with which an attacker could fabricate and replicate turbine control messages; use a worm to propagate malicious, detrimental commands within a turbine or throughout a wind plant network; or exploit flat wind plant network topology

[vi] OT refers to the hardware and software that effects and detects changes to operating conditions of real-world, physical processes via the direct monitoring and control of devices, processes, and events in an operational environment.

[vii] Software deployed "in the wild" has already passed through a development environment to become a publicly used and available tool. Once software is in the wild, it may be used or manipulated in a way not intended or anticipated by the original developers.

"to block, modify and fabricate control messages at will." The vulnerabilities exploited by the researchers were all related to the lateral, unsecured implementation of control devices and communications across wind plants, lack of network segmentation, and lack of encryption for wind plant communications—all commonly observed characteristics of wind plants.

In 2015, a cyber-researcher identified vulnerabilities in two wind turbine systems. The XZERES 442SR Wind Turbine uses a web-based interface and was found to be vulnerable to a cross-site request forgery that allowed the default user password to be retrieved and changed, thus allowing administrative rights to the entire system.[64] The exploit can cause a loss of power for all attached systems.[65] The German company RLE that produced the NovaWind Turbine was found to have an HMI vulnerability in which credentials listed in plain text could be used to gain unauthorized remote access to the device, allowing an attacker to change or modify all configurations and settings.[66]

In 2011, researchers from Iowa State University and the Virginia Polytechnic Institute demonstrated how several vulnerabilities in the SCADA systems of 2-MW wind turbines could be exploited to cause "major problems within a power system, including economy loss, overspeed of a wind turbine, and equipment damage."[67] The attack scenarios included:

- Physically accessing the local control panel on a wind turbine
- Injecting the turbine's controls with malicious code
- Installing surreptitious taps on fiber cables connected to wind turbines to pass false measurement data between turbines and the SCADA system using a man-in-the-middle (MiTM) attack
- Facilitating an accidental insider attack by dropping a Universal Serial Bus (USB) stick with malicious code, where a wind plant operator might find it and, out of curiosity, plug it in to a network computer.[68]

Patches and updates addressing vulnerabilities are usually issued quickly by respective vendors, yet the resolution of a vulnerability occurs only when patches and updates are applied. Unlike IT systems, OT involves automation of physical processes: OT systems require planned, scheduled maintenance, which cannot be momentarily interrupted to install updates. Unless updates are automatically pushed by a vendor, devices and systems could remain vulnerable to exploitation until the next scheduled shutdown—potentially months after a vulnerability is discovered.

3.2 Established Threat Actors

A malicious threat actor may demonstrate intent, capability, and/or opportunity to adversely impact a digital asset or system. Threat actors may employ sophisticated tactics, techniques, and procedures to plan, prepare, access, and execute intrusions or attacks, yet much of the information required to cause an adverse cyber event may be found via open-source publicly available resources. Tools, such as the ICS search engine SHODAN,[69] enable users to browse and discover Internet-connected equipment and software using search terms such as "wind," "turbine," or a specific device brand or model name. This indicates that even small groups or individuals may be able to achieve significant negative impacts in wind environments via cyber-means.

Wind energy technologies have attracted the attention of nation state level cyber threat actors, particularly those judged to be the most capable and active by the U.S. Intelligence Community.[70] In addition, Russia, China, and Iran are considered aggressive in collecting sensitive information about and exploiting critical U.S. technologies, among which wind turbines are judged to be of high interest.[71] A number of nation-state-sponsored advanced persistent threat (APT) groups have been identified as having targeted alternative energy, including wind energy, at least once.[72] All identified APTs may not be solely or directly targeting wind energy

technology, yet the number of well-resourced, capable, and sophisticated threat actors interested in alternative-energy sources indicates that the wind industry must also contend with serious cyber threats.

Opportunistic individuals and small groups, rather than nation-state actors, may also pose a serious threat to wind assets. In November 2015, a user on a Russian cybercrime forum posted a screenshot of the remote-access web-management interface for a GE 1.6-MW wind turbine.[viii] The actions available from the interface included tools to operate, maintain, and change settings of the turbine.[73] The user likely found information about the turbine's location, web-based control interface, and access credential information via the Internet using basic open-source search techniques. Irrespective of origin, this information would likely serve beneficial to nation state and unaffiliated actors alike.

3.3 Established Cyber Events

Incidents targeting wind energy systems have already occurred and will likely continue to increase in sophistication and number. Cyber events may emerge from intentional or unintentional circumstances. The occurrence of an unintentional or accidental cyber event indicates that similar or greater effects may be achieved via intentional, malicious cyber-means. One such event called the "first-of-its-kind" and the first cyber incident publicly known to directly affect a renewable energy source involved wind installations. In March 2019, the attempted exploitation of a vulnerability within a firewall resulted in a denial-of-service (DoS) condition, disrupting communications between a control center and wind and solar generation sites for a large, Utah-based wind owner/operator.[74] Post-event analysis revealed that a vulnerability in the web interface of a vendor's firewall was exploited, allowing the attacker to trigger unexpected reboots of the devices. This produced the DoS at the control center and resulted in short communication outages (less than five minutes) between field devices and the control center.[75] The incident did not affect generation at the wind and solar sites, but caused a loss of system integrity that was later resolved via a review of logs by the affected equipment vendor, and subsequent provisioning and application of a software patch to address the known vulnerability.[76]

During a cybersecurity presentation at the 2018 American Wind Energy Association (AWEA) Conference, a technical expert illustrated how an unintentional cyber event impacted an unnamed wind plant:

> In one incident, a technician logged on to his laptop in a hotel and downloaded malware by mistake. When he went to work the next day and logged on, the wind plant became infected and the turbines stopped working one by one.[77]

The malware downloaded and transmitted to the wind plant network may not have been designed to intentionally compromise wind networks, yet the introduction of IT-centric malware into OT environments can disrupt or halt wind plant operations by slowing down, impeding, or muddling process communications.

In 2018, Dragos founder Robert M. Lee discussed a cyber incident response engagement Dragos conducted at an undisclosed wind plant with the host of a cybercrime-focused podcast. According to Lee, the wind plant operator noticed abnormal behavior on the wind plant network, though turbine operations were unaffected. The operator reported that approximately a dozen workstations, each controlling and monitoring a turbine, were infected with malware and that the wind network was patching[ix] continuously exclusive of approved IT or OT

[viii] The forum and discussion thread indicated were retrieved from Russian cyber-crime website exploit.in by C. Glenn in March 2016. The origin URL has been withheld to prevent access to a malicious website.

[ix] Patching refers to the application of changes to software or firmware, usually to address or resolve flaws, vulnerabilities, or to improve performance.

personnel activity. Dragos discovered that the malware was an early form of cryptojacking[x] software that was exploiting the wind turbine workstations' extra processing power to mine cryptocurrency.[78] Dragos determined that the malware was slowing down the wind network, but not enough to directly impact the turbine control and monitoring functions enabled by the workstations.[79] Although the subject wind plant's operations were not affected by the malware in this incident, if allowed to persist or propagate in an OT environment or throughout a larger wind plant network, malware could interfere with physical processes by slowing, disrupting, or distorting control and monitoring.

An adverse cyber event disclosed in 2018 involving wind energy did not have effects on the surrounding power system, yet the incident demonstrated a threat actor's capability to remotely access and manipulate wind turbines.

> A wind power generator fell into Russia-linked hackers' crosshairs last year, but the attackers never managed to put the wider U.S. grid at risk, officials confirmed yesterday at a Department of Homeland Security cybersecurity conference…utility [Southern Company] said the hackers' reach appears to have been "very limited" — perhaps just 'one or two wind turbines' at an undisclosed power company.[80]

The wind facility was one of numerous U.S. generation assets targeted by Russian cyber threat actors.[81] Further, BlackEnergy2, a predecessor of the BlackEnergy3 malware employed in the 2015 cyber attack on the Ukrainian power system, is associated with Russian actors and is known to have targeted wind cyber assets as early as 2014.[82]

In 2014, partial details regarding a cyber event involving a utility-managed wind plant were released publicly:

> In the summer of 2014, a hacker of unknown origin, using masking software called Tor, took over the controls of a large utility's wind plant, according to a former industry compliance official who reviewed a report that was scrubbed of the utility's name. The hacker then changed an important setting, called the automatic voltage regulator, from "automatic" to "manual," he said.[83]

The incident demonstrated the impact of malicious access to wind control. Wind turbines grouped together as a plant usually operate as a single installation, all connected to the same control systems. This allows synchronous changes and monitoring to occur. However, if the installation is identically configured, manipulating the controls could negatively impact stable power generation.

3.4 Unique Consequences of Adversary-Controlled Wind Systems

Wind energy systems have some unique characteristics when compared to other energy-generation technologies that should be considered in the context of potential cybersecurity consequences. The most distinguishing characteristic of wind systems is the sizeable rotational kinetic energy of the rotor that forms the basis of its operation. With the largest rotor diameters now exceeding 220 m, with tip heights reaching 260 m above the ground,[84] this represents a visible, large, spinning mass that could cause significant permanent damage to the machine and risk to the surrounding area from flying debris in the most catastrophic cases. Historically, turbines are installed in remote locations without a physical operator, so there is limited direct risk to personnel or the public; however, more-recent market trends suggest future wind turbines will be installed closer to population centers,[85,86] which will increase risk. Absent any direct injuries, the visible and sometimes

[x] Cryptojacking is the use of malware to seize control or hijack a part or all of computers' processing power to mine cryptocurrency.

dramatic nature of catastrophic turbine failures could erode public confidence in the safety and reliability of the systems and broadly hinder further deployment of systems—even if gaps in physical and cybersecurity are patched. Beyond these characteristics, many of the potential consequences of compromised wind systems are similar to other energy-generation methods and include consequences such as those listed in Table 3.

Table 3. Unique Consequences of Adversary-Controlled Wind Systems.

Wind turbine generator (WTG) manipulation	WTG controls manipulated to reduce output power.
	WTG controls manipulated to increase output power.
	WTG controls manipulated to continuously or harmonically adjust power output.
	WTG controls manipulated to cause physical damage to turbine or connected equipment.
Communication infrastructure distortion	Impacts to normal operation of turbines, hindrance to grid stability, and scalability of access restriction to control centers of wind plants can all be affected by disruption of wired, wireless, and cellular communications. Communications that could be distorted, interrupted, or blocked include those between turbines and a control center and those between a wind plant network and remote-control center (potentially over Wide Area Network [WAN]).
Data falsification leading to miscoordination	Falsified field measurements feeding monitoring and control applications can lead to autonomous or human-in-the-loop operational mistakes that would affect the grid negatively. Systems that could be distorted include condition-monitoring systems, structure health-monitoring systems (SHMs), SCADA units, and remote monitoring and secure access.
Internal turbine communication	Widely adapted protocol, EtherCAT (the most widely used protocol standardized in International Electrotechnical Commission (IEC) 61158), based on traditional MAC/PHY layers, is subject to attacks like MAC spoofing.
	Wireless communication used in turbines for sending and receiving information from base to nacelle or from base to remote SCADA client is subject to denial-of-service (DoS) attacks, among others.
	Fiber optics enable long distance and fast communication, but information can be leaked or altered.
Bidirectional communication between turbine and control center	The most common wind plant networks consist of a switch in the turbine, either managed or unmanaged, and a central switch connected to all turbine switches. Brute-force attacks on one industrial Ethernet switch can potentially disrupt communications for the whole farm and potentially affect the grid at interconnection.

Traditional OT IEEE 1815 protocol (DNP3), used in bidirectional communications by SCADA applications, rarely employs many of the optional available security features. Therefore, it is subject to attacks like interruption, interception, modification, and fabrication of data in transit.

Unlike other forms of electricity generation, wind plants are usually composed of many individual generation sources: wind turbines. Wind plants often feature the same equipment and equipment configurations deployed throughout the site, or multiple sites including field devices (PLCs, RTUs, HMIs), engineering workstations

and operating systems, and networking equipment. This means that, if an exploitable vulnerability is discovered affecting a device used in a wind turbine or wind plant network, it is possible that an entire plant, SCADA network, and control network could be similarly exploited with greater ease than a site employing greater device variety and device configuration. The regular lateral application of technology in wind plants suggests that the exploitability of and impact to wind energy facilities by an adverse cyber incident could have disproportionately greater effects than to other forms of electricity generation.

4 Wind Cybersecurity R&D

It is critical to develop innovative technologies to thwart malicious cyber-actors. This section discusses some of the promising cybersecurity R&D topics that could be applied to wind power systems. The research areas are broken into topic areas that represent the five NIST areas in the Framework for Improving Critical Infrastructure Cybersecurity: Identify, Protect, Detect, Respond, and Recover. Many are crosscutting and could fit into multiple areas. Much of this discussion leverages prior work identifying R&D topics for solar cybersecurity R&D.[87] Topics for each of the NIST areas are shown in Figure 4.

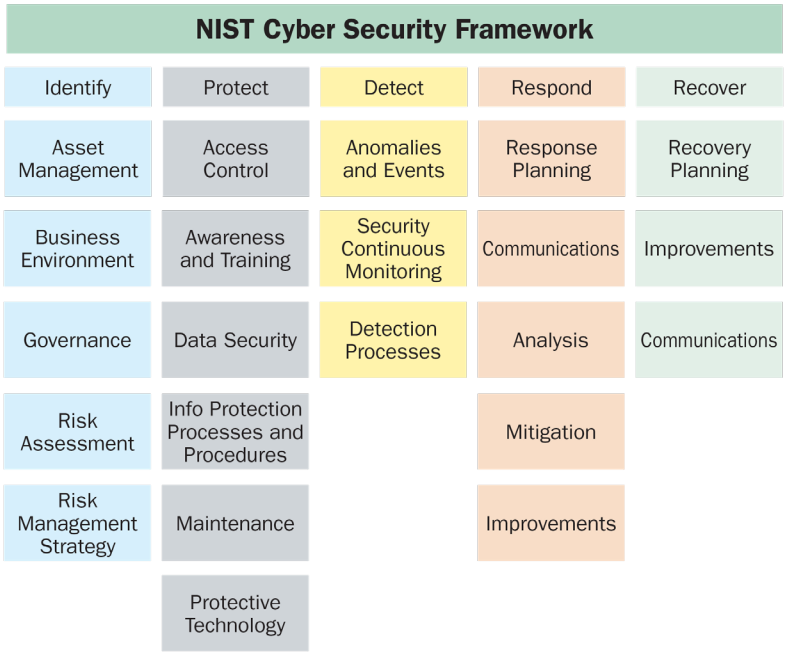

Figure 4. NIST Cybersecurity Framework.

R&D topics can also be associated with one or more locations in the communication network, as shown in Figure 5. In each of these areas, there is a separate responsible party. At the lowest level, component suppliers are responsible for cybersecurity capabilities. At the turbine level, turbine OEMs ultimately maintain responsibility for the security of the system. The owner/operators of the wind site are responsible for securing the demilitarized zone (DMZ) and control/SCADA centers. Last, Internet service providers have responsibility to secure, to some degree, the public Internet (though this is largely unmonitored and unregulated to provide the greatest Internet speeds for customers). On the right in Figure 5, R&D for each of the NIST Framework Areas are mapped to the tiers of the communication network. For instance, physical security is required at the wind turbine generator, SCADA systems, and DMZ. Due to this separation of responsibilities, cross-organizational collaboration will be essential to successfully identify and implement cybersecurity measures.

Also indicated in Figure 5, multiple general areas are in the network representing:

- Low-level sensors and actuators working with the physical processes.
- Field devices located at either the wind turbine or plant control center that gather data and send commands. These devices may be programmable logic controllers, real-time operating systems, field programmable gate arrays, or other single board processors.
- Control centers that aggregate data and can push site-wide commands to the wind turbines. Typically, historians will collect and store SCADA information, as well as HMIs, engineering workstations, and other servers to store and process data or process external requests (e.g., from grid operators).
- A DMZ that includes a firewall that filters external requests and permits VPN connections to the site.
- Other enterprise systems that are connected to the site through public Internet connections.

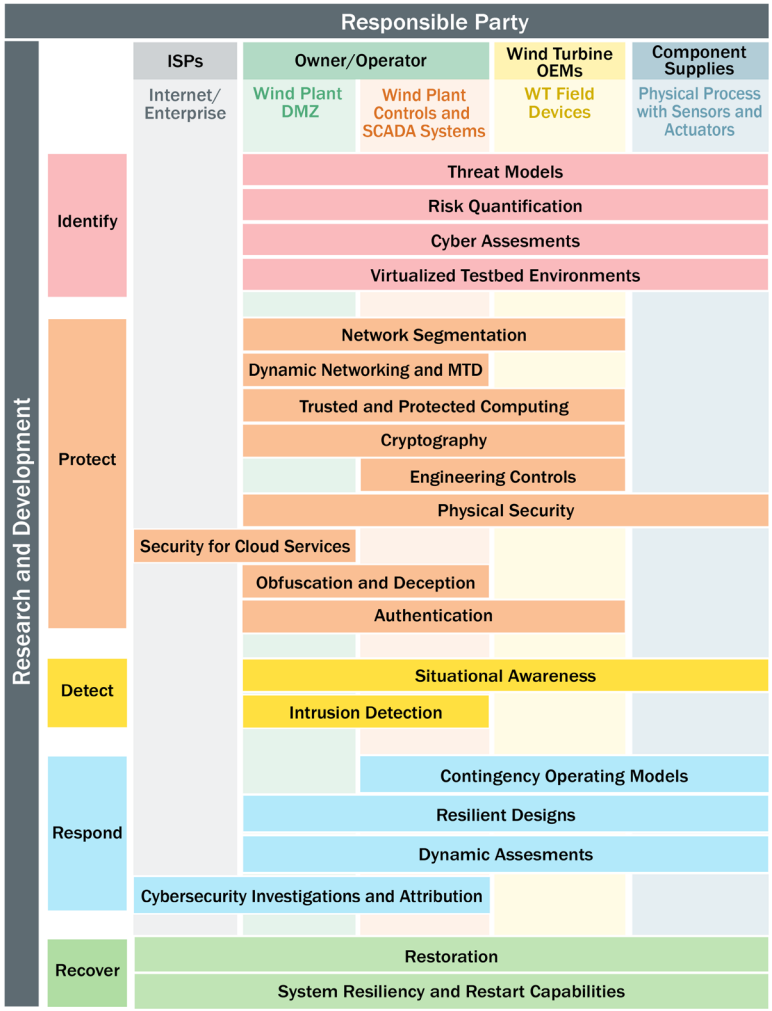

Figure 5. Notional wind power plant networking tiers and devices with the responsible parties and R&D components for each broken down based on the NIST Cybersecurity Framework.

4.1 Identify

It is essential to identify and document network components and critical assets to reduce the attack surface and potential cyber-attack impacts for wind cyber-systems. Certain tools can be used to help identify problems before an attack occurs, while others are updated after an attack has taken place. This section discusses many types of tools that may lead to a better protected environment. Critical wind assets (i.e., those that are either high priority/visibility or those that are deemed more vulnerable to cyber attack) could be identified using these tools.

