U.S. DEPARTMENT OF ENERGY

EERE Cybersecurity Multiyear Program Plan

Report to Congress
October 2020

United States Department of Energy
Washington, DC 20585

(This page is left intentionally blank)

Message from the Secretary

I am pleased to provide you with the *EERE Cybersecurity Multiyear Program Plan*. This report describes Federal agency cybersecurity strategies and activities for operational technologies within the Office of Energy Efficiency and Renewable Energy (EERE). In addition, this report includes milestones to track progress toward identified goals.

This report is being provided to the following agencies and Members of Congress:

- **The Honorable Richard C. Shelby**
  Chairman, Senate Committee on Appropriations

- **The Honorable Patrick Leahy**
  Vice Chairman, Senate Committee on Appropriations

- **The Honorable Nita M. Lowey**
  Chairwoman, House Committee on Appropriations

- **The Honorable Kay Granger**
  Ranking Member, House Committee on Appropriations

- **The Honorable Lamar Alexander**
  Chairman, Subcommittee on Energy and Water Development
  Senate Committee on Appropriations

- **The Honorable Dianne Feinstein**
  Ranking Member, Subcommittee on Energy and Water Development
  Senate Committee on Appropriations

- **The Honorable Marcy Kaptur**
  Chairwoman, Subcommittee on Energy and Water Development
  House Committee on Appropriations

- **The Honorable Mike Simpson**
  Ranking Member, Subcommittee on Energy and Water Development
  House Committee on Appropriations

If you have any questions or need additional information, please contact me or Ms. Katie Donley, Deputy Director for External Coordination, Office of the Chief Financial Officer, at (202) 586-0176.

Sincerely,

Dan Brouillette

List of Acronyms

AMO	Advanced Manufacturing Office
ANSI	American National Standards Institute
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
BCF	Buildings Cybersecurity Framework
BTO	Building Technologies Office
CESER	Office of Cybersecurity, Energy Security, and Emergency Response
DCS	Distributed Control Systems
DDoS	Distributed Denial of Service
DER	Distributed Energy Resource
DHS	U.S. Department of Homeland Security
DHS	U.S. Department of Homeland Security, Industrial Control Systems Cyber
ICS/CERT	Emergency Response Team
DOE	U.S. Department of Energy
EDS	Energy Delivery Systems
EERE	Office of Energy Efficiency and Renewable Energy
EISA 2007	Energy Independence and Security Act of 2007
EPAct 2005	Energy Policy Act of 2005
EO	Executive Order
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
F-C2M2	Facilities Cybersecurity Maturity Model
FCF	Facilities Cybersecurity Framework
FEMP	Federal Energy Management Program
FY	Fiscal Year
GMI	Grid Modernization Initiative
HECO	Hawaiian Electric Company
HVAC	Heating, Ventilation, and Air Conditioning
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IT	Information Technology
MYPP	Multiyear Program Plan
OT	Operational Technology
PLC	Programmable Logic Controllers
PV	Photovoltaic
R&D	Research and Development
RD&D	Research Development and Deployment
SCADA	Supervisory Control and Data Acquisition
SETO	Solar Energy Technologies Office
VTO	Vehicle Technologies Office

Executive Summary

This report responds to legislative language set forth in the Energy and Water, Legislative Branch, and Military Construction and Veterans Affairs Appropriations Act, 2019 (H.R. 5895) Conference Report, page 149.

> *Within available funds for EERE, the conferees include not less than $20,000,000 to bring cybersecurity into early-stage technology R&D so that it is built into new technology for this effort to encompass all EERE programs. Within 180 days of enactment of this Act, the Department shall submit to the Committees on Appropriations of both Houses of Congress a multi-year program plan for this effort to encompass all EERE programs.*

The U.S. Department of Energy (DOE) Office of Energy Efficiency and Renewable Energy (EERE) has prepared this Cybersecurity Multiyear Program Plan (MYPP) to guide cybersecurity research and development (R&D) for EERE technologies. This MYPP aligns with the U.S. Department of Energy Cybersecurity Strategy[1] and with the DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Cybersecurity RD&D Investment Integration Plan. EERE supports the DOE operational structure to formalize coordination and execute our program offices implementation plans for cybersecurity as an active member of a cross-agency Working Group that formally integrates current and planned cybersecurity RD&D investments and ensures strategy alignment. Implementation will also be carried out in close coordination with other relevant governmental offices and agencies, such as the Department of Homeland Security (DHS) and the Department of Commerce's National Institute of Standards and Technology (NIST).