4.1.1 Evaluate Potential High-Consequence Cyber Events

Certain attack scenarios may be relatively benign, whereas others could be catastrophic. Establishing methods and tools for calculating risk from different vulnerabilities, attack vectors, credible threat data, and associated targets helps prioritize security improvements. NIST SP 800-39 describes the four stages in the process as framing risk, assessing risk, responding to risk, and monitoring risk, but this is tailored to IT networks. McAfee offers an Operational Technology Risk Assessment course tailored to look across ICS plants' people, processes, and technologies for risk, vulnerabilities, and mitigations. Similarly, UK-based company BAE Systems offers consulting services to assess, design, and manage cyber-solutions through awareness trainings, penetration testing, risk management, etc. Sandia National Laboratories (Sandia) developed a modern approach for risk quantification called Risk-Informed Management of Enterprise Security, which weighs consequence and scenario difficulty to determine the risk of given scenarios. Each of these methods should be investigated for application to the wind industry.

Wind power plants feature a variety of control equipment using any of several different protocols. It is important to understand the interdependencies of these devices and their extent on operations. Failure in wind turbine control operation can result in death, fatal injuries, equipment loss, grid instability, and loss of reputation. A study focused on specific high-consequence events needs to be considered to build stakeholder buy-in as it informs the range of impacts from a cyber attack.

4.1.2 Threat Models

Threat actors exploit vulnerabilities to obtain information, damage, or otherwise manipulate assets. Understanding threats is necessary to successfully defend against attacks. Threat modeling identifies high-value assets, attack vectors, and vulnerabilities to determine credible threats. Systematically identifying and enumerating the threats to plant and turbine communication systems will help direct the design of appropriate security features for utility, aggregator, and networking equipment.

Vulnerabilities must be discovered, classified, and enumerated as part of the threat modeling process. As an example, in 2011, Idaho National Laboratory (INL) reported anonymized energy delivery control systems vulnerabilities discovered over 7 years as part of a DOE-OE-funded National SCADA Test Bed program. INL quantified the most common vulnerabilities and the risks to prioritize decisions made to minimize risk and defend against system threats. Multiple standardized approaches exist for threat modeling. Microsoft's STRIDE, though developed primarily for IT environments, is an example threat model methodology that could be applied to wind systems. STRIDE stands for the six threat categories:

- Spoofing of user identity
- Tampering
- Repudiation
- Information disclosure
- Denial of Service (DoS)
- Elevation of privilege.

Completing wind energy threat modeling and vulnerability assessments is a prerequisite for wind systems to create realistic threat models—these models should be designed with OT environments primarily in mind. In the meantime, cyber threat and vulnerability information sharing will be emphasized to help plant owners and operators recognize and utilize shared information. Ideally, this information sharing would be followed by sharing mitigation strategies regarding potential threat events against wind systems or known vulnerabilities. These near- to mid-term milestones involving information sharing are critical to enhance the wind cyber-culture that emphasizes information sharing—of cyber threats and vulnerabilities, lessons learned, and collaborative efforts—among the wind energy community.

Long-term, the establishment and continued maintenance of wind energy testbeds can also assist plant owners and operators with identifying evolving cyber threats and vulnerabilities to wind energy technologies. These testbeds, covered more in section 4.1.6 below, can certainly help the advancement of information sharing as they become another mechanism from which cybersecurity alerts, as well as threat and vulnerability information, can be distributed to owners and operators.

4.1.3 Cyber Assessments

Good offense can sometimes lead to better defense. In a Trend Micro survey of 250 SCADA vulnerabilities, most issues were found to be related to memory corruption,[xi] poor credential management,[xii] code injection bugs,[xiii] lack of authentication or authorization,[xiv] and insecure defaults.[xv,88] By performing cybersecurity assessments—inspecting and evaluating wind equipment, communication modules, and networks—in the pre-production or commissioning process, the discovery of many vulnerabilities can be made. Currently, it is unclear how many United States wind facilities have conducted or regularly conduct cyber assessments of wind assets and what assessment strategies are used. Cyber assessments should follow standardized methodologies provided by NIST SP 800-82, ICS-CERT Cyber Security Evaluation Tool, or custom assessment techniques like the Information Design Assurance Red Team (IDART™) methodology that consists of multiple attack vectors, including DoS, packet replay, man-in-the middle (MiTM) attacks, vulnerabilities scans, and modified firmware uploads, along with inspection of password handling and log management. Additionally, as mentioned in Section 2.2.1 DOE's CyTRICS™ program identifies cyber-vulnerabilities and threats by inventorying and testing critical energy sector ICS components and then conducting an analysis, which correlates threat information and supply chain information and other relevant data and sources. When third parties discover vulnerabilities, the information should be provided to the vendor and shared with the appropriate response organizations, such as ICS-CERT, E-ISAC, or other ISACs. It should be noted that wind system vulnerabilities have been discovered in the past using these approaches.[89,90] Sharing known vulnerabilities between communities is essential to maintaining up-to-date protection systems.

Cybersecurity assessments form a strong measure of a plant's cyber maturity. Assessments help identify specific controls that may be missing for safe operation of a wind power plant. The formation and distribution of cyber-focused workshops and trainings would help benefit cybersecurity assessments. Through enhanced

---

[xi] Memory corruption occurs when the content location of a computer program's memory is modified, usually due to a programming error, causing the program to crash or execute code not intended to run in the program.

[xii] Poor credential management refers to the poor, untimely, or weak administration of a credential management system. If access credentials and roles are not regularly maintained, sensitive information and systems may be at greater risk to unauthorized or malicious access.

[xiii] A code injection bug is a flaw in a computer program that allows the injection of computer code that is subsequently executed by the program. A code injection may, for example, allow access to access credential, sensitive information, or the propagation of malware.

[xiv] A lack of authentication or authorization includes, for example, allowing weak passwords, lacking access control to systems (no password protection), no requirement for re-authentication within sensitive systems, and lacking role separation for system access (i.e., all users designated with a role may access a system based on their role rather than individual authorized access.)

[xv] Insecure defaults refer to the insufficient or lack of security of a default system configuration. Related to a lack of authentication or authorization, insecure defaults include requiring no password for access system, all network ports being open, or allowing all users an administrator role.

awareness, plant owners and operators can learn and apply different behaviors and security approaches regarding, for example, cyber assessments of their plant(s). Long-term, more effective, methodological processes for conducting cybersecurity assessments may also help owners and operators better evaluate and document assessments for their wind energy systems.

Complementary to cybersecurity assessments, in-depth cyber-informed engineering principles can be applied to new and currently operating wind facilities. INL's Cyber-informed Engineering (CIE) and Consequence-driven Cyber-informed Engineering (CCE) processes guide asset owners in the implementation of system and procedural modifications to diminish or eliminate the potential impact of cyber attacks. The implementation of routine cyber assessments for the wind energy sector is a recommended best practice.

4.1.4 Cyber-Informed Engineering

Cybersecurity strategies often focus on reducing risk by improving cyber hygiene, but the dynamic nature of the problem challenges this approach. Cyber-informed Engineering (CIE)[91] is a body of knowledge and methodologies that bridge the gap between engineering design and cybersecurity. CIE represents one way to improve confidence in the resilience of critical systems by identifying the elements of a wind plant that must not fail (e.g., critical functions, protections, alarms) and then engineer controls that cannot be co-opted by a malicious actor. The CIE method characterizes risk and offers a strategy to apply engineering processes to mitigate these risks. This concept impacts many aspects of a wind plant, including design, procurement, and updates.

Many industrial control systems (ICSs) allow status and control of remote equipment to be easily obtained using digital interfaces. By design, many of these systems rely on a "trust" relationship that assumes the separation of control layers and the successful warding of cyber attackers. For example, if a wind turbine component receives a query or a command in the proper format, then the equipment will act upon (i.e., trust) the request. However, the request may not have originated from the HMI/engineering workstation that the component was designed to serve. Attackers co-adapt to the protections and engineering controls of an ICS such that the requests they issue to the ICS equipment appear authenticated. The CIE methodology would seek engineering controls that would eliminate the trust assumption, in this example, to mitigate the risk of a malicious request. INL published a CIE-based application and assessment aid[92] that includes a checklist, questionnaire, and an assessment methodology that invite cyber-risks to be considered throughout the wind plant life cycle.

4.1.5 Consequence-Driven Cyber-Informed Engineering

An extension to CIE, Consequence-driven Cyber-informed Engineering (CCE) provides organizations with a method to examine their own operational environments for high-impact events/risks; identify key devices and components that facilitate business priorities; illuminate specific, plausible cyber attack paths to manipulate these devices; and develop concrete mitigations, protections, and tripwires to address the high-consequence risk. CCE starts with an assumption markedly different from other security frameworks: that a well-resourced, determined adversary will succeed in gaining access to and manipulating control systems that support operations. CCE identifies the most valuable processes and most vulnerable elements (remote control and operation, supply chain, etc.) and delivers specific remediation recommendations to help asset owners "engineer-out" the cyber risk pathways available to adversaries. The activities of CCE occur throughout four phases: Phase I, Consequence Prioritization; Phase II, System of Systems Breakdown; Phase III, Consequence-based Targeting; and Phase IV, the development of Mitigations and Protections.

To begin, in Phase I, Consequence Prioritization, wind organizations define the most critical functions and services that allow them to accomplish their individual missions. Using CCE to distill High Consequence Events promotes a progressive risk management approach that integrates into existing cyber hygiene strategies

and escalates it by introducing engineering-based preventative measures. In Phase II, System of Systems Analysis, a wind owner evaluates their own infrastructure and operational processes to identify the critical systems, digital devices and components that impact the previously identified critical functions and services. Beyond the individual systems that support a critical function or service, the wind owner should be aware of any key information exchanges between these systems, the loss of or compromise of which could result in an operational failure.

Phase III, Consequence-based Targeting, uses an adversarial approach to identify how a malicious actor can target, disrupt, or destroy a system. To expend resources efficiently, this process involves an assessment of cyber adversaries' capabilities and methods. The operating question in Phase III is: in what ways can an adversary achieve a desired negative impact via cyber-means? If the adversary's attack is possible, then the next step is to map that attack, typically against a kill chain. A kill chain is a high-level model that describes the necessary steps required for adversary success. By mapping to a kill chain, organizations can identify weaknesses in the adversary approach that can be translated to active and disruptive cyber defenses. The goal of Phase IV, Mitigations and Protections, is to strategically improve the security posture of an entity by introducing technological, procedural, and operational changes that eliminate some cyber-attack impacts. Based on the work conducted in the other CCE phases, the wind owner can better understand the goals, capabilities, and progress of a cyber-adversary. Resiliency is bolstered by CCE approaches and periodic re-evaluations.

4.1.6 Virtualized Testbed Environments

The construction of virtualized testbeds is useful across all the R&D areas as they can be used to analyze, evaluate, and demonstrate cybersecurity resilience. These testbeds are used to develop preventative and protective measures, analytic tools, and security strategies. By virtualizing the network, devices, and power system, it is possible to quickly assess different cybersecurity approaches and compliance to standards or guides.

More specifically, research teams can replicate network topologies and generate alternative cyber-secure architectures by building co-simulation emulation platforms (e.g., Sandia's SCEPTRE environment and the Automated Vulnerability Assessment environment of INL, et al.) to create realistic wind/Distributed Energy Resource (DER) control network topologies with protocol exchanges between utilities, aggregators, and wind/DER. Emulation environments can be coupled to power simulations (Open decision support system [OpenDSS], PowerWorld, pypower, etc.) to realistically populate device (SCADA and wind/DER RTU) data fields and to demonstrate impacts on the power system when adversary actions are taken in the communication domain.

The National Renewable Energy Laboratory's (NREL) early research-based co-simulated virtualization and visualization platform (see Figure 6) utilizes Sandia's SCEPTRE, minimega,[93] and many other developing open source technologies to create potential control network topologies with protocol exchanges between power system devices. The platform attempts to emulate representative scenarios and allows users to introduce potential cyber attack vectors. The platform's visualization capability also aims to provide a view of cyber attack consequences.

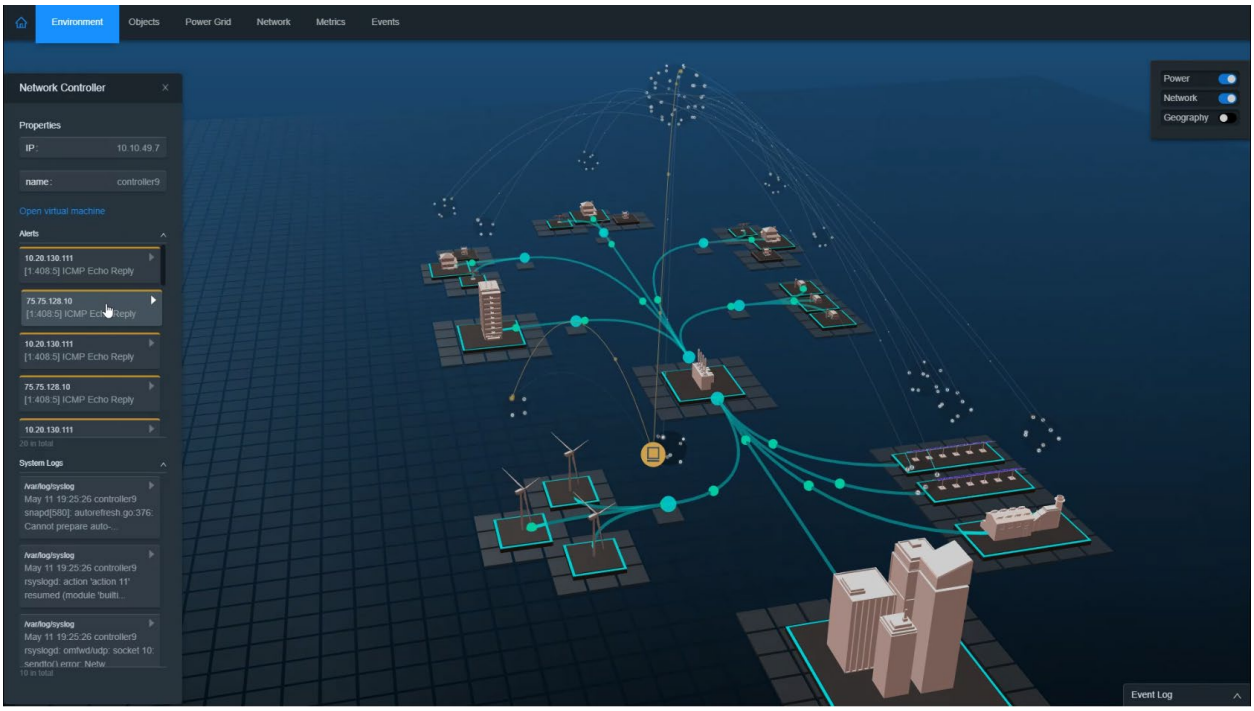

Figure 6. NREL's co-simulation virtualization and visualization platform utilizing Sandia's SCEPTRE, minimega, and open- source technologies to create realistic control network topologies with protocol exchanges between power-system devices.

With these research platforms, wind-specific cyber attacks can be analyzed using threat actors (red teams) and wind system operators (blue teams) to determine the effectiveness of cybersecurity countermeasures. Hardware-in-the-loop technologies can further represent how physical devices will behave in networked or power system attack scenarios. This will be particularly useful as working groups, standards development organizations, and research programs generate new recommendations. Realistic attacks on emulated communication networks can determine risk under different conditions when the network is constructed using various strategies, such as:

- Interoperability protocols and communication protocols (IEEE 2030.5, IEC 61850, SunSpec Modbus)
- Network topologies (e.g., utility-to-wind plant, utility-to-aggregator-to-wind plant)
- Encryption schemes (symmetric, asymmetric), key management, and key sizes
- Firewall rules and role-based access-control lists
- Firmware update/patch levels
- Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs)
- Novel research concepts.

Long-term, the maintenance of these established testbeds can help plant owners and operators recognize cyber threats and vulnerabilities to wind energy technologies. Related, these testbeds will be invaluable regarding the

research, analysis, and validation of cybersecurity resilience efforts and applications—including the pinpointing of attack vectors that could set the stage for a threat event against wind systems.

4.2 Protect

After identifying attack vectors, the next steps are to create cyber-safeguards to protect against these attacks. These can be as simple as network segmentation, secure remote access, access control protocols at all points of connection in the wind system, and warning signs near access points to deter individuals from malicious activity. Prioritizing the implementation of these cyber-safeguards would help the wind energy community minimize risk to their wind energy systems. In addition to these safeguards, several advanced protection methods, or perimeter defense techniques (e.g., firewall whitelisting/blacklisting, proxies, VPNs, inter alia), are discussed in the following sections. Additional approaches for preventing unauthorized network access are also discussed below.

4.2.1 Network Segmentation

Network segmentation is a technique to minimize common-mode vulnerabilities. Network enclaves are created with firewall rules, VPNs, proxies, or other networking technologies so that traffic between them is only allowed by exception. Extensive research on segmentation for military microgrids has been completed previously. The downside of this approach is that additional network administration and network latency is required, something the wind industry may oppose.

4.2.2 Dynamic Networking and Moving-Target Defense

Moving-target defense (MTD) is built on software-defined networking to secure control networks against cyber attacks by rotating network addresses, network parameters, application libraries, or applying other cryptographic tools. This approach is particularly effective against adversaries that rely on known static addresses for critical infrastructure devices. The CEDS-funded Artificial Diversity and Defense Security (ADDSec) project is currently investigating this topic; the team aims to detect threats through machine learning algorithms and then respond to those threats.

4.2.3 Trusted and Protected Computing

The Trusted Computing Group created a suite of standards for endpoint compliance assessment, network access control, and security automation. Many products include tamperproof Trusted Platform Module integrated circuits, designed to secure private keys and function alongside the main processor for cryptographic operations. The Trusted Computing Group also released the Trusted Network Connect protocol, which interrogated endpoint devices to determine their integrity and compliance with security policies. This allows system operators control over what software runs on the target device by authorizing network clients based on hardware configuration, BIOS, kernel version, operating system, software version, etc. The remote attestation feature allows system operators to query a cryptographic hash of a target device to certify the equipment. When there is a change to the software on the system, a new hash is generated.

Application of sandboxes and the principle of least privilege[xvi] access controls could also be employed in wind control equipment. The sandboxing technique isolates the execution of programs or code so that vulnerabilities are not able to spread. Anti-tamper techniques that determine whether software has been modified should also be used widely; some forms of this technology are encryption, checksums, software watermarking, code

[xvi] Least privilege is a basic information security principle that equipment, programs, and personnel should only be granted the minimum amount of access to information and resources as is necessary to perform their function. This limits the ability to inadvertently or malicious use access permissions in unwanted ways.

obfuscation, anti-debugging, and anti-emulation. Another method, called protected computing, requires two processors: one trusted and one untrusted. The public is not allowed to access the protected processor, but the application code is divided between the two processors in a mutually dependent way such that tampering and inconsistencies are detected.

4.2.4 Cryptography

Certain communication protocols require public-key infrastructure to encrypt transmissions and maintain data confidentiality. Unfortunately, no policies exist for exchanging keys for wind systems. Experience[xvii] from independent system operator/regional transmission operator/utility SCADA and solar/DER cryptography should be leveraged to ensure a smooth rollout of these new requirements for wind.

Extensive research on traditional and quantum cryptography, and quantum key distribution exists. This includes exploration of: (a) practical encryption options for wind turbines; (b) appropriate selection of elliptic curves; (c) industry guides for microprocessor selection; and (d) experimental determination of required key exchange times and encryption/decryption times for wind turbine device communications.

4.2.5 Physical Security

Wind plants are often located on leased land that can be freely accessed; therefore, there are limits to plant physical security. However, the turbines should be secured so that malicious actors cannot access the local plant control network (e.g., sending unsecured/encrypted traffic between turbines and the plant controller). Physical security best practice techniques, such as site perimeter controls, would minimize access to the intelligent electronic devices in the turbines or networking equipment. For instance, using fences (type, style, location, entire perimeter), gates (type, location, lockable), signage (no trespassing, closed-circuit television [CCTV]/electronic monitoring in use, who to call, etc.), and vegetation control to prevent blind spots.

4.2.6 Obfuscation and Deception

Intentionally deceiving an adversary may disrupt reconnaissance and attack attempts. Obfuscation can be conducted through a range of methods, such as generating false network traffic to disguise legitimate traffic or creating an overly complex program where a simpler, equivalent version would have sufficed. Similarly, honeypots and honeynets (device decoys or networks of decoys) can be inserted into the corporate network to confuse attackers and capture their actions prior to impact to physical systems. Obfuscation techniques are not common in ICS control systems, but these techniques may merit consideration in coming years. One example of ICS obfuscation was demonstrated in the DOE CEDS-funded CodeSeal program, in which a cryptographically secure, temper-resistant protocol was used to obfuscate software programs within the ICS. In networks with limited bandwidth, such as wind plant networks, the generation of pseudo-traffic may increase latencies but should nevertheless be explored.

4.2.7 Authentication

Connections between security boundaries are necessary for maintaining a functional control network. Research into authenticating access between regions using multifactor authentication mechanisms, one-time-use tokens, or other technologies that prevent password guessing attacks should occur. These exchanges and topologies should allow for MTD, IDS, and other countermeasures using unidirectional gateways, data diodes, DMZs with firewalls, etc.

[xvii] As required by California Electric Rule 21, the SunSpec Alliance recently announced their Public Key Infrastructure rollout for DER networks communicating IEEE 2030.5.

The establishment and continuation of cyber-focused workshops, trainings, and working groups could lead to the development of consensus-based security approaches for wind systems. Also, the sharing of cybersecurity alerts and the implementation of field-proven best practices can also help plant owners and operators establish cyber-safeguards and advanced protection methods to help protect against attacks.

Continuously refining the existing protection measures and developing innovative protection techniques will advance cyber-resilient wind plant designs, which is the ultimate goal to proactively protect wind plants from cyber attacks.

4.3 Detect/Analyze

Continuous, automated evaluation of the risks should be completed, and technical measures developed to reduce the exposure to cyber attack. Operational protective measures are designed to defend the control network to detect and respond to possible adversary access to control networks.

4.3.1 Situational Awareness

Advanced wind cybersecurity systems should include tools to capture, analyze, and visualize near-real-time data from all networks. These tools enable the monitoring, detection, alerting, remediation, and accounting of benign anomalies or hazardous incidents. NIST SP 1800-7, "Situational Awareness for Electric Utilities," describes the solution as comprising:

- Logging software or a security incident and event management system
- Bump-in-the-wire devices[xviii] for OT encryption and logging
- Commercial or open source software for collecting, analyzing, visualizing, and storing network data (e.g., historians, outage management systems, distribution management systems, and HMIs)
- Products that ensure telemetry and end-device data integrity.

Situational awareness (SA) is a predominant R&D area, with research in power system testbed designs, SA frameworks, wide-area SA with cloud computing and wireless sensors, design implementation, visualization, and attack detection and analysis. Given the expansion of cloud-based services into the energy sector, it is important for the wind industry to ensure the cybersecurity of these services. There is a clear need to inspect and visualize wind data traffic using SA tools with IDS analysis acting as the back-end alarm system. DOE programs like CyOTE™ and CATT™ (see section 4.4.1 for full details) could be leveraged for wind specific tuning of SA tools and techniques.

4.3.2 Intrusion Detection

Detecting adversarial actions on the wind control network is necessary to implement appropriate countermeasures. Wind system networks include a wide range of measurement and control information that can be used for anomaly identification and classification through inspection of communications metadata, or correlation/comparison with out-of-band data sources (SCADA, AMI, PMU, etc.) or nearby power equipment. For instance, if a wind inverter is reporting a low voltage, but other meters at the point of common coupling do not report the same behavior, this may indicate a spoofing, MiTM, or another type of attack. This control and measurement information may also indicate faulty equipment; therefore, efforts should be made through

[xviii] Bump-in-the-wire refers to a communication device that can be inserted into an existing network to monitor traffic and functionality on the network and to provide general situational awareness.

development and implementation of appropriate intrusion detection technologies to differentiate cyber-attack-related and non-cyber-related/operational events to determine the type of incident and its root cause. Top R&D priorities include research and validation of wind-specific anomaly-based IDSs and methods. Once validated, asset owners and other associated partners could implement these IDS technologies, while continuously improving the signatures and technologies. Long-term, the continued R&D for intrusion detection will be targeting the future of wind systems and their technologies.

Machine learning can be used to learn typical network traffic behavior and alert when unexpected (e.g., malicious) communications are detected. For instance, Sandia developed an adaptive resonance theory artificial neural network to provide real-time monitoring of a building automation system. Further IDS research should also be conducted in:

1. Protocol-aware sensors which internally conduct deep packet inspection.
2. Probing or perturbation techniques to differentiate artificial and actual data sources.
3. Creation of strong and weak indicators (based on data streams from all sensors) to warn or alert to malicious activity.
4. Creation of trust-weighting schemes that value information from highly secure telemetry over easily spoofed or accessed data sources.
5. Sensor correlation—possibly with power system state estimation—to identify suspect data streams.
6. Creation of "trust monitors" that monitor critical buses or equipment with out-of-band approaches (e.g., monitoring equipment power draw or anomalous traffic to identify malicious traffic).
7. Visualization techniques and exfiltration detectors.

Both IDS and machine learning should be coupled with whitelisting whenever possible. Only allowing necessary traffic by specifying protocol and application parameters and allowable executables is an effective means to preventing malware from progressing. The difficulty of specifying all allowable parameters is often a challenge as the complexity of wind control networks can be significant. Research should be performed to make whitelist specifications sharable and available to a wide audience to limit the impacts of a compromised application or endpoint.

Additionally, intrusion detection for physical security breaches of wind facilities and assets should be implemented. Complementary to measures described in Section 9.7, Physical Security, intrusion detection for physical security systems is necessary to alert personnel to unauthorized access inside protected areas, inside wind towers, and tampering with surveillance or communications equipment, among others. For example, fencing can be equipped with coaxial or fiber cabling with video or motion sensor surveillance to indicate tampering or climbing. Doors at the base of wind towers should be alarmed; alarms should alert the control center of unauthorized or forced entry.

4.4 Respond

The risk to the power system is represented by the probability of an attack and the consequences of such an action. Encouraging the development and implementation of appropriate response capabilities can minimize the effects of a cyber attack. By implementing countermeasures, wind systems can increase system resilience, extend the time and difficulty of perpetrating the attack, and minimize the impact to turbine equipment and grid. This section details various response strategies that may be employed after a successful cyber attack.

4.4.1 Dedicated, Recognized Information-Sharing Platforms

Improving cybersecurity situational awareness (SA) for wind energy stakeholders will help improve performance, lower costs, and reduce market barriers for the U.S. wind industry. The DOE Cybersecurity Strategy for 2018–2020 identified "enterprise-wide cybersecurity SA geared towards actionable intelligence" as a critical need.[94] This critical need could be addressed in the near term by performing wind-specific gap analysis, developing best practices, and sharing this information across the industry.

Sharing cybersecurity threat data among wind energy stakeholders may maximize the benefit of this resource. Defining the cybersecurity roles and responsibilities among developers, owners, operators, vendors, and service providers improves cybersecurity resiliency by ensuring active participation by all parties. Subsequently, the promoting and sharing of cybersecurity resources can help plant owners/operators and vendors to 1) better adopt and apply enhanced incident response technologies and 2) understand cybersecurity best practices guidance. The standardization of information-sharing methods and frameworks and the development of mechanisms to effectively create and share mitigation strategies among the wind energy community can benefit the larger cyber-information-sharing community through lessons learned at peer locations, thereby lowering costs to secure equipment. Learning from events at other wind plants may prevent a widespread cyber event from occurring or mitigate its impacts.

There is a need to ensure that existing information-sharing platforms can ingest both unclassified and classified information from wind energy stakeholders, and provide actionable threat information that includes technical context for wind farm owners and operators. Sharing threat data may have privacy, proprietary data, classification, and indemnification considerations. For example, personal information that is not redacted in the sharing process could be used for criminal prosecution or to expose companies and individuals to public scrutiny. Still, some significant benefits remain; secure platforms can be used to determine trends in sophisticated adversaries, indicate the possibility of coordinated attacks or vulnerabilities likely to be exploited, and notify appropriate stakeholders of potential mitigation actions.

Multiple programs provide mechanisms to share cybersecurity threat data between government agencies and the private sector. These include:

- The Department of Defense's Defense Industrial Base (DIB) Cybersecurity Program (DIBNet). DIBNet is a voluntary information-sharing platform between Department of Defense and DIB participants. DIBNET allows participants to share unclassified and classified cyber threat information using a structured question format.

- DHS's National Cybersecurity and Communications Integration Center (NCCIC). NCCIC is a hub for cybersecurity information and expertise. The NCCIC shares cybersecurity information via online web portals, email, automated data exchange, teleconferences, classified meetings, and onsite consultations. The NCCIC also houses the US-CERT and ICS-CERT portal that is a collaborative system to share cybersecurity protection and prevention information as well as cyber-indicators, incidents, and malware digests.

- DHS's Automated Indicator Sharing (AIS). AIS is an ecosystem that exchanges threat indicators (such as a malicious IP address or a phishing email address) between the federal government and the private sector in near real time. The goal of the AIS indicators is to limit the reach of an attack by alerting other observers of the attempted compromise such that they may protect against the same attack vector. AIS indicators are exchanged through a server located at a participant's location.

- DHS's Cyber Information Sharing and Collaboration Program (CISCP). The CISCP program allows analyst-to-analyst sharing of threat and vulnerability information between government and industry

partners. CISCP is a free membership program that requires entities to sign a Cyber Information Sharing and Collaboration Agreement to join. CISCP receives data from submitters who may dictate the dissemination and handling of the data using the Traffic Light Protocol. CISCP reports data using indicator bulletins as well as analysis and malware reports that are distributed to its members.

- E-ISAC's Cybersecurity Risk Information Sharing Program (CRISP). CRISP is a public-private partnership, originally funded by DOE in partnership with industry, and now managed by the Electricity Information Sharing and Analysis Center (E-ISAC). The purpose of CRISP is to collaborate with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information and to develop SA tools that enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources. CRISP leverages advanced sensors and threat analysis techniques developed by DOE along with DOE's expertise as part of the nation's Intelligence Community to better inform the energy sector of the high-level cyber risks.

DOE has several information-sharing and situational awareness programs that support the electricity sector. These include:

- DOE's CyOTE™ Cybersecurity for the Operational Technology Environment (CyOTE™) is a DOE program that demonstrates two-way data sharing and analysis within the complex OT environment, where utilities currently have less mature tools for threat detection. CyOTE™ could demonstrate and guide the collection of data on wind OT networks: determining what to monitor, how to collect and process data, and how to share sensitive data while protecting privacy. The results from CyOTE™ will inform the development of a repeatable, standard approach that the energy industry can use for real-time operational threat data sharing and analysis.

- DOE's Cyber Testing for Resilience of Industrial Control Systems (CyTRICS™). The CyTRICS™ program serves as a central capability in DOE's efforts to increase cybersecurity and reliability for the energy sector. In testing and enumeration critical electrical components, CyTRICS™ also conducts analysis of results to identify both systemic and supply chain risks and vulnerabilities by correlating threat information and supply chain information, and other relevant data and sources.[95]

- DOE's Cyber Analytics Tools and Techniques (CATT™ 2.0). Using unique and sophisticated U.S. government tools, the CATT™ program provides automated analysis of voluntarily provided energy sector IT and OT data enriched with classified threat information. Working with government partners and the energy sector, CATT™ also provides a secure platform to provide actionable information, mitigations, and to increase SA about advanced cyber threats among critical energy infrastructure.[96]

The Cybersecurity Information Sharing Act of 2015 is a federal law that aims to improve cybersecurity in the United States by protecting the sharing of cybersecurity threat and incident information. CISA provides liability protection for companies to share cyber threat indicators with the federal government[97] through the DHS process. Even with the CISA liability protections, the "free-rider" problem (entities consume incident information, but they do not contribute their own data) limits the extent to which the U.S. energy stakeholders participate in cybersecurity information-sharing programs. Some companies choose to share threat indicators among themselves (e.g., the Cyber Threat Alliance) instead of participating in government information-sharing programs.

CISA provided legal protection for companies to share cyber threat indicators, but companies should still weigh the benefit of sharing their cybersecurity incident data against the potential cost of collateral liability that would be absent if they kept these data to themselves. An expansion of an existing information-sharing program—or the creation of a new cyber threat information-sharing platform for wind plants—could allow

wind plant owners and operators an opportunity to share broader anomalies regardless of whether a wind asset owner can prove malicious cyber-activity, and would likely provide a stronger business case for companies to contribute and exchange data. Encouragement of information sharing among the wind energy community may include the sharing of cyber threat indicators; vulnerabilities; cyber incidents; lessons learned; tactics, techniques, and procedures (TTPs); and best practices.

4.4.2 Cyber Forensics

Google has created an open-source incident response framework with distributed forensics, called the Google Rapid Response platform. This system is helpful for determining the source of leaked corporate data post-event, conducting periodic health checks of system state, and isolating malware attacks. This framework, or similar technology, can be leveraged for use in OT/ICS/CPS environments to quickly find, then isolate or quarantine, malware attacks on wind power networks.

4.4.3 Identification of Contingency Operating Modes

The goal of many cybersecurity response and recovery actions is to establish methods to recover system functionality in a timely manner, while maintaining interdependent operations. Effective adaptive response should coordinate autonomous, semi-autonomous, and manual defense activities in a coordinated and federated response among grid and wind plant operators. Ideally, the response will absorb the cyber attack and recover to a known operable state quickly. Wherever possible, the adoption of fault-tolerant algorithms can challenge adversaries and increase the difficulty of compromising a cluster of systems. Additionally, emerging technologies, namely software-defined networks and MTDs, can be used by grid and wind plant operators reconfigure the network autonomously. Similarly, quarantine techniques such as enclaves can quickly isolate compromised devices, for example by using clustering and factorization techniques.

Another cyber-attack response strategy could involve reverting centrally controlled or automated operations to manual or distributed operating modes. Such a temporary contingency mode will allow time for forensics, restoration operations, or other recovery systems to take over while still maintaining critical functionality. For wind control systems, this could be the reversion to default, low risk operating modes. This will allow grid operators to regain control of the network while wind systems are still providing nominal voltage and frequency regulation. Modeling or simulation of contingency operating modes, either with virtualized or physical testbeds, will allow operators to create and gain confidence in new and more effective contingency modes.

4.4.4 Resilient Designs

Cyber-resilience is the ability of the system to maintain critical operations in the presence of adversary actions. This is typically performed using adaptive systems with components engineered to fail gracefully so that backup, fail-over, and recovery equipment may be brought online. Cyber defenders may also isolate or quarantine certain networks or transfer operation to different processes. In the case of wind networks, just as with the broader energy sector, switching operations to redundant backup communication networks or control systems may be possible. In the near term, wind turbines can be configured with local control operating rules when communications are lost for extended periods of time. Autonomic self-repair, adaptive defenses, or pushing known good firmware updates to equipment could be novel approaches to future resiliency-in-design of wind energy technologies. Machine learning techniques may also be used to learn from past compromises and continue critical functions while under attack.

4.4.5 Dynamic Assessment

Like SA tools, dynamic assessment technologies conduct real-time analytics on data streams. In this case, the analytics are designed to understand the tactics and approach of the adversary. This information is used to

assess system damage, manage future compromises, and plot a recovery course so that a compromised wind component can be timely transitioned to alternative equipment to slow down or stop the spread of an attack.

4.4.6 Cybersecurity Investigations and Attribution

Following a cyber attack, it is necessary to dissect the sequence of events that led to the breach so that security gaps can be patched. It is also necessary to identify those responsible to begin criminal proceedings or other law enforcement arrangements. Log file inspection tools for attribution and other forensics technologies implemented by groups such as those within ICS-CERT Advanced Analytical Laboratory are necessary to begin the judicial processes. Reverse engineering malware can determine the creator, the target equipment, and accessed data. One longer-term objective of the National Science and Technology Council's approach to cybersecurity is to develop technologies to accurately and automatically identify malicious actors in real-time with enough precision to impose rapid prosecution, sanctions, or other responses.

As mentioned in section 4.4.1 above, establishing wind-industry-specific practices for cyber incident response reporting and post-incident investigations can help support the implementation of new (or enhance existing) cyber threat, vulnerability, incident, and mitigation information-sharing platforms for wind systems. Ideally, the results of both cyber incident response and investigations could be shared with other plant owners and operators in the wind energy sector.

4.5 Recover/Manage

4.5.1 Wind and Electric System Restart Capabilities

Recovery capabilities, similar to response actions, are designed to improve an organization's ability to address cyber attacks. These capabilities, however, improve an organization's ability to return to normal operations rather than quickly responding to and stopping an active cyber attack (response capabilities). The wind industry has developed methods to address or recover from disrupted operating states. For example, wind turbines, whether land-based or offshore, have built-in mechanisms to lock and feather blades (reducing the surface area that is pointing into the wind) when wind speeds exceed ~55 miles per hour. The wind turbine is in "survival mode," essentially, waiting for a storm to subside so it can safely continue generating power. Offshore, storms can be even stronger, so in addition to wind impacting the turbine, the offshore wind turbine's foundation must also contend with large, powerful waves. The engineers who design wind turbine systems use models to understand how different loads, such as winds and waves, will impact a wind turbine and its foundation.

Although these models exist to assist operators with responding to weather changes, the wind industry has not developed similar models or techniques to respond to cyber incidents. The research community and wind industry could learn from existing modeling techniques. As an example, PowDDeR (Power Distribution Design for Resilience) is an INL produced analytics computer program that analyzes a wind plant system's overall ability to absorb a cyber event or physical disturbance.[98] PowDDeR considers the real and reactive capabilities of the wind system in a time-based response to a disturbance to visualize and identify the resilience weaknesses and strengths of the system. The characterization of a wind system, in terms of resilience, enables analyses to be performed in the design phase so inherent weaknesses can be rectified. Questions such as "how do we recover from a cyber attack?" require specific answers, which could be developed through interagency coordination. Models that characterize operational disruption need to be used to understand turbine responsiveness to attacks. Researchers should then perform simulations of turbines and controllers to generate countermeasures. This will not only help build better logic for wind plant operations in times of cyber attacks, but it can also help develop effective cyber incident response procedures for wind owners and operators.

One aspect of recovering from a cyber attack includes blackstart capability of the electrical grid. Current blackstart capabilities are dependent on traditional rotating machines that do not require electricity to start such

as diesel generators. Enabling wind turbines or wind plants to provide or assist in blackstart restoration of the electrical grid could enhance grid resiliency to a cyber attack on the electrical grid. Wind turbines could allow additional restoration locations, and increased speed of restoration. However, wind energy systems must be proven to be cyber-secure and -resilient before serving as a blackstart resource; wind energy technologies possessing known cyber-vulnerabilities may provide new attack vectors into the power grid for malicious actors. Additionally, research, testing, and validation of controls, methods, turbine types, and hybrid systems combinations are necessary to prove these capabilities by wind turbines or farms for industry adoption on both local distribution levels and a nation-wide transmission level.