EERE's mission is to conduct early-stage energy research in the transportation, buildings, manufacturing, and renewable power sectors. Technologies developed by EERE are part of DOE's strategy to advance energy dominance and ensure a secure, reliable, resilient, affordable, and enduring supply of American energy. As EERE technologies become more affordable with corresponding market uptake, it becomes a mission priority to integrate these technologies into the Nation's energy systems.

The focus of EERE's early-stage research is to effectively integrate renewable generation at the bulk power and distribution levels, and to advance energy efficiency and storage technologies, as well as intelligent demand management in the buildings, manufacturing, and transportation sectors. Sensors and controls that are connected to communicate through the Internet or other information technology (IT) platforms are key to fully integrating EERE technologies to deliver on more affordable and efficient energy use. Many semiconductor devices for sensors, controls, and power electronics in EERE technologies are identical or very similar, so EERE must

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

address cybersecurity cohesively. A reliable and resilient energy supply depends on improving cybersecurity defenses and mitigating the cyber vulnerabilities of these technologies.

This MYPP supports the implementation of White House Executive Order (EO) 13800[2], which directs Federal agencies to support cyber risk management efforts for critical infrastructure, and to work with the energy sector to identify, protect, detect, respond, and recover from cyberattacks targeting energy infrastructure. It also utilizes the NIST Framework for Improving Critical Infrastructure Cybersecurity (the Framework)[3] as recommended by the EO to guide EERE's R&D activities, and will leverage other NIST standards and the investments of other Federal agencies.

All R&D discussed in this report will be planned and executed in coordination with CESER, DOE's designated lead on cybersecurity, to enhance synergy and mitigate duplication.

Current Situation

- EERE's offices develop operational technologies and systems ("EERE technologies") critical to all 16 of the Department of Homeland Security's critical infrastructures sectors[4].
- EERE and its stakeholders are addressing, and must continue to address, evolving cyber threats to secure these infrastructures.
- EERE's increased attention to cybersecurity is the result of recent advancements made in functionality and interoperability in EERE technologies that now make cybersecurity a more pressing issue. New technologies must be designed with cybersecurity as a requirement.
- Cyber threats targeting EERE technologies present an immediate risk to the integrity and availability of energy infrastructure and other systems critical to the Nation's economy, security, and well-being.

EERE's Strategy

- Support the goals of White House EO 13800, align with DOE's Office of Electricity and Energy Reliability Multiyear Plan (MYP) for Energy Sector Cybersecurity[5] and complement cyber strategies from DHS and the Department of Defense.

[2] White House Executive Order (EO) 13800. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.
[3] NIST Framework for Improving Critical Infrastructure Cybersecurity. https://www.nist.gov/cyberframework.
[4] Department of Homeland Security. https://www.dhs.gov/cisa/critical-infrastructure-sectors
[5] DOE's Office of Electricity and Energy Reliability MYP for Energy Sector Cybersecurity. https://www.energy.gov/sites/prod/files/2018/05/f51/DOE Multiyear Plan for Energy Sector Cybersecurity _0.pdf.