4.5.2 Restoration

The concept of resetting the system to a known good state or "trusted gold-master" is not new but is not a standard practice. In some cases, equipment or service vendors may not allow customers to self-reset, instead mandating that the vendor manage system recovery. Regardless, wind asset owners should have and maintain incident response plans that include (internal and/or vendor-executed) procedures, including those detailing safe restart, power system communication and coordination, and system integrity validation, among others. The National Cyber Incident Response Plan offers general recommendations for enabling restoration and recovery following a cyber incident,[99] but a similar document addressing wind energy-specific restoration procedures is not currently available. Some wind equipment manufacturers offer incident or emergency response plan implementation including safe restoration techniques as a service,[100,101] but there does not currently appear to be a wind industry-wide standard or guidance for system recovery or restoration. Therefore, the creation of wind energy-specific restoration best practices represents an opportunity for future research and collaboration among wind stakeholders. Broad field testing of system restart and resilient capabilities (e.g., fast-switching communications, safe roll-back/restoration, etc.) in the near term would aid in the development of best practices.

At minimum and if possible, organizations should consider maintaining copies of all software to enable quick reinstallation of programs used for system operations. Using virtual machines or containers (e.g., Docker applications) would allow more rapid re-deployment to a previous secure state stored before network penetration. However, understanding when the system became compromised is essential to select the correct image to restore. Change controls, software, and firmware updates should be mirrored in the gold-master copies. Allowing the gold-masters to be updated opens new attack vectors; safeguarding the good state images is paramount to effective recovery. This technology is not used in ICS/OT systems currently but could provide a means to rapidly recover from certain types of security breaches. Finding the right frequency of checkpointing software without degrading OT network performance is a challenge that would need to be addressed to restore software to more current states.

Continued R&D for incident response—addressing new and evolving cyber threats—is aimed to couple with the establishment of wind industry-specific guidelines for cyber incident reporting and post-incident investigations. Related, the formation of guidelines for cyber event response and recovery is another long-term goal that could assist in the management of cyber incident response.

Many potential wind cybersecurity R&D topics have been identified in this chapter for each of the five NIST Cybersecurity framework areas. Those topics are not exhaustive, and new R&D topics will continue to emerge as wind technologies advance and as cyber attacks become more complex. Table 4 summarizes the proposed R&D activities discussed in this section.

Table 4. Summary of Proposed R&D Activities.

Strategies	Develop Wind Cyber-Culture	Identify and Protect	Detect	Respond and Recover
Research and Development	▪ Facilitate and support partnership opportunities among wind energy stakeholders to collaborate on cybersecurity R&D ▪ Develop and utilize incident response capabilities such as cyber forensics and network traffic/log analysis among wind owners/operators ▪ Provide guidance on effective intrusion detection system implementations in wind energy networks	▪ Identify methods and frameworks to quantify cyber-risk ▪ Develop threat models ▪ Explore effective cryptographic methods for wind energy technologies ▪ Evaluate the resilience of and vulnerabilities to wind energy equipment using testbeds ▪ Investigate cybersecurity and applicability of cloud services for wind energy ▪ Design cyber-resilient wind energy technologies ▪ Study adversary obfuscation and deception techniques potentially used in wind energy networks ▪ Investigate authentication methods for wind energy control regions	▪ Research tools and methods to increase situational awareness in wind energy networks ▪ Conduct intrusion detection research focusing on: creating protocol-aware sensors; understanding adversary probing techniques; creating threat indicators, trust-weighting schemes, and visualization techniques	▪ Explore and enhance contingency operating models ▪ Further investigate the potential grid-level impacts of cyber attacks on grid-interconnected wind energy systems ▪ Research dynamic assessment technologies and strategies to analyze real-time adversarial activity ▪ Explore and develop effective cyber forensics techniques for wind OT environments ▪ Design cyber-informed wind energy equipment resilient to cyber-physical events through automated response to known and unknown threats

5 Standards Development

Cybersecurity standards are not singularly effective means of preventing all cyber attacks because the standards development process typically takes years while new vulnerabilities are discovered regularly. Standards are also created by analyzing past known vulnerabilities to protect against them, rather than anticipating future risks. However, standards provide a good base level of security. Such standards could be developed for wind energy components, communication protocols, and management of cybersecurity risks.

5.1 Equipment

The NERC CIP standards (currently in their fifth version) cover physical security, cybersecurity, and other reliability issues for the bulk power system. These standards apply to bulk equipment (>20 MW) connected at 100 kV or greater, so only some wind systems will apply. The structure and language of these standards could be used as a foundation for an equivalent series of wind standards. CIP-002-5.1a identifies and categorizes cyber-systems and assets; CIP-003-6 specifies security management controls; personnel training and security awareness is in CIP-004-6; electronic security perimeters for critical assets and border access point protections are in CIP-005-5, physical security is in CIP-006-6, security system management is in CIP-007-6; incident reporting and response planning is in CIP-008-5; recovery plans are in CIP-009-6, configuration change

management and vulnerability assessments are in CIP-010-2; and NREC CIP also covers information protection (CIP-011-2), identification and protection for critical transmission stations (CIP-014-2), and supply chain management (forthcoming in CIP-013-1).[102]

5.2 Communication

Numerous standards and guidelines for wind communications exist; however, very few of these standards address cybersecurity for wind communications. IEC Technical Committee 57 has created an extensive collection of communications security standards for IEEE 1815, IEC 61850, and other communications protocols. Based on common security issues arising from security layers associated with organizational, informational, and technical practices as illustrated in Figure 7, IEC standards and guidelines addressing different levels of the communication stack are shown in Figure 8. The standards and guidelines cover a range of security requirements, such as key management, role-based access controls, security architectures, and data-in-flight requirements. As shown in Figure 9, the IEC has established a joint working group to investigate communications for wind power plants.

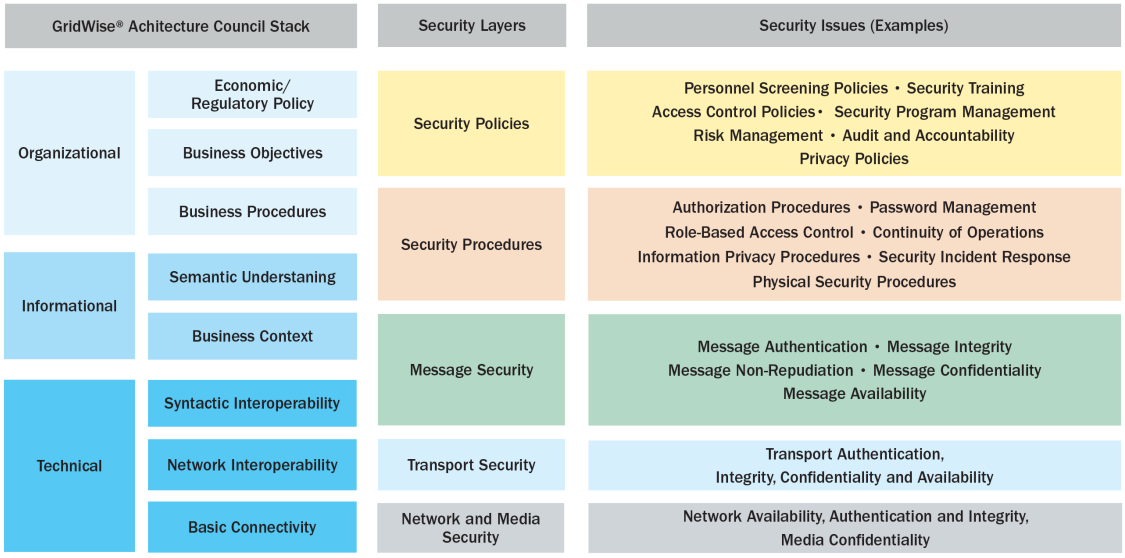

Figure 7. Common security issues associated with the security layers of organizational, informational, and technical practices.

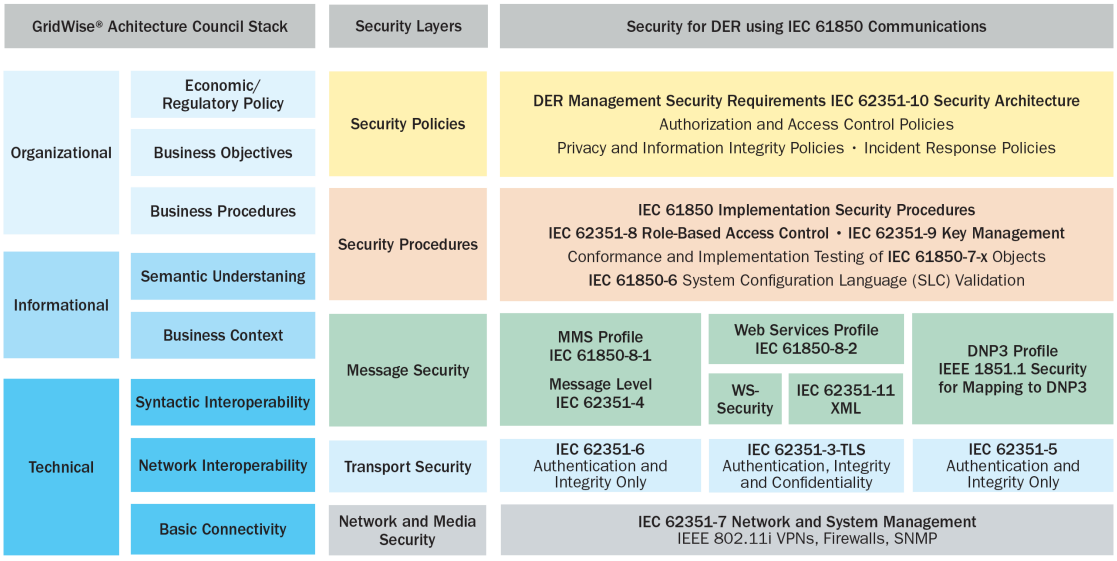

Figure 8. Mapping of IEC standards, technical committees, and working groups.[103]

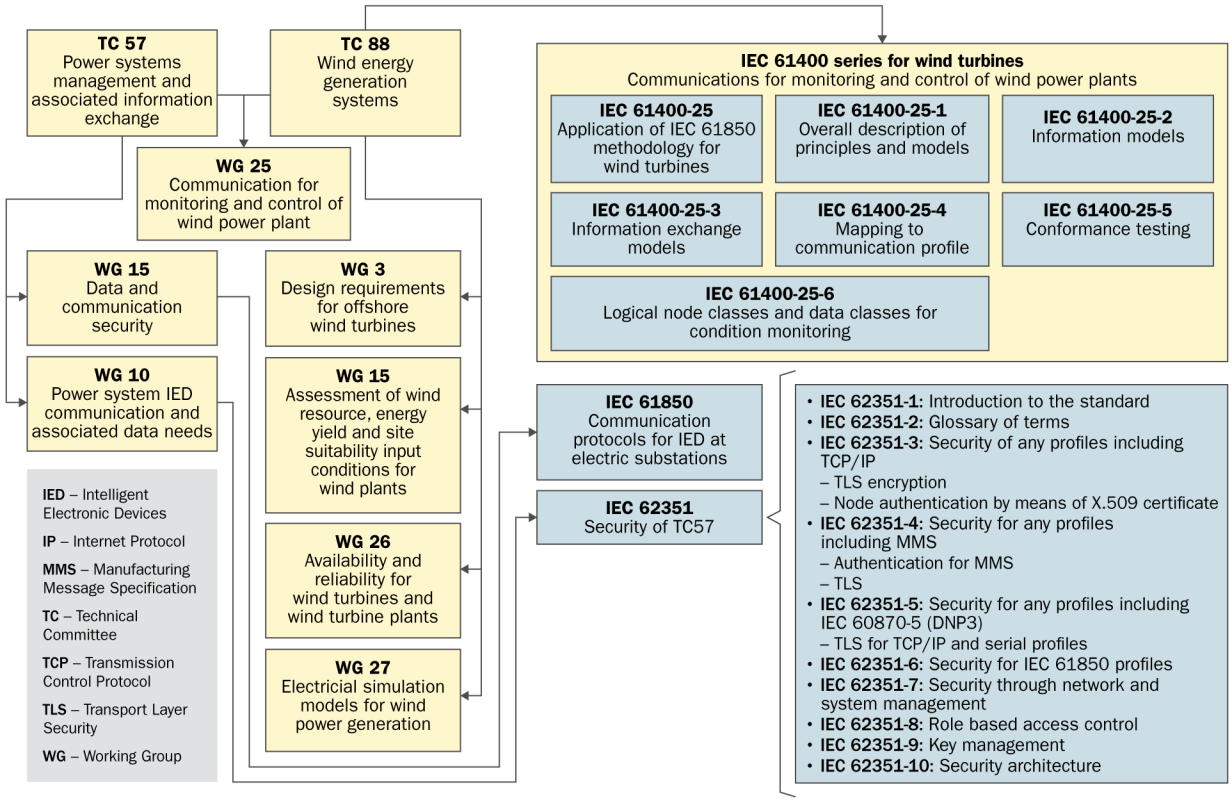

Figure 9. Mapping of IEC wind and communication standards.

5.3 Certification of Standards

Establishing a list of standards that address cybersecurity is a good first step, but a certification process is necessary to establish that wind facilities, components, and networks possess at least a minimum level of protection. If one wind facility has not adopted and implemented established standards, a malicious actor may leverage these deficiencies to pivot and attack other systems. For this reason, personnel from one utility interviewed for the Roadmap stated that standards related to cybersecurity should be more strictly enforced, fearing that other wind stakeholders may only enact the bare minimum of cyber hygiene practices to meet standards.[104] The creation of a wind-specific organization responsible for certifying and enforcing standards could ensure basic cybersecurity best practices are implemented in wind systems. According to wind owners, such an intermediary body could be created as a consortium of wind industry stakeholders that represents government, commercial industry, owners and operators, and research and academia groups.

6 Best Practices

Numerous practices are available that wind stakeholders can adopt to improve cybersecurity for wind energy systems. Practical and effective solutions are not universal: wind owners should individually determine cyber risk by conducting regular cybersecurity assessments and defining a desired cybersecurity posture to determine what practices should be changed, implemented, or augmented. Based on resource availability and overall feasibility, wind owners may consider different approaches to cybersecurity, some concepts of which are discussed below.

6.1 Cyber Hygiene

Cyber hygiene broadly refers to all practices and steps that individuals take to ensure systems remain secure and operational. These are generally preventative actions that become part of a routine and serve as a defense against the most frequent cyber threats. Cyber hygiene includes practices like two-factor authentication, awareness of phishing schemes via email, secure passwords, maintaining software updates, protecting and backing up data, and many others. Verizon issues an annual Data Breach Investigations Report, the 2018 edition stated that "phishing and pretexting represent 98% of social incidents and 93% of breaches. Email continues to be the most common vector (96%)."[105] This demonstrates that human behaviors remain one of the biggest vulnerabilities in any broad cybersecurity plan.

More specific to industrial control systems, the private security services company Dragos also publishes an annual report related to ICS related security statistics.[106] The 2018 report highlights an increase in "Adversaries using traditional malware and techniques to make the jump from IT to operations continued to be a major issue across ICS," and concludes with a recommendation that, "Organizations can lower their risk profiles and proactively protect against common attack techniques by performing security best practices. Implement proper security hygiene and the principle of least privilege based on a deep knowledge of the environment." This recommendation further indicates the importance of cyber hygiene best practices in the ICS environment.

Wind industry organizations can improve their cyber hygiene practices by following guides from NIST, such as its Guide to Industrial Control Systems (ICS) Security[107] or through participation in a variety of industry-formed organizations like the Edison Electric Institute which has resources on cyber and physical security.[108]

Figure 10 illustrates an example of security best practices such as those detailed by NIST, as implemented in typical wind farm network architecture. In near term, the wind energy community could work together and prioritize the development of basic cyber hygiene practices specifically for wind energy business and operational environments using existing government and private sector guides as well as first-hand experience from the wind energy community.

Ongoing training programs are important in keeping personnel up to date on their roles and responsibilities in securing wind systems. DHS ICS-CERT, in addition to many private companies, offers online and classroom training in ICS security.[109] Additionally, as noted by one utility, well-resourced wind owners and operators with established cybersecurity operations programs may be well-situated to provide cyber hygiene best practices or even training to smaller wind owners and operators.[110]

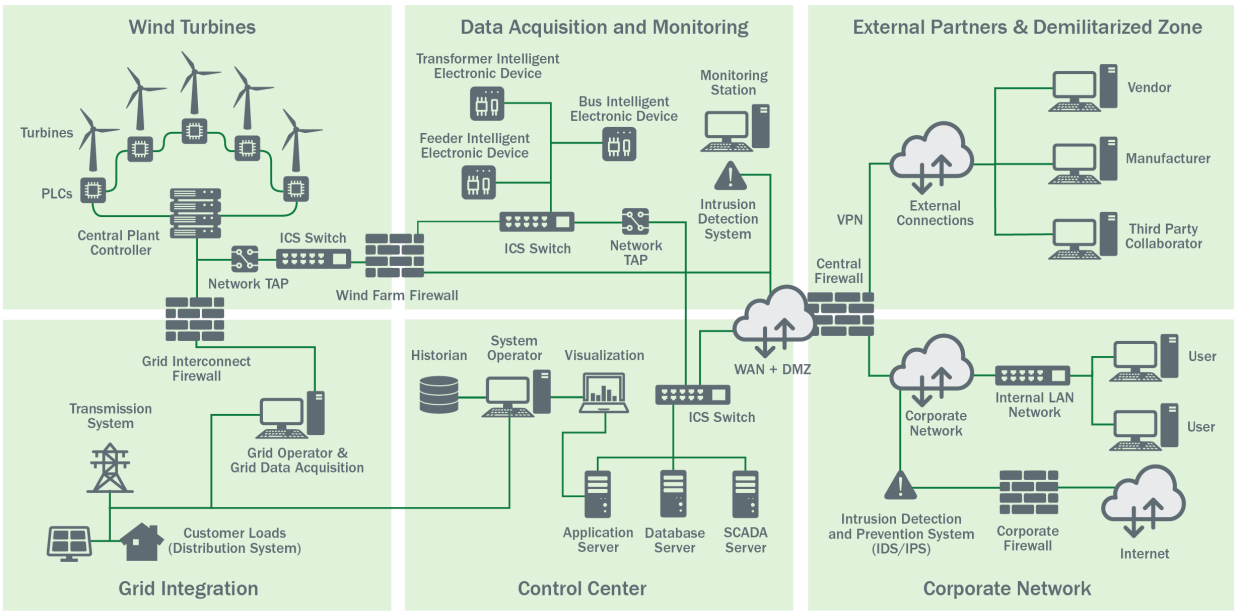

Figure 10. Wind farm reference architecture with secure best practice approaches like Network Segmentation, Zoning, Monitoring, and Intrusion Detection and Prevention System (IDS/IPS) for control and SCADA environment.

6.2 Technical Practices

According to the FY 2016 ICS-CERT assessment summary, boundary protection was the largest vulnerability for ICS systems. Asset owners and operators are recommended to implement the following technical measures in their systems in the near term: network segmentation and zoning, role-based access control and more secure remote access (including two-factor authentication and limiting remote functionality).[111] Regular review of these best practices are needed to ensure they are using the latest technology from the R&D community. Some common measures to prevent network penetration are explained below.