- Accelerate cybersecurity R&D to strengthen technologies and systems that are critical to transportation, buildings, renewable power, and manufacturing, which are increasingly interconnected and vulnerable.
- Empower EERE stakeholders to better identify, protect, detect, respond to, and recover from evolving cyber threats and vulnerabilities through R&D focused on cybersecurity.
- Facilitate robust engagement and partnership with industry, academic, and government stakeholders to ensure EERE's early-stage research accurately tracks the dynamic needs of operational technology cybersecurity without duplicating ongoing efforts.
- Provide a unified approach towards improving the cybersecurity of EERE technology, and support flexibility of focus at the technology office level to address the diversity of risk profiles:
    - *Renewable Energy*. EERE R&D has contributed to falling costs of renewable energy technologies and increased use in U.S. electricity generation. The long-term security and sustainability of this success requires increased cyber resilience of systems that are increasingly integral to our Nation's electricity infrastructure. New renewable energy technologies, such as advanced solar inverters, must be designed with cybersecurity as a requirement.
    - *Transportation*. Vehicles are increasingly connected through new communication capabilities and electrification requiring connection to the grid to enhance performance. However, malicious actors could exploit these capabilities to disrupt or deny normal operations and functionality of consumers, public fleets, electric-vehicle charging stations, and the electric grid.
    - *Manufacturing*. Digitization and automation have greatly increased the complexity and inherent risk of globally distributed cyber-physical supply chains in manufacturing. Advances in automation technologies, including sensors and controls, hold promise for increased performance, energy efficiency, and economic growth, but have also introduced new cyber vulnerabilities.
    - *Buildings*. With 350,000 Federal facilities, 5.5 million commercial buildings, and 118 million homes, connected devices and systems offer building owners, managers, and occupants increased performance, physical security, productivity, energy management options, and value across a host of products. Proliferation of these technologies presents new cyber threats and vulnerabilities to buildings and their business and residential occupants.
- Achieve the following goals and objectives across represented sectors and technology offices. This unified approach includes integrated projects that take advantage of synergies across these four sectors. EERE activities that map to the Framework's core functions are delineated by italics within the sub-bullets.

Goal 1: Accelerate Cyber Resilience R&D of EERE Operational Technologies

1.1 Improve cybersecurity defenses and resilience. Enhance EERE stakeholders' ability to *detect* and *protect* against cyber threats and vulnerabilities. Develop metrics and consequence analysis to prioritize future cyber resilient R&D opportunities.

1.2 Mitigate vulnerabilities. Improve capability to *respond* to threats and mitigate vulnerabilities in a timely manner. Identify actionable cyber defense capabilities for EERE stakeholders and validate solutions.

1.3 Next-generation cyber resilient technologies. Defend against evolving cyber threats by designing new EERE technologies with cybersecurity as a requirement, such as adaptive and self-healing technology solutions and systems resilient to cyberattacks.

Goal 2: Increase EERE Stakeholder Cybersecurity Awareness

2.1 Improve situational awareness. EERE stakeholders must improve their ability to *identify* critical EERE cyber technology threats, vulnerabilities, and defenses through R&D, training, assessments, adopting, and implementing cybersecurity risk management best practices.

2.2 Enhance EERE technology cybersecurity maturity. EERE stakeholders will research, develop, implement, and assess cybersecurity best practices to *protect* EERE technology, including cybersecurity maturity and tools.[6]

2.3 Identify opportunities for EERE stakeholder participation in cyber incident response exercises. Enhance understanding of EERE stakeholder cyber exercise requirements to advanced preparedness and ability to rapidly *recover* from cyberattacks, including incident response and recovery plans and engagement with appropriate sector-specific agencies (SSAs).

EERE's holistic and unified approach addresses these goals by investing in cybersecurity R&D and preparedness measures across its technology offices. Its R&D activities aim to mitigate common threats and vulnerabilities in hardware and software throughout its portfolio, including, but not limited to: power electronics, sensors, control systems, and information communication technology. These technologies are driving increased connectivity and interoperability of both new and legacy systems. Innovations made to secure machine learning algorithms for cyber analytics or converged legacy and smart system environments can be implemented in technologies across transportation, renewable power, buildings, and manufacturing sectors.

A holistic approach to the cyber challenge will also help better identify critical communications, device architectures, and associated cyber vulnerabilities across EERE's diverse portfolio. Stakeholders will be able to better develop and implement cyber best practices from other industries to drive future sector-specific or cross-cutting cyber R&D to achieve resilience.

[6] The common elements of existing frameworks and models will be used by EERE technology offices as appropriate, thereby ensuring a unified and coordinate approach; for example, the Federal Energy Management Program's Facilities Cybersecurity Maturity Model. https://facilitycyber.labworks.org/fc2m2.html.

Cybersecurity is a continuous process, not an end state. Realization of EERE's overall cybersecurity goals requires this MYPP to be accompanied by robust engagement and partnership with industry, academic, and government stakeholders. See Appendix C for an overview of each office's technological focus area in 2019.