6.2.1 Network Segmentation and Zoning

The functions throughout the SCADA of a wind plant can be isolated into distinct network zones using network segmentation.[112] The system components that do not need to communicate with each other should not be allowed to communicate with each other. This network separation simplifies the roles of a network zone and allows the boundary firewalls to prohibit all traffic that does not have an exception rule. With the increase in distributed wind facilities, there are challenges to segment the networks for wind plant communications systems because the entire network will not necessarily be owned by a single entity.

Network segmentation is typically achieved by placing a filtering device, such as a packet filtering or stateful inspection firewall at a zone boundary. Firewalls at the network boundaries ensure that:

- Only authorized traffic can cross between zones

- Unauthorized traffic (inbound and outbound) is denied
- Authorized traffic is limited to specific systems within a zone.

Additionally, segmentation should help stop the most basic types of attacks and filter noisy protocols, such as inbound Internet Control Message Protocol, syslog, and Simple Network Management Protocol. An additional layer of security can be achieved by requiring the firewall to authenticate users prior to accessing a zone. Segmenting into defined security zones improves a site's defensibility by:

- Reducing attack surface
- Limiting exposure of critical production assets
- Using access controls to restrict movement from segment to segment
- Focusing security monitoring and controls on the zones where they can be most effective
- Improving detection and mitigation capabilities
- Aid in incident and forensics support.

Network segmentation is a powerful mechanism to protect wind plant network boundaries from unauthorized access, as it makes it harder for an attack to occur or propagate in wind plants.[113]

6.2.2 Role-Based Access Control (RBAC)

Role-based access control limits the roles and responsibilities of wind plant personnel to the least privilege that enables each person to perform their job function. Although not always convenient, it has the following benefits:

- Eliminates redundant access to sensitive equipment, processes, and data
- Logging is simplified because only limited roles are allowed access to a given resource
- An organization may meet compliance requirements by auditing a set of roles versus every employee
- Administration is simplified because role hierarchy allows permissions to cascade to subordinate objects.[114]

The cyber maturity of a wind plant can be increased due to the organization that an RBAC process requires.

6.2.3 Remote Access

Remote access to a wind plant should be limited to only those roles that require this access. One way to implement remote access to the wind plant is by allowing a VPN connection to the enterprise zone demilitarized zone (DMZ). To make a connection to the VPN, a user should authenticate with two forms of identification (e.g., username/password and a one-time password from a hardware token). Once authenticated, a user is granted access to a limited set of functions in the DMZ network zone. If the user role requires remote access inside the control system environment, it should require an additional two-factor authentication to either a gateway device or access system before allowing the remote user to access the resource inside the control system network zone. However, using other processes that eliminate the need for this level of remote access would prevent an attacker from pivoting an attack from inside the DMZ zone to the control network zone.[115]

6.3 Administrative Practices

In terms of cybersecurity, cooperation between entities implies that the parties work together to fortify, protect, and defend their equipment, resources, and processes from a cyber attack. Information sharing is the vehicle that enables cybersecurity cooperation between entities. Cooperation perpetuates when the entities involved believe that the relationship is mutually beneficial.

On its face value, cybersecurity cooperation (i.e., entities banding together for the common goal of improving cybersecurity preparedness versus going it alone) appears to be a positive practice that the energy community would be happy to embrace. However, many forces preclude industry partners and government agencies from sharing their collective cybersecurity knowledge, including the following:

- **Cost:** Industry partners are primarily focused on revenue generation. If an industry partner does not perceive clear and immediate incentives, they may choose to accept the cost of a cyber attack versus allocating resources to defend against a potential threat.[116] A government program may be scoped such that the funding is limited in time or focus that does not align with an industry partner's timetable.

- **Competitive advantage:** An industry partner that has spent considerable funds to build up cybersecurity capabilities may view the knowledge gained in this research as a competitive advantage that it does not want to give away. By contrast, a company that shares data about a cyber incident they experienced could damage their brand (at least in the short term) and lose customers to a competitor.[117]

- **Liability:** Details of a cyber incident may expose a company, its customers, or an equipment vendor to litigation, criminal prosecution, release of personal identifiable information (PII), and other retribution costs.

- **Silos:** Government agencies and businesses suffer from information silos where data flows vertically through the chain of command, but not horizontally, where it could be applied to address current engineering challenges. In these cases, it may be difficult to share cybersecurity data outside the established communication channels.

- **Control:** Cybersecurity incident data is sensitive because it may contain PII, unpatched vulnerabilities, and evidence of an attack. Government and industry have a vested interest in directing who can and should share these data. An entity may choose not to share cybersecurity incident data versus risking the data being shared with an adversary (e.g., a competitor).

The cyber emergency response of wind installations may benefit more from cybersecurity coordination and information-sharing policies in their leadership boardrooms than individual engineering decisions in server rooms. Sharing cybersecurity incident data involves a measure of risk (including possible compromise, loss of control, liability, and exposure), but not sharing these data could invite even more danger because the same cyber attack could be repeated at another wind installation. Dr. Amos N. Guiora, professor of law at the University of Utah, stated "The impact of cybercriminals is increased by the incapacity of their potential targets to recognize the advantages of adopting a cooperative model."[118] Coordination for coordination sake is not enough to get and keep industry partners active in the cybersecurity information-sharing process. Instead, "collaborative mechanisms must produce value to give businesses a reason to participate."[119] Legislatures are reluctant to regulate ICS,[120] which means that wind energy stakeholders are unlikely to be coerced into further cooperation with information-sharing programs if they have not already elected to do so. Wind energy stakeholders have diverse resources, priorities, and perspectives on cooperation with information-sharing programs, so the key to attracting participation is to focus on areas where they align.

6.4 Supply Chain Security

A report from Dragos highlights the increasing exploitation of trust between organizations and their vendors to gain access to secure systems.[121] The 2018 Wind Technologies Market Report tracks estimates of wind-related imports to the United States.[122] Figure 11 shows the total value of selected, tracked wind-specific imports to the United States in 2018, by country of origin. Around 50% of the import value in 2018 came from Asia (led by China), 35% from Europe (led by Spain), and 20% from the Americas (led by Mexico). This international supply chain exposes the power system to risks, as the control behavior of this equipment could be compromised. Currently, remote access to wind turbine equipment from foreign companies is permitted; while this could provide critical patches to software systems, it also expands the power system attack surface. Wind turbine manufacturers could establish cyber supply chain risk management (C-SCRM) programs as frontlines for supply chain security.

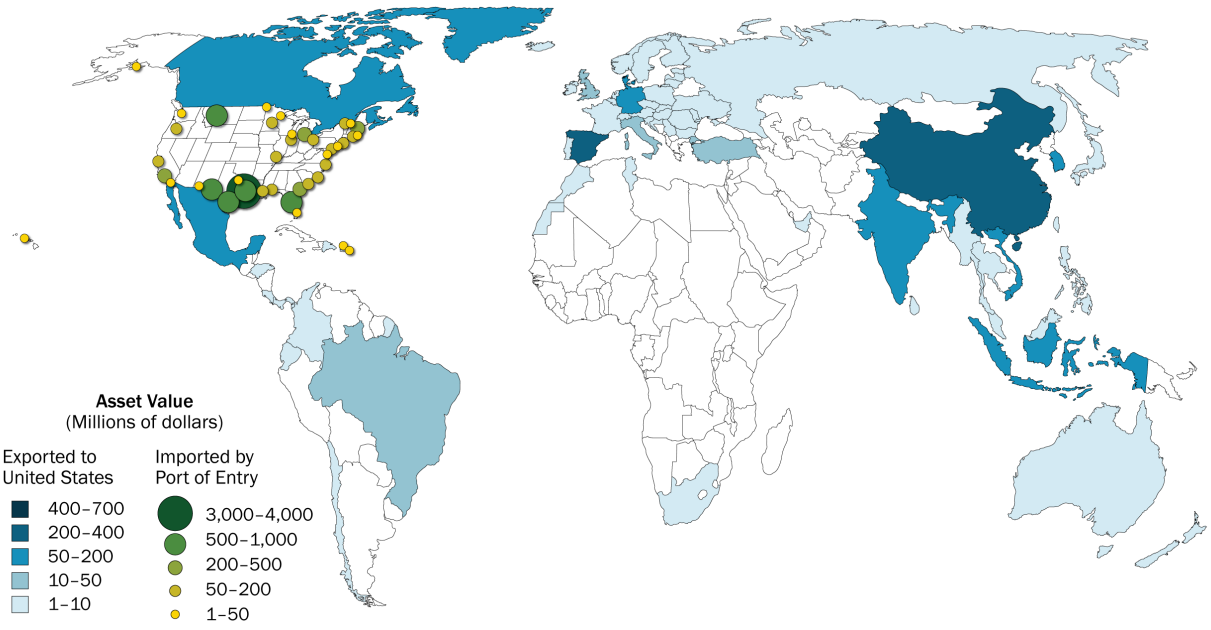

Figure 11. Summary map of tracked wind-specific imports in 2018: countries of origin and U.S. districts of entry.[123]

As discussed in Section 4.4.1, Dedicated, Recognized Information-Sharing Platforms, the CyTRICS™ program seeks to identify cyber vulnerabilities and threats to key energy sector ICS components by applying a targeted, prioritized, and collaborative approach to testing, analyzing , and correlating this information with supply chain information. CyTRICS™ could be used to investigate critical wind system components and to better understand wind energy digital component supply chains. This may be particularly beneficial for the wind industry, given the variety of manufacturers and vendors of wind energy technologies,[124] and the number of foreign countries from which the U.S. wind industry imports wind assets as indicated in Figure 11.

In 2015, NIST hosted a conference on cyber supply chain best practices. At this conference, they provided a brief that included the following supply chain risks:[125]

- Third-party service providers or vendors with physical or virtual access to information systems or software
- Poor information security by lower-tier suppliers

- Compromised software or hardware purchased from suppliers
- Software vulnerabilities in supplier systems or supply chain management
- Third-party data storage or data aggregators.

NIST also provided recommendations for protecting the supply chain along with interviews from many leading experts at Northrop Grumman,[126] Cisco,[127] Boeing and Exostar,[128] and NIST[129] to defend against these risks. The SANS institute has provided recommendations for combatting supply chain cyber risks by establishing recommendations for people, processes, and technology elements.[130] Also, several supply chain risk management standards and best practices apply to aerospace (SAE ARP9134[131]), electrical equipment/medical imaging (NEMA CPSP 1-2015[132]), and automotive industries (SAE AS5553A,[133] SAE AS5553B[134]). On October 18, 2018, the FERC approved the NERC Reliability Standard CIP-013-1, "Cyber Security—Supply Chain Risk Management."[135] This new reliability standard will supplement the current NERC CIP standards to mitigate cybersecurity risks associated with the supply chain for grid-related cyber-physical systems. The new CIP-013-1 standard will become effective on July 1, 2020.[136] Wind turbine equipment supply chain standards should reference these standards or adopt similar best practices to reduce the supply chain cyber risk.

6.5 Physical Security

Existing wind plant infrastructure often have poor on-site physical security. This is partially due to the remote nature of wind installations and amount of time necessary for personnel to respond to on-site security issues. Access to a single turbine, IED, communication switch, or feeder allows alteration of wind plant operations, can scale-up the attack, and can cause multiple wind sites to fail. Numerous recommendation documents and implementation guides for physical security of electricity sector assets are available. The NERC Security Guideline for the Electricity Sector: Physical Security[137] is intended to provide guidance for identifying and protecting bulk electric system assets, yet the physical security measures described are highly applicable to wind sites and control centers. Among the physical security guidelines relevant to wind assets are:

Access control to wind facilities should include considerations for:

- Issuance of ID cards/access badges to staff, separate from third-party contractors
- Forming an authority that issues, revokes, and maintains records of site access grants
- Conducting periodical inventories of access control points, access history, and authorized access lists
- Maintaining procedures for lost access credentials, revoking credentials/access when no longer needed.

At the plant level, wind plants should possess at least basic perimeter control that may include:

- Fences, gates, locks
- Adequate lighting
- Secured/locked handholes
- Prominent signage (No Trespassing, CCTV/Electronic Monitoring in use, who to call, etc.)
- Video surveillance, intrusion detection sensors
- Vegetation control to prevent hiding spots/blind spots.

At the turbine level, the base of turbine stalks should also include at least:

- Locks on turbine base doors
- Turbine base door alarm system
- Locks on electronics and equipment cabinets within the base.

Physical security of wind plant control centers should include:

- Redundant access control to building, control center, and control center workstations or other operating equipment
- Related to general access control measures, a control center should include measures to identify and log all entering persons
- Ideally, security personnel should be present and able to regularly monitor the control center perimeter and interior.

These guidelines describe basic physical security for wind energy facilities and should be considered and reevaluated throughout a wind plant's lifecycle to ensure continued efficacy and completeness in application.

Several wind cybersecurity best practices have been identified in this chapter, and are summarized in Table 5. The topics discussed are not exhaustive, and new best practices will continue to emerge with the continued advancement of cybersecurity techniques, wind technology innovation, and more frequent and sophisticated cyber attacks. As some of the best practices may be applicable to other critical infrastructures, public and private stakeholders should feel empowered to adopt those aspects that best meet their individualized needs.

Table 5. Summary of Best Practices.

Strategies	**Develop Wind Cyber Culture**	**Identify and Protect**	**Detect**	**Respond and Recover**
Recommended Practices	▪ Promote and provide resources for cyber hygiene awareness and implementation ▪ Invite stakeholders to attend and participate in cybersecurity working groups, cyber assessments ▪ Encourage vendors to solicit customer feedback for cybersecurity feature requirements and participate in information-sharing programs ▪ All stakeholders participate in post-cyber event response and recovery efforts	▪ Conduct cyber assessments ▪ Provide basic cyber hygiene training for personnel ▪ Maintain up-to-date cyber-asset lists ▪ Use effective network segmentation techniques ▪ Require device-level authentication ▪ Employ appropriate physical security controls to buildings and equipment ▪ Vendors design cyber-resilient wind energy technologies	▪ Maintain full situational awareness of OT environment ▪ Utilize intrusion detection techniques ▪ Continuously monitor and analyze network data for anomalous activity and threats ▪ Conduct multi-party/role cybersecurity exercises ▪ Vendors improve supply chain security and accountability practices	▪ Learn to better recognize and report potential cyber incidents or malicious activity ▪ Implement cyber emergency response plans ▪ Establish internal cybersecurity roles and responsibilities ▪ Vendors provide timely updates and patching ▪ Owners/operators establish cyber incident response teams with wind-energy focus and expertise

7 Stakeholder Engagement

Major industry stakeholders include original equipment manufacturers, operators, utility companies, and wind plant owners. According to AWEA's 2018 annual market report, the top four wind turbine manufacturers in the U.S. market are GE Renewable Energy, Vestas, Siemens Gamesa Renewable Energy, and Nordex USA (Figure 12). GE currently offers a suite of products and services to evaluate, harden, and maintain the cybersecurity posture for wind assets. Based on the AWEA report, no solutions are currently being provided by Vestas and Siemens Gamesa, and the same appears to be the case for Nordex.[138]

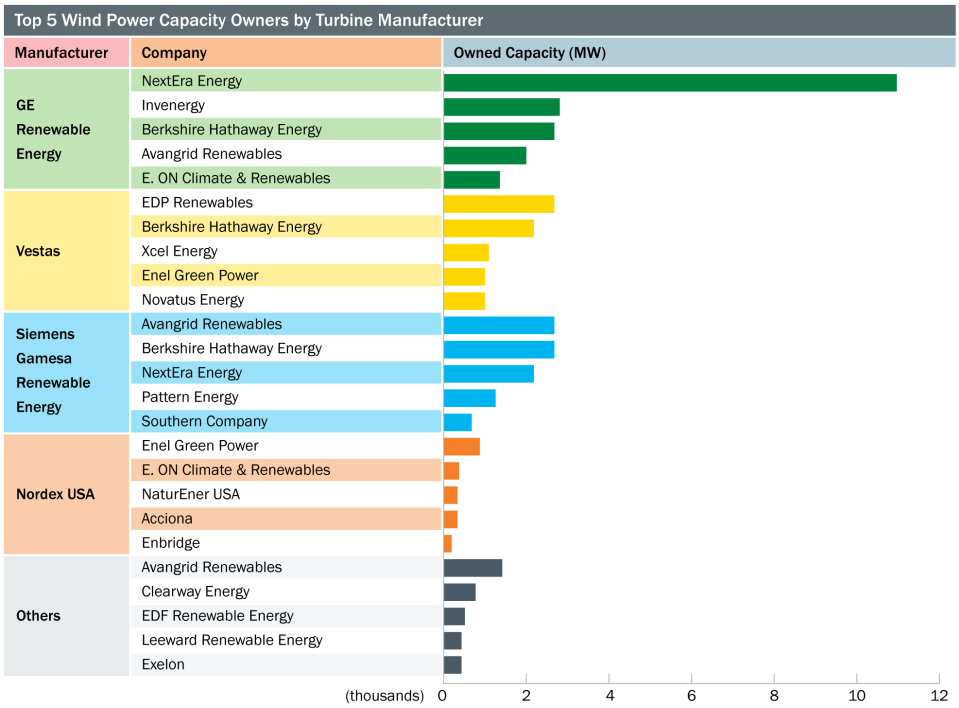

Figure 12. Top 5 wind power capacity owners by turbine manufacturer. Reproduced from AWEA 2018 Annual Market Report.[139]

The AWEA annual market report shows the top 25 owners of wind assets in the U.S. market (Figure 13). It also lists the top ten U.S. utilities with ownership of wind assets (Figure 14), the top five of which have wind capacities greater than 500 MW. Among these ten companies, the majority of them (about 90%) offer various degrees of cybersecurity solutions to their customers. One of the reasons for utility companies to excel in cybersecurity might be the experience they have accumulated in traditional power generation.[140]

Additionally, academia can play a greater role in R&D of cybersecurity for wind. In recent years, the number of university research groups focusing on wind power has increased. A few active representatives include Purdue University,[141] Stanford University,[142] Texas Tech University,[143] University of Massachusetts–Amherst,[144] and University of Massachusetts–Lowell.[145] Most R&D activities conducted by these groups focus on technical, economic, or policy-related topics, rather than cybersecurity, though recent research projects conducted by groups from the University of Tulsa,[146] and from the University of Washington with the Virginia Polytechnic Institute[147] focused on the susceptibility of wind plant control devices and networks to cyber intrusions and attacks.