EERE CYBERSECURITY MULTIYEAR PROGRAM PLAN

Table of Contents

Introduction

The U.S. Department of Energy's (DOE's) Office of Energy Efficiency and Renewable Energy (EERE)[7] invests in research and development (R&D) of technologies used in the generation, distribution, storage, and consumption of energy. The Department of Homeland Security (DHS) has warned of increasing cyberattacks targeting energy technologies and associated industrial control systems (ICS), which are essential to the operations of technology and systems across EERE offices ("EERE technologies").[8]

EERE technologies represent a large and diverse number of devices, equipment, and systems, but share common vulnerabilities across various aspects of Operational Technology (OT), which includes but is not limited to: ICS, supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures.[9] EERE focus areas include:

- *Power Electronics*. Power electronics have enabled new performance capabilities and are pervasive across EERE technologies, introducing hardware with various vulnerabilities in both new and legacy technologies.

- *Sensors, Control Systems, and Communications*. Advances in digitization, automation, and enterprise integration have contributed to the rapid progression and sophistication of EERE technologies. Often, greater efficiency or savings can be achieved by systems optimization enabled by sensors and controls even without the same devices being installed. However, the cyber-physical convergence of operational and

INTEGRATION REQUIRES CYBERSECURITY

Advances in functionality and interoperability within the transportation, manufacturing, buildings, and renewable power sectors have significantly impacted the demand profiles of the U.S. electric grid. EERE technology and system innovation will influence the grid of tomorrow by contributing to improvements to renewable bulk power technologies, energy storage, and intelligent load control.

Previously many of these technologies, equipment, and systems were non-connected to the Internet and thus had minimal cybersecurity vulnerabilities. Current EERE R&D integrates new functionalities and capabilities for enhanced flexibility and resiliency, which introduces cyber vulnerabilities that need to be continuously addressed.

[7] DOE's Office of Energy Efficiency and Renewable Energy. https://www.energy.gov/eere/office-energy-efficiency-renewable-energy.
[8] EERE is organized across 11 offices: Solar Energy Technologies Office, Wind Energy Technologies Office, Water Power Technologies Office, Geothermal Technologies Office, Bioenergy Technologies Office, Vehicle Technologies Office, Fuel Cells Technologies Office, Building Technologies Office, Advanced Manufacturing Office, Federal Energy Management Program, and the Weatherization and Intergovernmental Programs Office.
[9] National Institute of Standards and Technologies. May 2015. "Guide to Industrial Control Systems (ICS)." NIST Special Publication 800-82 Rev 2.

informational technologies represents potential new attack surfaces as some technologies have prioritized functionality over security.

- *Connectivity*. EERE technologies are increasingly internet- and grid-connected, bringing new opportunities for energy savings, agility to changing grid conditions, and consumer comfort – but also expanding the cyberattack surface.

- *Legacy Systems*. Operational equipment generally faces a much longer lifespan than information technology (IT) and lacks basic cyber defenses. Improving the cybersecurity of systems dependent on legacy equipment is difficult and costly.

EERE Cyber Strategy

The EERE R&D portfolio aims to reduce the threat of malicious actors exploiting vulnerabilities that would disrupt critical energy efficient and renewable energy infrastructures vital to our Nation's economy, national security, environment, and well-being. This EERE Cybersecurity Multiyear Program Plan (MYPP) outlines the approach, encompassing all EERE programs, to further bring **cybersecurity into early-stage technology R&D** so new technology is more cyber-resilient by design to better identify, protect, detect, respond to, and recover from cyber threats and vulnerabilities.

This MYPP aligns with DOE's Office of Electricity and Energy Reliability Multiyear Plan (MYP) for Energy Sector Cybersecurity[10][11], which discusses three overarching goals: 1) Strengthen energy sector cybersecurity preparedness; 2) Coordinate cyber incident response and recovery; and 3) Accelerate game-changing R&D of resilient energy delivery

MELTDOWN & SPECTRE

Publicly disclosed in January 2018, Meltdown and Spectre represent a class of wide-ranging vulnerabilities that affects nearly every computer chip manufactured in the last 20 years.

These hardware flaws allow malicious actors to bypass system security protections in a wide range of systems critical to EERE technologies and critical energy infrastructure, from industrial control systems used in advanced manufacturing to building automation.

Exacerbating the challenge, Meltdown and Spectre take advantage of a hardware flaw across multiple vendors and hardware manufacturers. DHS ICS-CERT has warned that software patches to protect against these vulnerabilities have had limited success in mitigating the threat. Solutions can also even severely reduce the capabilities required by EERE technologies and systems such as ICS/SCADA and building automation systems.

[10] DOE's Office of Electricity and Energy Reliability MYP for Energy Sector Cybersecurity. https://www.energy.gov/sites/prod/files/2018/05/f51/DOE Multiyear Plan for Energy Sector Cybersecurity _0.pdf.
[11] The DOE Office of Electricity and Energy Reliability responsibility for Energy Sector cybersecurity has transferred to the DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

systems. EERE's core mission is to support early-stage R&D, thus, the focus of its activities aligns with Goal 3.

EERE focuses on **early-stage research and development of innovative EERE technologies and tools** that prioritizes cybersecurity. Given the speed and rate at which cyber threats evolve, the second focus is on EERE **stakeholder preparedness and improved situational awareness** to inform R&D needs. This MYPP supports implementation of White House Executive Order (EO) 13800[12], which supports cyber risk management for critical infrastructure owners and operators.[13]

The Director of the EERE Federal Energy Management Program (FEMP) is leading the EERE efforts in cybersecurity and will continue to lead these implementation efforts. FEMP is the only office within EERE to have a dedicated security and resilience program; additionally, FEMP provides a convening role across and within the federal government to understand and address key energy and water cybersecurity challenges within federal facilities – many of which are addressed by technologies developed by EERE offices. FEMP's subjective and objective experience on cybersecurity provides a useful lens in which to view overall goals and progress towards integrating cybersecurity into EERE's programmatic activities. Integration across EERE ensures that lessons learned from cybersecuring R&D activities related to system components commonly found in operational technologies (OT) are coordinated to ensure efficient use of resources.

EERE plans to continue to work with industry, academic, and government partners to ensure that this MYPP is successfully accomplished. It will leverage existing activities from industry, like work currently being conducted by professional societies such as the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE), American National Standards Institute (ANSI), International Electrotechnical Commission (IEC), the Institute of Electrical and Electronic Engineers (IEEE), Society of Automotive Engineering (SAE) International, and others. These stakeholders also provide input back to EERE on key cybersecurity challenges and research needs.

EERE's Integration and Storage Priorities Require Cybersecurity

Grid modernization is increasing the digitization, automation, and complexity of energy infrastructure. As the cost of renewable energy technologies such as utility-scale onshore wind and photovoltaic solar fall, adoption has increased. EERE is working to improve grid integration

[12] White House Executive Order (EO) 13800. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[13] EO 13800 encourages Federal agencies to use the NIST Framework to address cyber risk while protecting critical infrastructures. EERE's activities map directly to the five Framework Core Functions (identify, protect, detect, respond, and recovery). This ensures that while EERE offices face diverse threats across technology and actors, EERE technologies will be better equipped to address, respond to, and recover from cyber threats.

to increase the flexibility of those and other generation, storage, and demand "resources" via cross-cutting initiatives such as the Grid Modernization Initiative (GMI)[14]. In addition, office-specific initiatives such as improving advanced power electronics from the Advanced Manufacturing Office and developing adaptive control technologies from the Building Technologies Office are critical to a future, more flexible grid.

EERE's portfolio-based approach to energy storage increases the reliability, resiliency, and diversity of the electric grid. The Energy Storage Grand Challenge takes a holistic view of energy storage technologies from next-generation battery technologies to electric vehicles[15], to energy-efficient, grid-interactive building technologies[16], to pumped storage hydropower, to Hydrogen at Scale[17].

EERE stakeholders face both consumption and generation cyber challenges. End users must simultaneously deal with the cyber-performance of systems that include technologies developed by EERE funded R&D interconnected with other devices, including those embodied in the Internet of Things (IoT).[18] The number of business that use IoT devices almost doubled between 2014 and 2019 and the worldwide number of IoT devices is expected to triple between 2018 and 2023 to 43 billion devices.[19] This increasing interconnectivity of technologies and devices increases their overall cyber vulnerability and the need to improve the cyber resilience of EERE developed technologies. This MYPP considers the overlapping vulnerabilities and solutions by utilizing a systems perspective on cybersecurity, recognizing that individual fixes will not successfully resolve all cybersecurity issues on their own.

Attention to state-of-the-art cybersecurity advances during the earliest stage of EERE research ensures alignment of innovations with broader cyber solutions. EERE R&D's focus on cybersecurity is the result of recent advancements that now make cybersecurity a more pressing issue. Cybersecurity is vital to EERE's priorities; without cyber-secure power electronics, communications, and connectivity, these technologies cannot be securely integrated into the broader energy system.