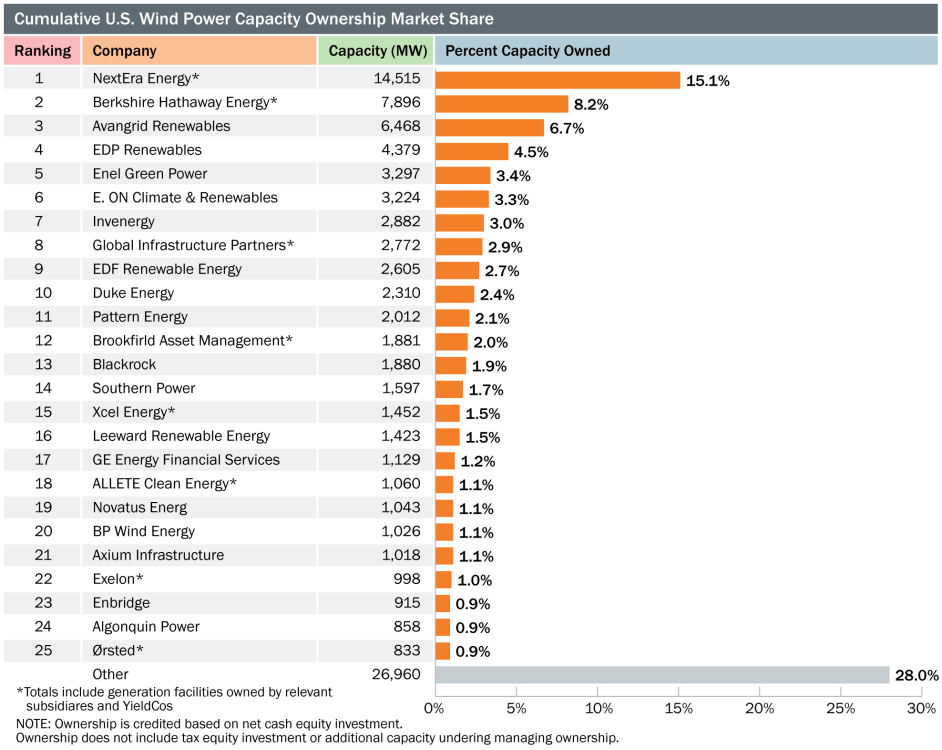

Figure 13. Cumulative U.S. wind power capacity ownership market share. Reproduced from AWEA 2018 Annual Market Report.[148]

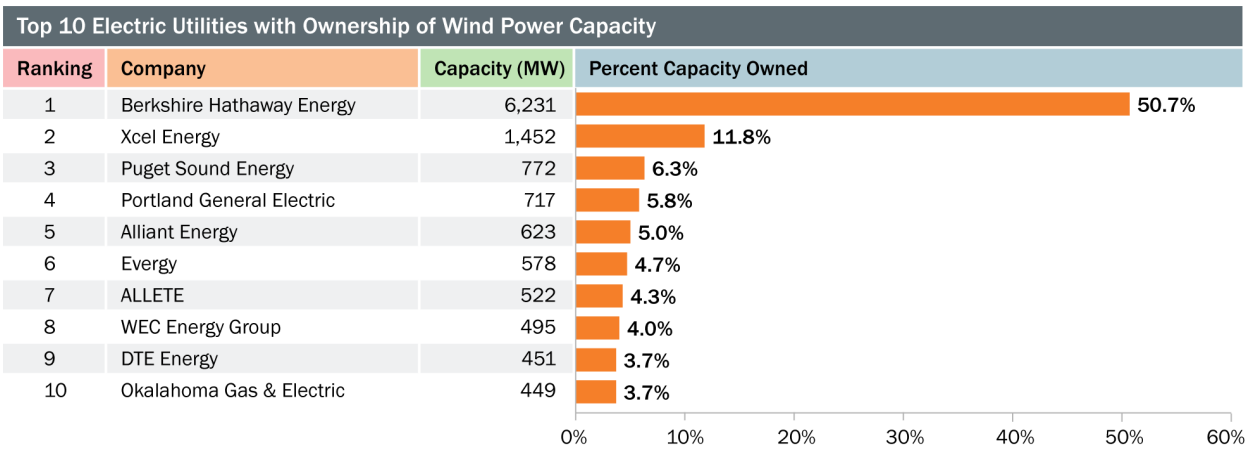

Figure 14. Top 10 electric utilities with ownership of wind power capacity. Reproduced from AWEA 2018 Annual Market Report.[149]

Also, various governmental agencies have wind programs, including several national laboratories: DOE's NREL, Sandia, INL, and Pacific Northwest National Laboratory. The wind cybersecurity R&D and initiatives led by DOE and its national laboratories play a critical role in helping the wind industry become more cyber secure because they tackle wind generation as a holistic problem versus the single product focus a vendor would focus on. The interactions between these government organizations and the regulatory agencies (NERC, NARUC, etc.), other research institutes (e.g., EPRI), or commercial organizations (AWEA, Energy Systems Integration Group [ESIG], etc.) are important to solve common wind generation cybersecurity challenges.

Most private-sector stakeholders (e.g., turbine manufactures, utility companies, and owners) are AWEA members. ESIG Operation & Maintenance users group represents about 80 to 85% of the U.S. installed capacity and is a platform through which engagement could have potential impact. However, a large utility with significant renewables holdings noted that topics related to wind cybersecurity are still infrequently presented at industry events.[150] Due to the participation rate in organizations such as ESIG and AWEA, these groups have an opportunity to expand cybersecurity awareness by including more opportunities to discuss, share, and learn about cybersecurity for wind during their events.

Stakeholder engagement is critical to developing cyber-secure wind communication systems. Engagement activities bring together individuals across industry, academia, and government to exchange ideas and educate one another. This will predominantly be directed by government agencies, such as the DOE, but other organizations (IEEE, Electric Subsector Coordinating Council, etc.) may also conduct these activities.

Wind technology is difficult to isolate because of the differences of companies that create wind products, operate wind turbines, and distribute wind energy. Figure 12 shows how widespread the number of entities involved is just for manufacturing and operating of wind technologies. Figure 13 details the large array of owners, while Figure 14 shows that even several of the largest utility companies are involved in owning wind assets. Because there are many actors in the wind industry, each company needs to play a role in protecting their products.

Coordinated stakeholder engagement can create effective forums for academia, government, national laboratories, industry, grid operators, and others to congregate and discuss short- and long-term direction. These forums will enable the processes for (a) reporting, analyzing, and responding to cyber attacks, (b) prioritizing R&D investment, and (c) accelerating commercialization by establishing pilot projects to demonstrate innovative technologies. Additional details of these components are provided in the following sections.

Like cybersecurity for the photovoltaic (PV) industry,[151] stakeholder engagement is critical to developing cyber-secure wind communication systems. It will enable information exchange among industry, academia, and government. The channels can be through special gatherings organized by the government (e.g., DOE and its laboratories) and various organizations (AWEA, ESIG, the Electricity Subsector Coordinating Council,[152] NERC, etc.), and information sharing through publications (papers, technical reports, etc.) or dedicated platforms (E-ISAC,[153] etc.). The objectives for stakeholder engagement laid out for PV cybersecurity[154] are also applicable to wind and are reproduced below:

Using the DHS National Infrastructure Protection Plan as a guide, stakeholder engagement should help the private sector secure wind energy cyberspace by:

- Managing infrastructure by maintaining awareness of critical assets, vulnerabilities, and risk
- Participating in information-sharing programs
- Assessing the security of networks by conducting regular audits, implementing best practices, and creating continuity plans
- Improving resiliency and minimizing risks by examining alternative cybersecurity solutions
- Promoting secure out-of-the-box implementations of software and hardware systems
- Encouraging adoption of cyber-secure communication protocols and guidelines
- Demonstrating of the ease and practicality of operating cybersecurity features

- Identifying existing or newly created research gaps.

Details on various stakeholders and their current cybersecurity activities status and engagement channels are provided in the following sections.

7.1 Information Sharing

As the President and CEO of NERC said in a February 2017 House of Representatives Subcommittee on Energy hearing, the United States "cannot win a cyber war with regulation and standards alone. Industry should be agile and continuously adapt to threats and to do that we need robust sharing of information regarding threats and vulnerabilities."[155]

Cyber vulnerability and threat information sharing among the wind industry is difficult due, in part, to direct business and market share competition among renewables stakeholders. According to one large wind owner/operator, wind owners are less willing to share available cybersecurity information, including best practices, with other stakeholders for fear of losing a competitive advantage by voluntarily assisting a competitor in improving the latter's cybersecurity posture.[156] Wind energy and other energy sector stakeholders also have concerns that cyber incident data shared with a government-administered information-sharing platform could be used against them in the future. Additionally, there is no established cyber threat and vulnerability information-sharing platform for the wind industry. One utility indicated that unique cyber vulnerabilities and threats associated with wind energy technology may not be easily accessible or available via general energy sector or other information-sharing platforms.[157] Wind owners/operators generally rely on various third-party cybersecurity services to provide cyber threat information, which often addresses broader IT-specific threats, rather than cyber threats to OT, and does not provide wind-specific threat, vulnerability, and advisory information.

Often sharing actionable threat information is difficult because it tends to be sensitive or classified because of the source, collection methods, or associated proprietary information. However, mechanisms are being developed for sharing this type of information between government agencies and stakeholders. Within the energy sector, CRISP is a public-private partnership designed to facilitate the exchange of classified and unclassified threat information. CRISP is also developing near-real-time SA tools for critical energy infrastructure to identify and protect these resources. Utility data is provided via information-sharing devices to DOE's Pacific Northwest National Laboratory and NERC E-ISAC to conduct semi-automated threat analytics.[158] While this program has been oriented to utility systems to date,[159] an expansion of this technology could be offered to wind system aggregators and others involved in communications to distributed energy assets; whether this is a new wind-specific cybersecurity information-sharing program or a subset of a previously created organization is to be determined. Additionally, the costs associated with participating in CRISP may be prohibitive to mid-sized and small wind energy facilities, meaning any expansion of CRISP to benefit wind energy would likely require a lower financial commitment. Stakeholder engagement programs should also define mechanisms for disseminating credible, actionable threats or vulnerability information between industry and government at the classified and unclassified levels.

The NERC Security Guideline for the Electricity Sector: Threat and Incident Reporting, provides requirements for reporting cybersecurity incidents.[160] Similar requirements can be established for wind control systems so that the latest attack behaviors are known by all stakeholders. This information could be provided through an established cybersecurity risk sharing program or a newly developed program specific to DER control networks. In the case of DER devices, customer data privacy is a concern with information sharing. Working within standards organizations and working groups, policy makers, federal agencies, and industry should determine the quantity and type of customer data necessary to generate effective threat and vulnerability assessments. Several information-sharing recommendations were provided in the Bipartisan Policy Center's

Electric Grid Cybersecurity Initiative,[161] which may be used a foundation for wind-focused security recommendations.

7.2 Workforce Development

A common trend in wind plant network and digital asset management is to rely on the cybersecurity resources of a broader owner/operator utility's IT team. IT personnel are trained to construct and maintain IT assets based on data and functional priorities for (in order of importance) confidentiality, integrity, and availability. However, wind plants are composed of OT assets, the priorities of which (availability, integrity, confidentiality) are inverse of the IT priorities and require different considerations to ensure cybersecurity. One utility noted that a team of only a few IT technicians primarily tasked with maintaining the utility's broader business operations were also tasked with maintaining network security for all utility wind assets.[162]

Beyond common reliance on IT personnel for OT maintenance and troubleshooting, the wind industry currently lacks hybridized IT-OT professionals with cybersecurity expertise specific to wind energy. Wind technologies use much of the same OT equipment as other electricity subsector assets, but have some unique technological needs and limitations, many of which involve the blending of IT and OT technologies in wind plant environments. According to a 2019 SANS Survey, two of the top six initiatives for increasing OT/control system and network security in operational environments and facilities included investing in cybersecurity awareness and cybersecurity training for IT, OT, and IT/OT hybrid personnel.[163] By adopting similar initiatives, the wind industry can ensure future wind personnel have the appropriate experience to recognize and address the particular cybersecurity needs of wind plant networks and equipment. Further, educating the wind industry about the risks, solution space, and codes and standards for cybersecurity is essential for efficient improvements to wind cybersecurity posture. This education can occur in a range of methods, including:

- Technical and non-technical publications from industry experts, government organization, NGOs, etc.
- Workshops such as the NREL Cybersecurity and Resilience Workshop[164] and DOE's Cyber Fire training events[165]
- Conferences such as DEFCON, Security Week's ICS Cyber Security Conference, Black Hat conference series, IEEE Cybersecurity Development Conference, etc.
- Training offered by the SANS Institute, DHS Cyber Storm, and ICS-CERT courses developed and facilitated by INL or simple webinars from Sandia Energy or the NREL Smart Grid Educational Series that often cover cybersecurity topics[166]
- General discussions with the PV industry about the impacts of improved cybersecurity on reliability, cost, efficiency, etc.

7.3 Working Groups

Existing working groups (e.g., NERC, IEC Technical Committees) on cybersecurity can be leveraged to benefit wind cybersecurity. Cybersecurity-specific working groups can be established within commercial organizations (e.g., AWEA, ESIG), governmental agencies, or standards committees (e.g., IEC, IEA). These groups can have regular meetings to exchange up-to-date information, discuss needs, develop best practices, and prioritize R&D opportunities, etc. One such event is the NERC GridSecCon,[167] in which wind cybersecurity stakeholders can participate.

In 2017, SNL and the SunSpec Alliance launched the DER Cybersecurity Workgroup to bring together DER interoperability and cybersecurity experts to discuss security for DER devices, gateways, and other networking equipment, owned or operated by end users, aggregators, utilities, and grid operators. The objective of establishing the group is to generate a collection of best practices that act as basis for, or input to, national, or international DER cybersecurity standards. Initially, the work was subdivided into four subgroups:[168]

- **Communication and Protocol Security** to define requirements and draft language for data-in-transit security rules
- **Secure Network Architecture** to create DER control network topology requirements and interface rules
- **Access Controls** to classify data types, associated ownership, and permissions, and define a set of protection mechanisms
- **DER/Server Data and Communication Security** to define standardized procedure for DER and server vulnerability assessments.

Bringing together experts in this working group and standards development organizations (SDOs) to discuss best practices and requirements for wind equipment is necessary as interoperability requirements are implemented. It is also essential that representatives from cybersecurity working groups and SDOs coordinate through open, honest dialogue about the focus of each effort and how the activities complement each other. The focus of the group is on PV systems; however, it could serve as a model for a new, but complimentary and coordinated effort covering wind energy.

7.4 Vendor Engagement

Wind energy technology vendors serve as one of the foremost influencers for wind cybersecurity. OEMs and technology service providers may be guided by cyber-related regulatory requirements, but these providers may be hesitant to enhance cybersecurity via engineering changes to equipment or services without a compelling business case or overwhelming customer demand. According to one utility with significant wind energy assets, wind owners should conduct stringent vetting of OEM equipment for regulatory compliance or internal cybersecurity policy reasons before implementing equipment in wind plants. However, large vendors may still lack cybersecurity consideration in their software and firmware development practices, change management, or supply chain security; therefore, the vendors may be introducing new cyber threats to customers.[169] Additionally, because wind energy technology is part of a global market, U.S. wind owners may lack control of or full visibility into foreign wind vendors' and service providers' cybersecurity posture. Greater dialogue between vendors and customers about customers' cybersecurity needs and preferences can influence vendors to consider CIE for designing wind energy technologies, and potentially shift vendors' priorities for digital equipment from quantity and speed to quality and design.

7.5 Cybersecurity Exercises

It is recommended that, in addition to internal cybersecurity training, utilities, wind system operators, and wind system vendors participate in simulated cybersecurity exercises. These exercises would be similar to, or integrated with, (a) NERC GridEx exercises, (b) U.S. Cyber Command, DHS and Federal Bureau of Investigation Cyber Guard attack simulations,[170] or (c) the DOE/National Association of State Energy Officials energy cyber-preparedness exercise Liberty Eclipse.[171] Exercises can expose gaps in the defense of wind power networks prior to compromise by state-sponsored persistent threats or less organized actors. Wind systems could play the role of another attack vector for the U.S. power system because of the potential damage that can be done. The benefit of conducting these exercises is that unknown vulnerabilities in wind power equipment or distributed communications networks will be exposed prior to exploitation.

DOE's CESER continues to collaborate with E-ISAC and INL in hosting CyberStrike workshops for a growing number of participants in the U.S. electricity sector. CyberStrike engagements prepare staff and management to recognize and respond to a cyber incident impacting that targets ICS. The training offers attendees a hands-on, simulated demonstration of a cyber attack, drawing from technical elements of the 2015 and 2016 cyber incidents in Ukraine. CyberStrike is designed to challenge course participants to understand adversarial behavior in preparation for and execution of a cyber attack, and to defend against cyber attacks on the equipment routinely encountered within power generation systems and power distribution substations.[172] Much of this OT equipment is also found in wind energy facilities, but dedicated wind cybersecurity training workshops using the CyberStrike platform is needed.

DHS provides an extensive hands-on training called Industrial Control Systems Cybersecurity (301) in Idaho Falls, Idaho. The training focuses on understanding, protecting, and securing industrial control systems (ICSs) from cyber attacks, and includes a Red Team/Blue Team exercise conducted within an actual control systems environment.[173] Trainees learn about common vulnerabilities and the importance of understanding the environment they are tasked to protect. Learning the weaknesses of a system enables trainees to implement mitigation strategies and institute policies and programs that will provide the defense-in-depth needed to ensure a more secure ICS environment. In addition, the training provides the opportunity to network and collaborate with other colleagues from around the world that are involved in operating and protecting control system networks. Further, a successive 401-level course that will include more technical hands-on exercises is currently in development.

7.6 Incident Response

In the event of a cybersecurity incident, detection and appropriate response to the situation will help lead to quick mediation. NIST SP 800-61, "Computer Security Incident Handling Guide," discusses some of the standardized approaches to this response covering containment, eradication, and recovery. It is likely that integration and coordination with government agencies may be necessitated. In 2016, President Obama issued PPD-41, "United States Cyber Incident Coordination," for the coordination of the federal response.[174] The National Cyber Incident Response Plan describes the U.S. approach to cyber incidents and the roles for the private sector, local and state government agencies, and the federal government.[175] While the private sector will naturally be the primary responders, DHS offers assistance through NCCIC for affected entities and coordinates with federal agencies to initiate a unified response, facilitate restoration processes, and contact law enforcement to begin legal action.[176] Understanding the roles and responsibilities of each organization during a cybersecurity incident and the support provided by government organizations is important as wind energy systems become a major component of power system infrastructure. Ultimately, incident response coordination directly with DHS and DOE is recommended so that all members of the wind energy community may establish an effective wind-specific incident response capability.

7.7 Power System Contingency Planning

Due to the increased penetration of wind in the electricity market and the intelligence level of both these generating systems and the grid, communication and data transmission speed and capacity needs are exponentially increasing. Most communications and data transfers are achieved via wired connections or wireless networks, with bidirectional connections to the broader Internet. As with PV systems, this increases the vulnerability of wind, and a contingency plan needs to be considered that can provide critical reliability services and system response and recovery in case threat events occur.[177] Failure scenarios with a large portion of wind tripping off-line caused by common-node vulnerabilities should be studied.

The large-scale deployment of wind energy is transforming today's power grid. Communications systems are enabling utility system operators to interact with wind plants. As significant thermal generation capacity is

displaced, wind turbines will be required to provide critical reliability services, such as frequency and voltage regulation. Because many of these interactions will occur through communication channels including the open Internet, where additional cyber vulnerabilities come into play, there is a concern about cybersecurity and information protection. A key question is the extent to which vulnerabilities can compromise the ability of wind plants to provide critical reliability services and system response and recovery in case threat events occur. Grid operators should consider new types of N-1 failure scenarios. Instead of sizing the operating reserves based on system needs when the largest generator trips, failure scenarios can be studied in which common-mode vulnerabilities are exploited resulting in large portions of wind generation tripping off-line such as all turbines from a single vendor.

8 Conclusions

Based on the findings of this Roadmap, including observations about the state-of-the-art, current practices, and opportunities for further R&D in wind energy technologies (Table 4), the path forward in developing effective cybersecurity for wind involves all wind energy stakeholders. As illustrated in the Roadmap, one strategy that can help fulfill a cultivation and increase in stakeholder involvement is to promote a wind cyber culture that encourages information sharing among wind energy community stakeholders. To facilitate this information-sharing paradigm shift, the wind industry can invest in, partner in, and pursue the following mechanisms:

- **Research and develop better technologies, methods, and tools for wind energy cybersecurity.** Academia, research laboratories, and industry can research and productize new technologies to identify, protect, detect, respond, and recover from wind energy cybersecurity attacks. See Table 4 for more information.