[14] The Grid Modernization Initiative (GMI) works across the U.S. Department of Energy (DOE) to create the modern grid of the future. Participating offices include EERE, the Office of Electricity and Energy Reliability, Office of Policy, and Office of Fossil Energy. https://www.energy.gov/grid-modernization-initiative.
[15] Next-Generation Electric Vehicles. https://www.energy.gov/eere/vehicles/batteries.
[16] Grid-interactive efficient buildings. https://www.energy.gov/eere/buildings/grid-interactive-efficient-buildings.
[17] Hydrogen at Scale. https://www.energy.gov/eere/fuelcells/h2scale.
[18] The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.
[19] McKinsey & Company. July 22, 2019. "Growing Opportunities in the Internet of Things." Accessible: https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things

EERE's Cyber Risk Landscape

DOE's Multiyear Plan for Energy Sector Cybersecurity details the growing cyber threat to the energy sector as reported by DHS's Industrial Control Systems Cyber Emergency Response Team. For the purposes of this MYPP, EERE defines threats, vulnerabilities, and risk as:

- **Threats** are any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service.[20]
- **Vulnerabilities** are a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.[21]
- **Risk** is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.[22]

EERE technology stakeholders' cybersecurity efforts often prioritize *availability* over *confidentiality* and *integrity*, whereas tradition IT cybersecurity efforts tend to focus on confidentiality and integrity of data. The prioritization of availability complicates cyber defense because of the reluctance to take systems offline temporarily for patching and other purposes. Cyber threats continue to target critical OT, including both energy delivery systems (EDS) and ICS, a general term that encompasses several types of control systems and associated instrumentation used for industrial process control. Ranging from building environmental controls (HVAC, lighting) to complex systems integral to electrical

EMERGING CYBER THREATS

In 2017, a research team from the University of Tulsa in Oklahoma demonstrated proof of concept attacks of wind turbines. These attacks exploited a combination of cybersecurity and physical security flaws to ultimately gain control of wind turbines within a farm.

Researchers were able to physically break into a wind turbine and plant a Raspberry Pi unit to gain remote access to the turbine's control network. By exploiting default user names and passwords with a control network that did not segment individual turbines nor require authenticated communications, researchers demonstrated their ability to send commands that could physically impact a turbine's activities. Malicious actors could utilize such vulnerabilities to cause wear-and-tear on the turbines or disable them entirely - potentially allowing them to hold wind farms ransom.

[20] National Institute of Standards and Technology. September 2012. "Guide for Conducting Risk Assessments." NIST SP 800-30 Rev. 1.
[21] Ibid.
[22] National Institute of Standards and Technology. April 2018. "Cybersecurity Framework Version 1.1".

power grid operations, ICS must meet numerous and often conflicting safety, performance, security, reliability, and operational requirements. The shared basis of ICS semiconductor devices creates a shared set of vulnerabilities, but the diversity of EERE technologies leads to diverse risks from these shared vulnerabilities. EERE sees the need to optimize the impact of efforts to address cybersecurity through a coordinated and cohesive strategy.

The increasing digitization, automation, and connectivity of critical EERE technologies has been accompanied by increased cyberattack surfaces and risks. According to a 2017 Pentagon report[23], "although progress is being made to reduce the pervasive cyber vulnerabilities of U.S. critical infrastructure, the unfortunate reality is that, for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructures." Increased connectivity of electricity infrastructure, alongside the simultaneous rise of high-computing systems and technologies requiring faster and more intense data exchange between critical energy systems, has dramatically increased the threat to national security.

Cyber risk to EERE technologies is difficult to quantify as the consequences of cybersecurity breaches do not scale linearly with time or frequency. Compromising a single Distributed Energy Resource (DER) node such as a wind turbine may not have a significant impact on the energy grid, however a coordinated attack could potentially have a cascading effect and disrupt regional electrical service. Similarly, if a critical building, such as a hospital or manufacturing plant loses power or operational control for an hour or less, the loss of life or production may be minimal, whereas a prolonged interruption could result in significant damages.

A few examples of common vulnerabilities across EERE technologies include, but are not limited to: SCADA utilities across systems in energy, manufacturing, water, locks and dams, etc. Distributed control systems (continuous process and manufacturing, etc.); Energy management, control and automation systems; Distributed energy resource management systems; various storage systems from pumped hydroelectric to bulk hydrogen energy storage systems; Intelligent transportation and electric vehicle charging infrastructure (EVs, EVSE, charging network operators, and aggregators).

Below are some of the major challenges facing EERE technology offices associated with identifying, detecting, mitigating, protecting, and responding to cybersecurity threats.

Detecting and Mitigating OT Cyber Vulnerabilities

There is a lack of adequate best practices, standards, tools, and technology to address OT cybersecurity vulnerabilities and preparedness. Many of these systems are owned and operated by individual customers and 3rd party operators. Stakeholders often lack basic

[23] 2017 Pentagon report. https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

cybersecurity awareness resources, metrics, monitoring, and defense capabilities. Attacks are often not detected because of a lack of monitoring, logging, and visibility of critical cyber assets. This presents a number of challenges to OT cybersecurity solutions for monitoring, protecting, and maintaining the security of these devices and their communications. It requires adoption of cybersecurity best practices across all stakeholders, including consumers, facility managers, operators, and third-party aggregators and enhancing the speed, accuracy, and effectiveness of threat detection and response capabilities.

Limited Cybersecurity Protection

Many of the systems that enable EERE technologies have limited computational, bandwidth, storage, and memory capabilities. This often limits the ability of devices to host cybersecurity solutions, such as monitoring and encryption that protect against cyberattack. These legacy devices may also lack availability of security patches, as equipment lifespan dramatically exceeds the refresh rate of consumer electronics (e.g., ICS expected lifetime of 10–20 years in the field whereas consumer electronics have a two- to five-year life span).

Identifying Cybersecurity Threats

Historically, control systems were pneumatic, analog, and not connected to the Internet. Today's EERE technology solutions often weave together networked sensors and cyber and physical systems, leading to increases in safety, efficiency, conservation, cost savings, interoperability, and integration of systems. However, the integration of IT and OT systems not only increases cyber threats and vulnerabilities, but also increases complexities and the difficulty in identifying threats. Securing these systems requires proactive cyber risk management and new operational processes that will allow managers, operators, and owners of EERE technologies to identify, understand, and mitigate cyber threats appropriately.

Workforce Lacking Resources

Traditionally, cybersecurity was the responsibility of IT personnel, such as chief information security officers. As operational technologies and information technology networks converge facility, energy, fleet, and control systems engineers and managers are increasingly being asked to respond to cybersecurity challenges. These new responsibilities are not accompanied by the necessary tools, technology, and workforce development to train and respond to a rapidly evolving cyber threat.

The number of cybersecurity experts has not kept up with demand. According to a 2018 $(ISC)^2$ study[24], there is a significant number of open cybersecurity-related positions, almost 500,000 in

[24] 2018 $(ISC)^2$ study. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0.

North America alone. With the 2018 U.S. Energy and Employment Report[25] reporting 3.2 million Americans worked in wind, solar, energy efficiency, and other clean energy jobs in 2017, it is likely that these sectors will be requiring additional cybersecurity experts to detect and manage risk.

[25] 2018 U.S. Energy and Employment Report. https://static1.squarespace.com/static/5a98cf80ec4eb7c5cd928c61/t/5afb0ce4575d1f3cdf9ebe36/1526402279839/2018+U.S.+Energy+and+Employment+Report.pdf.

MYPP Goal 1: Accelerate R&D of EERE Cybersecurity Operational Technologies

EERE intends to accelerate cybersecurity R&D, including next-generation research to create systems that can survive advanced cyberattacks without loss of operations. Achieving this goal requires the transition of innovative, early-stage research into capabilities that EERE stakeholders can incorporate into practice in the near-, mid-, and long-term to reduce cyber risk.

Key Challenges

Retrofit Solutions: Legacy systems and infrastructure within the EERE sectors are often installed with expectation of decade-plus lifespans, and correspondingly may lack the ability to encrypt data and receive security updates, for example due to lack of firmware capability (e.g. limited bandwidth or storage) or vendor support. Retrofitting existing technology to support defense against emerging cyber threats will require specialized attention and consideration.