- **Conduct routine cyber assessments**. Threat modeling and cyber vulnerability assessments for wind energy are an integral part of cybersecurity for the industry. Stakeholders cannot accurately define cyber risk without conducting assessments that provide a full view of the cyber threat landscape and wind sites' preparedness for adverse cyber events.

- **Participate in cyber-emergency response and other cyber preparedness exercises.** Wind industry personnel can reduce the risk of a cyber attack by participating in regular cybersecurity training. Additionally, as a best practice, stakeholders could participate in multi-role simulated cybersecurity exercises to prepare for an adverse cyber event.

- **Define cybersecurity roles and responsibilities within wind entities, and throughout industry.** Each wind stakeholder needs to accept responsibility for protecting their assets (downstream consumers) by demonstrating robust cybersecurity capabilities. However, stakeholders are not only wind owners and operators: OEMs, standards developers, government, and academia have an important role in developing cybersecurity measures and adopting best practices.

- **Develop robust, consistent cybersecurity programs at wind facilities.** Wind energy stakeholders can create and enforce internal policies and procedures that impose cybersecurity within their individual entities. These policies and procedures should thoughtfully consider, among other things, activities before, during, and after a cyber attack. These activities include creating cyber incident reports, teams, response plans, and system recovery procedures.

- **Further develop cybersecurity standards for wind energy technologies.** Currently, cyber-related standards for wind OT are underdeveloped. Wind stakeholders can work together to create standards that improve the overall cybersecurity posture of the wind sector. Stakeholders can also utilize

standardized methodologies (i.e., NIST SP 800-82) to improve the consistency of assessments. Establishing cybersecurity-specific wind working groups would increase the industry's focus on cybersecurity. Stakeholders could also consider supporting a wind facility certification process to ensure that each asset has a minimum level of protection.

- **Define and implement basic cyber hygiene.** Best practices include ensuring that personnel complete basic cybersecurity training and creating cyber asset lists and change management records. Having a full view of their cyber assets allows wind stakeholders to develop effective defensive and offensive methods to prevent and deter cyber attacks. Developing better means of communicating cyber threat and -vulnerability information would also aid in the development of cybersecurity best practices.

- **Develop and encourage participation in wind-specific cybersecurity information-sharing mechanisms.** Leveraging existing cybersecurity information-sharing programs in the energy sector is a good start, but the current and growing diversity of wind technology suggests that the wind industry may benefit from its own information-sharing platform in which more technologically-specific threat and vulnerability information can be shared. Wind energy does not currently possess an industry-specific cyber threat and -vulnerability sharing platform. Many stakeholders rely on myriad distinct cybersecurity information sources, such as commercial vendors and organizations such as AWEA and ESIG, but stakeholders are not receiving the entirety of relevant and critical cybersecurity information. The wind industry could create an industry-specific information-sharing platform or mechanism.

Addressing cyber risk in the wind industry requires continuous effort, as cybersecurity R&D efforts for wind energy continue to be defined and focused. Ultimately, only a wind energy owner can determine cyber risk for his or her own wind energy system. Communicating and collaborating on needs, findings, best practices, and lessons learned with others in the wind industry will help wind stakeholders identify methods and frameworks for quantifying cyber risk.

The roles of wind owners and operators, manufacturers and vendors, standards developers, academia, and research organizations cannot exist independently in the development of cybersecurity for wind energy. Effective wind cybersecurity requires that all stakeholders participate and communicate in its research, development, and implementation. Engendering and sustaining a collaborative environment among so many stakeholders may be challenging, but it provides the best opportunity to produce and capture the best ideas of all those with an interest in the success of wind energy.

The long-term vision of this Roadmap is that the combined efforts of wind energy stakeholders have designed, retrofitted, and operated wind energy systems for resiliency to cyber threat events, decreasing the potential impacts to turbine equipment and the power grid. To complement the primary efforts of the wind industry in the near term, other long-term efforts to fulfill this vision include the research and development of cyber-resilient wind plant designs; maintenance of testbeds; education for relevant government and private sector partners regarding wind energy technologies; continued R&D for intrusion detection and incident response; and establishing industry-specific guidelines for cyber incident reporting and post-incident investigations, as well as for cyber event response and recovery. Composed of these objectives and others, this roadmap effort will help serve as a common foundation from which future needs and innovations in wind energy cybersecurity can be explored and prioritized.

This Roadmap is centered around but beyond wind energy technology. For other critical infrastructures that share commonalities with wind, some of the Roadmap findings, best practices, and potential next steps could be generalized, adopted, or adapted for the best of their individual cybersecurity needs.

References

1 American Wind Energy Association. *AWEA U.S. Wind Industry Fourth Quarter 2019 Market Report*. 2019.

2 U.S. Energy Information Administration (EIA). "What is U.S. electricity generation by energy source?" Feb. 27, 2020. https://www.eia.gov/tools/faqs/faq.php?id=427.

3 U.S. Department of Energy, Office of Energy Efficiency & Renewable Energy. *2018 Wind Technologies Market Report*, by Ryan Wiser and Mark Bolinger. DOE/GO-102019-5191. August 2019. https://www.energy.gov/sites/prod/files/2019/08/f65/2018%20Wind%20Technologies%20Market%20Report%20FINAL.pdf.

4 U.S. Department of Energy, Wind Energy Technologies Office. "How Distributed Wind Works." https://www.energy.gov/eere/wind/how-distributed-wind-works.

5 U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy. *2017 Distributed Wind Market Report*, by Alice Orrell, Nik Foster, Scott Morris, Juliet Homer, Danielle Preziuso, and Eric Poehlmann. DOE/EE-1799. August 2018. https://www.energy.gov/sites/prod/files/2018/08/f54/2017_dwmr_081018.pdf?.

6 U.S. Department of Energy, Office of Energy Efficiency & Renewable Energy. *2018 Offshore Wind Technologies Market Report*, by Walter Musial, Philipp Beiter, Paul Spitsen, Jake Nunemaker, and Vahan Gevorgian. DOE/GO-102019-5192. August 2019. https://www.energy.gov/sites/prod/files/2019/08/f65/2018 Offshore Wind Market Report.pdf.

7 U.S. Department of Homeland Security. "CISA: Cyber + Infrastructure, Critical Infrastructure Sectors." Accessed October 1, 2019. https://www.dhs.gov/cisa/critical-infrastructure-sectors.

8 U.S. Department of Homeland Security, "CISA: Cyber + Infrastructure, Energy Sector." Accessed October 1, 2019. https://www.dhs.gov/cisa/energy-sector.

9 U.S. Department of Homeland Security, U.S. Department of Energy. Energy: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan (Redacted). May 2007. https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Energy_SSP_Public.pdf.

10 U.S. Department of Homeland Security, "CISA: Cyber + Infrastructure, Energy Sector." Accessed October 1, 2019. https://www.dhs.gov/cisa/energy-sector.

11 U.S Department of Energy. *Multiyear Plan for Energy Sector Cybersecurity: 2018–2020*. July 2018. https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf.

12 U.S Department of Energy. *Multiyear Plan for Energy Sector Cybersecurity: 2018–2020*. July 2018. https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf.

13 U.S Department of Energy. *Multiyear Plan for Energy Sector Cybersecurity: 2018–2020*. July 2018. https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf.

14 U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. "About Us." Accessed October 1, 2019. https://www.energy.gov/ceser/about-us.

15 U.S. Department of Energy, Office of Science. "Research Areas and Impact." Accessed October 1, 2019. https://science.osti.gov/sbir/Research-Areas-and-Impact#CESER.

16 U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. "About Us." Accessed October 1, 2019. https://www.energy.gov/ceser/about-us.

17 U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. "Cybersecurity Research, Development, and Demonstration (RD&D) for Energy Delivery Systems." Accessed September 30, 2019. https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and.

18 U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. 'Energy Sector Cybersecurity Preparedness." Accessed January 24, 2019. https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity.

19 U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy. "About the Office of Energy Efficiency and Renewable Energy." Accessed October 1, 2019. https://www.energy.gov/eere/about-office-energy-efficiency-and-renewable-energy.

20 U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy. "EERE Initiatives and Projects." Accessed October 1, 2019. https://www.energy.gov/eere/about-us/initiatives-and-projects.

21 U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy. "DE-FOA-0002071: Fiscal Year (FY) 2019 Wind Energy Technologies Office Funding Opportunity Announcement." Accessed October 1, 2019. https://eere-exchange.energy.gov/Default.aspx#FoaIdb3bff091-3531-4356-b234-d079118ccce3.

22 U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy. "DE-FOA-0002071: Fiscal Year (FY) 2019 Wind Energy Technologies Office Funding Opportunity Announcement." Accessed October 1, 2019. https://eere-exchange.energy.gov/Default.aspx#FoaIdb3bff091-3531-4356-b234-d079118ccce3.

23 U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy. "Wind Energy Technologies Office." Accessed October 1, 2019. https://www.energy.gov/eere/wind/wind-energy-technologies-office.

24 U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy. "Wind Energy Technologies Office Projects Map." https://www.energy.gov/eere/wind/wind-energy-technologies-office-projects-map.

25 U.S. Department of Homeland Security. "Mission." Last modified July 3, 2019. https://www.dhs.gov/mission.

26 U.S. Department of Homeland Security, National Cybersecurity and Communications Integration Center. "NCCIC ICS." Accessed October 1, 2019. https://www.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_NCCIC%20ICS_S508C.pdf.

27 U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. "Infrastructure Security Division." Accessed October 1, 2019. https://www.dhs.gov/cisa/infrastructure-security-division.

28 U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. "Industrial Control Systems." Accessed October 1, 2019. https://ics-cert.us-cert.gov/.

29 Cybersecurity and Infrastructure Security Agency. "National Risk Management Center." November 15, 2018. https://www.dhs.gov/sites/default/files/publications/NRMC%20100%20Days%20Fact%20Sheet%20201 81115_CISA%20v2.pdf.

30 Federal Energy Regulatory Commission. "About FERC." Last modified August 30, 2019. https://www.ferc.gov/about/about.asp.

31 Federal Energy Regulatory Commission. "Office of Energy Infrastructure Security (OEIS)." Last modified October 3, 2018. https://www.ferc.gov/about/offices/oeis.asp.

32 Federal Energy Regulatory Commission. "Cyber & Grid Security." Last modified August 27, 2019. https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp.

33 Federal Energy Regulatory Commission. "FERC Acts on Cyber Security Risks with New Supply Chain-Related Reliability Standards." News Release, October 18, 2018. https://www.ferc.gov/media/news-releases/2018/2018-4/10-18-18-E-1.asp#.XQKKE4JKg-V.

34 North American Electric Reliability Corporation. "Frequently Asked Questions." August 2013. https://www.nerc.com/AboutNERC/Documents/NERC%20FAQs%20AUG13.pdf.

35 North American Electric Reliability Corporation. "About NERC." Accessed September 30, 2019. https://www.nerc.com/AboutNERC/Pages/default.aspx.

36 North American Electric Reliability Corporation. "About NERC." Accessed September 30, 2019. https://www.nerc.com/AboutNERC/Pages/default.aspx.

37 North American Electric Reliability Corporation. "Critical Infrastructure Protection Committee (CIPC)." Accessed September 30, 2019. https://www.nerc.com/comm/CIPC/Pages/default.aspx.

38 North American Electric Reliability Corporation. "Critical Infrastructure Protection Committee (CIPC)." Accessed September 30, 2019. https://www.nerc.com/comm/CIPC/Pages/default.aspx.

39 North American Electric Reliability Corporation. "United States Mandatory Standards Subject to Enforcement." Accessed October 1, 2019. https://www.nerc.com/pa/Stand/Pages/ReliabilityStandardsUnitedStates.aspx.

40 North American Electric Reliability Corporation. "Electricity Information Sharing and Analysis Center." Accessed September 30, 2019. https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx.

41 North American Electric Reliability Corporation. "Electricity Information Sharing and Analysis Center." Accessed September 30, 2019. https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx.

42 U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. "Cybersecurity Risk Information Sharing Program (CRISP): Enhanced threat analysis with U.S. Intelligence insights for faster threat identification and mitigation." September 2018. https://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf.

43 North American Electric Reliability Corporation. "GridSecCon." Accessed October 1, 2019. https://www.nerc.com/pa/CI/CIPOutreach/Pages/GridSecCon.aspx.

44 North American Electric Reliability Corporation. "GridEx." Accessed September 30, 2019. https://www.nerc.com/pa/ci/cipoutreach/pages/gridex.aspx.

45 North American Electric Reliability Corporation. "GridEx." Accessed September 30, 2019. https://www.nerc.com/pa/ci/cipoutreach/pages/gridex.aspx.

46 The White House. *National Cyber Strategy of the United States of America.* September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

47 The White House. *National Cyber Strategy of the United States of America.* September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

48 The White House. *National Cyber Strategy of the United States of America.* September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

49 U.S Department of Energy. *Cybersecurity Strategy: 2018–2020*. July 2018. https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf.

50 U.S Department of Energy. *Cybersecurity Strategy: 2018–2020*. July 2018. https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf.

51 U.S Department of Energy. *Cybersecurity Strategy: 2018–2020*. July 2018. https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf.

52 U.S Department of Energy. *Cybersecurity Strategy: 2018–2020*. July 2018. https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf..

53 U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability. *Multiyear Plan for Energy Sector Cybersecurity*. March 2018. https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf.

54 U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability. *Multiyear Plan for Energy Sector Cybersecurity*. March 2018. https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf.

55 U.S. Department of Energy, Office of Energy Efficiency & Renewable Energy. *2018 Wind Technologies Market Report*, by Ryan Wiser and Mark Bolinger. DOE/GO-102019-5191. August 2019. https://www.energy.gov/sites/prod/files/2019/08/f65/2018%20Wind%20Technologies%20Market%20Report%20FINAL.pdf.

56 Karthikeya, Bhat, and Reiner Schütt. "Overview of Wind Park Control Strategies." *IEEE Transactions on Sustainable Energy*, vol. 5, no. 2 (April 2014): 416-422. DOI: 10.1109/TSTE.2013.2285392.

57 Ahmed, Mohammed, Yong Cheol Kang, and Young Chon Kim. "Modeling and simulation of ICT network architecture for cyber-physical wind energy system." Paper presented at the 2015 IEEE International Conference on Smart Grid Engineering, Oshawa, Canada August 2015. DOI: 10.1109/SEGE.2015.7324601.

58 Ahmed, Mohamed A., Minho Song, Jae-Kyung Pan and Young-Chon Kim. "Remote Monitoring with Hierarchical Network Architectures for Large-Scale Wind Power Farms." *Journal of Electrical Engineering and Technology* 10, no. 3 (2015): 1319-1327. DOI: 10.5370/JEET.2015.10.3.1319.

59 Kluge, Martin and Michael Danitschek. "Condition Monitoring Systems (CMS) in wind turbines." July 22, 2010. Accessed May 24, 2019. https://www.ifm.com/obj/ifm_wind_power_CMS_EN.pdf.

60 U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, Wind Energy Technologies Office. "Renewable Systems Integration." https://www.energy.gov/eere/wind/renewable-systems-integration.

61 Zabetian-Hosseini, Asal, Ali Mehrizi-Sani, and Chen-Ching Liu. "Cyberattack to Cyber-Physical Model of Wind Farm SCADA." Paper presented at the 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, D.C., October 2018. DOI:10.1109/iecon.2018.8591200.

62 Zabetian-Hosseini, Asal, Ali Mehrizi-Sani, and Chen-Ching Liu. "Cyberattack to Cyber-Physical Model of Wind Farm SCADA." Paper presented at the 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, D.C., October 2018. DOI:10.1109/iecon.2018.8591200.

63 Staggs, Jason, David Ferlemann, and Sujeet Shenoi. "Wind Farm Security: Attack Surface, Targets, Scenarios and Mitigation." *International Journal of Critical Infrastructure Protection* 17 (2017): 3-14. DOI:10.1016/j.ijcip.2017.03.001.

64 ICS-CERT. "XZERES 442SR Wind Turbine Vulnerability." Last modified August 27, 2018. https://ics-cert.us-cert.gov/advisories/ICSA-15-076-01.

65 ICS-CERT. "XZERES 442SR Wind Turbine Vulnerability." Last modified August 27, 2018. https://ics-cert.us-cert.gov/advisories/ICSA-15-076-01.

66 ICS-CERT. "RLE Nova-Wind Turbine HMI Unsecure Credentials Vulnerability (Update A)." Last modified August 27, 2018. https://ics-cert.us-cert.gov/advisories/ICSA-15-162-01A.

67 Yan, Jie, Chen-Ching Liu, and Manimaran Govindarasu. "Cyber Intrusion of Wind Farm SCADA System and Its Impact Analysis." Paper presented at the 2011 IEEE/PES Power Systems Conference and Exposition, Phoenix, Arizona, March 2011. DOI:10.1109/psce.2011.5772593.

68 Yan, Jie, Chen-Ching Liu, and Manimaran Govindarasu. "Cyber Intrusion of Wind Farm SCADA System and Its Impact Analysis." Paper presented at the 2011 IEEE/PES Power Systems Conference and Exposition, Phoenix, Arizona, March 2011. DOI:10.1109/psce.2011.5772593.

69 Shodan. “ICS Radar.” Accessed February October 1, 2019. https://ics-radar.shodan.io/.

70 Office of the Director of National Intelligence. *Worldwide Threat Assessment of the U.S. Intelligence Community*. January 29, 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

71 Office of the Director of National Intelligence. *Worldwide Threat Assessment of the U.S. Intelligence Community*. January 29, 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

72 FireEye. "Industry Brief: Utilities." FireEye Threat Intelligence. 2018. Accessed August 05, 2019. https://intelligence.fireeye.com/reports/18-00012169.

73 GE Renewable Energy. *1.5 MW Wind Turbine* (2009). Accessed August 30, 2016. http://geosci.uchicago.edu/~moyer/GEOS24705/Readings/GEA14954C15-MW-Broch.pdf.

74 Sobczak, Blake. “First-of-a-kind U.S. grid cyberattack hit wind, solar.” *Energywire*. October 31, 2019. Accessed November 20, 2019. https://www.eenews.net/energywire/2019/10/31/stories/1061421301.

75 North American Electric Reliability Corporation. *Lesson Learned: Risks Posed by Firewall Firmware Vulnerabilities*. Published September 4, 2019. Accessed November 20, 2019. https://www.eenews.net/assets/2019/09/06/document_ew_02.pdf.

76 North American Electric Reliability Corporation. Lesson Learned: Risks Posed by Firewall Firmware Vulnerabilities. Published September 4, 2019. Accessed November 20, 2019. https://www.eenews.net/assets/2019/09/06/document_ew_02.pdf.

77 Davidson, Ros. "AWEA 2018: Increase in Cyber Security Attacks 'inevitable', Expert Warns." *Windpower Monthly*. May 8, 2018. Accessed August 05, 2019. https://www.windpowermonthly.com/article/1464061/awea-2018-increase-cyber-security-attacks-inevitable-expert-warns.

78 "Episode 22: Mini-Stories: Vol 1." Interview by Jack Rhysider. Darknet Diaries (audio blog), September 15, 2018. Accessed August 5, 2019. https://darknetdiaries.com/episode/22/.

79 "Episode 22: Mini-Stories: Vol 1." Interview by Jack Rhysider. Darknet Diaries (audio blog), September 15, 2018. Accessed August 5, 2019. https://darknetdiaries.com/episode/22/.

80 Sobczak, Blake. "Grid Leaders Clear the Air around Russian Hacking." *Energywire*. August 1, 2018. Accessed August 05, 2019. https://www.eenews.net/stories/1060091819.

81 Sobczak, Blake. "Grid Leaders Clear the Air around Russian Hacking." *Energywire*. August 1, 2018. Accessed August 05, 2019. https://www.eenews.net/stories/1060091819.

82 Bennett, Cory. "Russian Hackers Have Infiltrated the US." *The Hill*. November 04, 2016. Accessed August 05, 2019. https://thehill.com/policy/cybersecurity/223266-report-russian-hackers-infiltrate-us.

83 Burke, Garance. "AP Investigation: US Power Grid Vulnerable to Foreign Hacks." *AP News*. December 21, 2015. Accessed August 05, 2019. https://apnews.com/c8d531ec05e0403a90e9d3ec0b8f83c2.

84 GE Renewable Energy. “Haliade-X Offshore Wind Turbine Platform.” Accessed July 30, 2019. https://www.ge.com/renewableenergy/wind-energy/offshore-wind/haliade-x-offshore-turbine.

85 Kovacs, Eduard. “Attackers Using Havex RAT Against Industrial Control Systems.” *Security Week*. June 24, 2019. https://www.securityweek.com/attackers-using-havex-rat-against-industrial-control-systems.

86 Overton, Thomas. “DHS Issues New Alert on ICS Malware.” *Power Magazine*. November 5, 2014. https://www.powermag.com/dhs-issues-new-alert-on-ics-malware/.

87 Johnson, Jay. *Roadmap for Photovoltaic Cyber Security*. 2017. SAND2017-13262. https://energy.sandia.gov/download/43738/.

88 Gorenc, Brian and Fritz Sands. *Hacker Machine Interface: The State of SCADA HMI Vulnerabilities.* Trend Micro. May 2017. https://documents.trendmicro.com/assets/wp/wp-hacker-machine-interface.pdf.

89 ICS-CERT. "XZERES 442SR Wind Turbine Vulnerability." Last modified August 27, 2018. https://ics-cert.us-cert.gov/advisories/ICSA-15-076-01.

90 ICS-CERT. "RLE Nova-Wind Turbine HMI Unsecure Credentials Vulnerability (Update A)." Last modified August 27, 2018. https://ics-cert.us-cert.gov/advisories/ICSA-15-162-01A.

91 Anderson, Robert and Joseph Price. "Cyber-Informed Engineering: The Need for a New Risk Informed and Design Methodology." Paper presented at the International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange, Vienna, Austria, June 2015. INL/CON-15-34244. https://inldigitallibrary.inl.gov/sites/STI/STI/6618307.pdf.

92 Anderson, Robert, Jacob Benjamin, Virginia Wright, Luis Quinones, and Jonathan Paz. *Cyber-Informed Engineering*. Idaho National Laboratory. March 2017. INL/EXT-16-40099. https://inldigitallibrary.inl.gov/sites/sti/sti/7323660.pdf.

93 Minimega. "Minimega: A distributed VM management tool." https://minimega.org/.

94 U.S Department of Energy. *Multiyear Plan for Energy Sector Cybersecurity: 2018–2020*. July 2018. https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf.

95 U.S. Department of Energy. Testimony of Assistant Secretary Karen S. Evans Office of Cybersecurity, Energy Security, and Emergency Response U.S. Department of Energy Before the Committee on Energy and Commerce. U.S. House of Representatives. July 12, 2019. https://www.energy.gov/sites/prod/files/2019/07/f64/7-12-19-Karen%20Evans-FT-HEC-Energy.pdf.

96 U.S. Department of Energy. Testimony of Assistant Secretary Karen S. Evans Office of Cybersecurity, Energy Security, and Emergency Response U.S. Department of Energy Before the Committee on Energy and Commerce. U.S. House of Representatives. July 12, 2019. https://www.energy.gov/sites/prod/files/2019/07/f64/7-12-19-Karen%20Evans-FT-HEC-Energy.pdf.

97 U.S. Congress. Senate. *Cybersecurity Information Sharing Act of 2014 (CISA 2014).* S.2588. 113th Cong., 2nd sess. Introduced in Senate July 10, 2014. https://www.congress.gov/bill/113th-congress/senate-bill/2588/text.

98 Boire, Liam D. "Energy Research at Idaho National Laboratory." *Idaho National Laboratory*. Prepared for the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability. INL/MIS-19-52482-Revision-0. February 2019. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_11091.pdf.

99 U.S. Department of Homeland Security. *National Cyber Incident Response Plan*. December 2016. https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

100 GE Renewable Energy. "Digital Wind Cyber Security from GE Renewable Energy." *General Electric*. Accessed October 16, 2019. https://www.ge.com/digital/sites/default/files/download_assets/GE-Digital-Wind-Cyber-Security-Brochure.pdf.

101 Siemens Industrial Cybersecurity. "Catalogue of Offerings." *Siemens*. Accessed October 16, 2019. https://assets.new.siemens.com/siemens/assets/api/uuid:630aca9f-fe0a-404c-a105-915295e8cc65/version:1560294066/cybersecurity-catalogue-of-offerings.pdf.

102 North American Electric Reliability Corporation. "CIP Standards." Accessed October 9, 2019. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

103 Cleveland, Frances. *IEC TC57 WG15: IEC 62351 Security Standards for the Power System Information Infrastructure*. International Electrotechnical Commission. June 2012. http://iectc57.ucaiug.org/wg15public/Public%20Documents/White%20Paper%20on%20Security%20Standards%20in%20IEC%20TC57.pdf.

104 Utility 2. (1 August 2019). Phone interview with C. Glenn.

105 Verizon. *2018 Data Breach Investigations Report, 11th Edition.* April 2018. https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf.

106 Dragos. *Year in Review: ICS Activity Groups and the Threat Landscape*, 2018. https://dragos.com/wp-content/uploads/yir-ics-activity-groups-threat-landscape-2018.pdf.

107 National Institute of Standards and Technology. *Special Publication 800-82 Rev. 2: Guide to Industrial Control Systems (ICS) Security*. May 2015. http://dx.doi.org/10.6028/NIST.SP.800-82r2.

108 Edison Electric Institute. "Cyber & Physical Security." http://www.eei.org/issuesandpolicy/cybersecurity/Pages/default.aspx.

109 U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. "Training Available Through ICS-CERT." Accessed October 1, 2019. https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT.

110 Utility 1, interviewee 2. (9 July 2019). Phone interview with C. Glenn.

111 National Cybersecurity and Communications Integration Center, Industrial Control Systems Cyber Emergency Response Team. *ICS-CERT Annual Assessment Report FY 2016*. 2016. https://www.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf.

112 U.S. Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. September 2016. https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

113 Obregon, Lucinda. "Secure Architecture for Industrial Control Systems." *The SANS Institute*. October 15, 2015. https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327.

114 Weber, Hazen. "Role-Based Access Control: The NIST Solution." *The SANS Institute*. December 13, 2003. https://www.sans.org/reading-room/whitepapers/sysadmin/role-based-access-control-nist-solution-1270.

115 Department of Homeland Security, Centre for the Protection of National Infrastructure. *Configuring and Managing Remote Access for Industrial Control Systems*. November 2010. https://www.us-cert.gov/sites/default/files/recommended_practices/RP_Managing_Remote_Access_S508NC.pdf.

116 Guiora, Amos N. "Cybersecurity: A Cooperation Model." *OpenMind*. Last modified September 30, 2019. https://www.bbvaopenmind.com/en/articles/cybersecurity-a-cooperation-model/.

117 Drinkwater, Doug. "Does a data breach really affect your firm's reputation?" *CSO Online*. January 7, 2016. https://www.csoonline.com/article/3019283/does-a-data-breach-really-affect-your-firm-s-reputation.html.

118 Guiora, Amos N. "Cybersecurity: A Cooperation Model." OpenMind. Last modified September 30, 2019. https://www.bbvaopenmind.com/en/articles/cybersecurity-a-cooperation-model/.

119 Wells, Linton II, Motohiro Tsuchiya, and Riley Repko. *Improving Cybersecurity Cooperation between the Governments of the United States and Japan*. Sasakawa Peace Foundation USA. February 2012. https://spfusa.org/wp-content/uploads/2017/02/Improved-Cybersecurity-cooperation.pdf.

120 Brumfield, Cynthia. "Congress steers clear of industrial control systems cybersecurity." *CSO Online*. March 14, 2019. https://www.csoonline.com/article/3365239/congress-steers-clear-of-industrial-control-systems-cybersecurity.html.

121 Pope, Thomas. "Supply chain threat to industrial control third-party compromise." *Dragos*. May 22, 2018, https://dragos.com/blog/industry-news/supply-chain-threats-to-industrial-control-third-party-compromise/.

122 U.S. Department of Energy, Office of Energy Efficiency & Renewable Energy. 2018 Wind Technologies Market Report, by Ryan Wiser and Mark Bolinger. DOE/GO-102019-5191. August 2019. https://www.energy.gov/sites/prod/files/2019/08/f65/2018%20Wind%20Technologies%20Market%20Report%20FINAL.pdf.

123 U.S. Department of Energy, Office of Energy Efficiency & Renewable Energy. *2018 Wind Technologies Market Report*, by Ryan Wiser and Mark Bolinger. DOE/GO-102019-5191. August 2019. https://www.energy.gov/sites/prod/files/2019/08/f65/2018%20Wind%20Technologies%20Market%20Report%20FINAL.pdf.

124 U.S. Department of Energy, Office of Energy Efficiency & Renewable Energy. *2018 Wind Technologies Market Report*, by Ryan Wiser and Mark Bolinger. DOE/GO-102019-5191. August 2019. https://www.energy.gov/sites/prod/files/2019/08/f65/2018%20Wind%20Technologies%20Market%20Report%20FINAL.pdf.

125 National Institute of Standards and Technology. "Cyber Supply Chain Best Practices." Materials used during *Best Practices in Cyber Supply Chain Risk Management Workshop*, Gaithersburg, M.D., October 2015. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Managements/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf.

126 National Institute of Standards and Technology. "Best Practices in Cyber Supply Chain Risk Management: Northrop Grumman Corporation Trusted, Innovative, World-Class Supply Chain." *U.S. Resilience Project.* 2015. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Northup_081615.pdf.

127 National Institute of Standards and Technology. "Best Practices in Cyber Supply Chain Risk Management: Cisco Managing Supply Chain Risks End-to-End." *U.S. Resilience Project*. 2015. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Cisco_071515.pdf.

128 National Institute of Standards and Technology. "Best Practices in Cyber Supply Chain Risk Management: Boeing and Exostar Cyber Security Supply Chain Risk Management." *U.S. Resilience Project*. 2015. https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-Boeing-Exostar-Case-Study.pdf.

129 National Institute of Standards and Technology. "Best Practices in Cyber Supply Chain Risk Management: Utility Sector Best Practices for Cyber Security Supply Chain Risk Management." *U.S. Resilience Project*. 2015. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Utility_093015.pdf.

130 Shackleford, Dave and Joshua Douglas. "Combatting Cyber Risks in the Supply Chain." *SANS Institute*. September 2015. https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252.

131 SAE International. "Standard ARP9134A: Supply Chain Risk Management Guideline." February 6, 2014.

132 National Electrical Manufacturers Association. "NEMA CPSP 1-2015: Supply Chain Best Practices." Document ID: 100742. June 25, 2015.

133 SAE International. "Standard AS5553A: Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria." August 26, 2014.

134 SAE International. "Standard AS5553B: Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition" September 12, 2016.

135 U.S. Department of Energy. "Federal Energy Regulatory Commission, 18 CFR Part 40, Supply Chain Risk Management Reliability Standards." *Federal Register* 83, no. 208 (October 26, 2018): 53992-53993. https://www.govinfo.gov/content/pkg/FR-2018-10-26/pdf/2018-23201.pdf.

136 Edison Electric Institute. “Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk Version 1.0.” March 2019.

137 North American Electric Reliability Corporation. “Security Guideline for the Electricity Sector: Physical Security.” June 20, 2012. https://www.nerc.com/comm/CIPC/Security%20Guidelines%20DL/Physical%20Security%20Guideline%202012-05-18-Final.pdf.

138 American Wind Energy Association. *AWEA U.S. Wind Industry Annual Market Report Year Ending 2018.* 2019.

139 American Wind Energy Association. *AWEA U.S. Wind Industry Annual Market Report Year Ending 2018.* 2019.

140 American Wind Energy Association. *AWEA U.S. Wind Industry Annual Market Report Year Ending 2018.* 2019.

141 Purdue Engineering. “Research and Education Programs in WIND energy Systems (WINDS).” *Purdue University*. Accessed October 1, 2019. https://engineering.purdue.edu/Wind.

142 Stanford Energy. “Wind.” Stanford University. Accessed October 1, 2019. https://energy.stanford.edu/research/renewable-energy/wind.

143 National Wind Institute. “NEI Spotlight.” *Texas Tech University*. Accessed October 1, 2019. http://www.depts.ttu.edu/nwi/.

144 University of Massachusetts Amherst. “Wind Energy Center.” Accessed October 1, 2019. https://www.umass.edu/windenergy/.

145 University of Massachusetts Lowell. “Center for Wind Energy.” Accessed October 1, 2019. https://www.uml.edu/research/wind-energy/.

146 Staggs, Jason, David Ferlemann, and Sujeet Shenoi. "Wind Farm Security: Attack Surface, Targets, Scenarios and Mitigation." International Journal of Critical Infrastructure Protection 17 (2017): 3-14. DOI:10.1016/j.ijcip.2017.03.001.

147 Zabetian-Hosseini, Asal, Ali Mehrizi-Sani, and Chen-Ching Liu. "Cyberattack to Cyber-Physical Model of Wind Farm SCADA." Paper presented at the 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, D.C., October 2018. DOI:10.1109/iecon.2018.8591200.

148 American Wind Energy Association. *AWEA U.S. Wind Industry Annual Market Report Year Ending 2018.* 2019.

149 American Wind Energy Association. *AWEA U.S. Wind Industry Annual Market Report Year Ending 2018.* 2019.

150 Utility 1, interviewee 2. (9 July 2019). Phone interview with C. Glenn.

151 Johnson, Jay. *Roadmap for Photovoltaic Cyber Security*. 2017. SAND2017-13262. https://energy.sandia.gov/download/43738/.

152 Electric Subsector Coordinating Council, Homepage, http://www.electricitysubsector.org/.

153 Electric Information Sharing and Analysis Center, Homepage, https://www.eisac.com/.

154 Johnson, Jay. *Roadmap for Photovoltaic Cyber Security*. 2017. SAND2017-13262. https://energy.sandia.gov/download/43738/.

155 U.S. Congress. House of Representatives. Subcommittee on Energy of the Committee on Energy and Commerce. *The Electricity Sector's Effort to Respond to Cybersecurity Threats.* 115th Cong., February 1, 2017.

156 Utility 1, interviewee 2. (9 July 2019). Phone interview with C. Glenn.

157 Utility 2. (1 August 2019). Phone interview with C. Glenn.

158 Light, M., Jeffrey Mauth. *Cybersecurity Risk Information Sharing Program (CRISP*). PNNL-SA-109415. April 2015.

159 Smith, Michael E. "Cybersecurity Risk Information Sharing Program (CRISP): Bi-Directional Trust." Presented at the 2016 RSA Conference, San Francisco, C.A. February 29-March 4, 2016.

160 North American Electric Reliability Corporation. "Security Guideline for the Electricity Sector: Threat and Incident Reporting Version 2.0." April 1, 2008. https://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=2CF9E4DE983F97C24EAABEC6C529064E?doi=10.1.1.184.5167&rep=rep1&type=pdf.

161 Hayden, Michael. "Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat." *Bipartisan Policy Center*. February 28, 2014. https://bipartisanpolicy.org/report/cybersecurity-electric-grid/.

162 Utility 2. (1 August 2019). Phone interview with C. Glenn.

163 Filkins, Barbara, Douglas Wylie. *SANS 2019 State of OT/ICS Cybersecurity Survey.* SANS Institute. 2019. https://www.sans.org/reading-room/whitepapers/analyst/2019-state-ot-ics-cybersecurity-survey-38995.

164 National Renewable Energy Laboratory. "NREL Workshop Convenes Industry Experts on Cybersecurity and an Evolving Grid." Accessed October 1, 2019. https://www.nrel.gov/esif/news-cybersecurity-workshop-2017.html.

165 U.S. Department of Energy. "Cyber Fire 15 / ICS International Hackathon." Accessed October 9, 2019. https://www.energy.gov/cio/events/cyber-fire-15-ics-international-hackathon.

166 National Renewable Energy Laboratory. "Smart Grid Educational Series." Accessed October 1, 2019. https://www.nrel.gov/esif/sges-webinars.html.

167 North American Electric Reliability Corporation. "GridSecCon." Accessed October 1, 2019. https://www.nerc.com/pa/CI/CIPOutreach/Pages/GridSecCon.aspx.

168 Johnson, Jay and Danish Saleem. "Distributed Energy Resource (DER) Cybersecurity Standards." Presented at the NREL Cyber Security & Resilience Workshop, Denver, C.O., October 9, 2017. https://www.nrel.gov/docs/fy18osti/70454.pdf.

169 Utility 2. (1 August 2019). Phone interview with C. Glenn.

170 U.S. Department of Defense. "Teams Defend Against Simulated Attacks in Cyber Guard Exercise." *U.S. Cyber Command*. July 5, 2017. https://www.defense.gov/News/Article/Article/1237898/teams-defend-against-simulated-attacks-in-cyber-guard-exercise/.

171 U.S. Department of Energy. "Liberty Eclipse Energy—Energy Assurance Exercise & Event, December 8–9, 2016." May 2017. https://energy.gov/sites/prod/files/2017/05/f34/LE%20FINAL%20Exercise%20Summary%201May2017_Public%20Doc.pdf.

172 Idaho National Laboratory. "Cyber Strike Workshop." February 18, 2018. https://www.inl.gov/wp-content/uploads/2018/02/18-50019_Cyber_Strike_Workshop_R0-2.pdf.

173 U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. "Training Available Through ICS-CERT." Accessed October 16, 2019. https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT#workshop.

174 The White House. "Presidential Policy Directive 41: United States Cyber Incident Coordination." July 26, 2016. https://fas.org/irp/offdocs/ppd/ppd-41.html.

175 U.S. Department of Homeland Security. *National Cyber Incident Response Plan*. December 2016. https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

176 U.S. Department of Homeland Security. "DHS Role in Cyber Incident Response." Accessed October 1, 2019. https://www.dhs.gov/sites/default/files/publications/DHS%20Cyber%20Incident%20Response%20Fact%20Sheet%20v15%20-%20508%20Compliant.pdf.

177 Johnson, Jay. *Roadmap for Photovoltaic Cyber Security*. 2017. SAND2017-13262. https://energy.sandia.gov/download/43738/.

This page intentionally left blank

U.S. DEPARTMENT OF
ENERGY

Office of
ENERGY EFFICIENCY &
RENEWABLE ENERGY

For more information, visit:
energy.gov/eere/wind

DOE/GO 102020 8441 • July 2020