Increasing Cyberattack Surface: Increased digitization, automation, and connectivity of EERE technology has increased the number of potential cyberattack vectors. Stakeholders need to be able to identify and limit cyber vulnerabilities within the technologies and systems they develop or manage to improve their ability to protect, detect, respond and recover. New systems must be developed with cybersecurity requirements and tested using adversary simulation activities to test penetration detection and response capabilities.

Continuation of Critical Functions: In the event of a cyberattack, operations of EERE technologies could be degraded or denied—reducing available energy and operation to critical facilities, sites, and the power grid. Next-generation technologies must continue EERE's core mission of improving energy efficiency, reducing cost, and improving performance, but must also be equipped with cybersecurity capabilities to minimize loss of critical function in the event of cyberattack.

VEHICLE THREATS

Cybersecurity vulnerabilities within the transportation sector add an additional element of risk – mobile connectivity. Research over recent years has revealed that malicious actors can utilize flaws in on-board communications systems to take control of vehicles – raising the possibility of fatal outcomes.

A parallel risk exists with the potential to exploit vulnerabilities within electric vehicle charging stations, which could spread quickly between vehicles, infrastructure, and the grid. Interference in this equipment could impact the car's charging ability, resulting in physically damaging the car from over-charging, manipulate grid demand from charging, or access driver personal and financial information.

EERE is conducting R&D to enhance existing cybersecurity and building cybersecurity requirements in to next-generation technology.

Objectives and Activities

Objective 1.1: Improve cybersecurity defenses

- **Develop detection tools:** EERE proposes to work with stakeholders to research and develop tools and technologies for EERE technology cyber threat detection. EERE plans to leverage other Federal efforts and public and private stakeholder existing efforts, case studies, and forums to expand stakeholder awareness and integrate with energy efficiency awareness.
- **Develop defensive tools:** EERE proposes to research and develop methods to enhance stakeholders' ability to defend against cyber threats. These methods will leverage lessons learned from other Federal and non-Federal efforts, as well as lessons learned from challenges in identifying cybersecurity threats. These methods will then lead stakeholders toward actionable mitigation responses.

Objective 1.2: Mitigate vulnerability

- **Validate EERE cybersecurity solutions**: EERE proposes to validate cybersecurity solutions across relevant cybersecurity frameworks to accelerate sector-wide improvements in EERE technology cybersecurity posture. This activity includes researching and validating sector-specific legacy equipment solutions.
- **Improve understanding of vulnerability:** EERE proposes to research and develop vulnerability assessments, helping stakeholders to quantify, evaluate, and test for the effectiveness and timeliness of different cybersecurity vulnerability mitigation technologies and strategies.
- **Develop response solutions:** EERE proposes to research response and mitigation methods to enable EERE stakeholders to proactively instrument and monitor systems for effective response and mitigation efforts. Stakeholders need to better understand which existing standards can be applied to specific EERE sectors, and which sectors might require new or validated standards.

Objective 1.3: Next-Generation Cyber Resilient Technologies

- **Conduct R&D for EERE cyber-physical interactions**: EERE proposes to research and develop EERE technology that improves its cybersecurity posture and resilience to cyberattack. EERE plans to focus on R&D on hardware and software solutions that remove or limit vulnerabilities in cyber-physical interactions, working to address vulnerabilities while limiting impact to energy performance.
- **Research adaptive and self-healing technologies**: EERE proposes to develop technologies that are adaptive and self-healing, designed and deployed with cybersecurity protections built-in that can be securely updated over time as threats evolve.
- **Research system resiliency to cyberattacks:** EERE proposes to invest in research to create next-generation systems that can survive a cyber assault with minimal loss of critical function.

Integrated Solutions

Leveraging Advanced Communications: Communications, sensing, and automation enable new system-level benefits from the integration of diverse energy resources and flexible grid components. Tools and methods must enable cyber analytics that leverage machine learning, and merge information streams and leverage threat intelligence to provide a more complete picture of advanced adversary activity. Developing more granular data for cyber analytics will improve EERE program coordination and advance cybersecurity solutions for the future integrated energy system.

Scalable Solutions to Wide-Scale Enhance Grid Flexibility: Enabling dynamic, automated, and cost-effective management of dispatchable energy generation supplies (e.g. wind and solar), demand response, and wide-scale energy storage on to the grid requires new hardware and software solutions that are scalable, interoperable, data-driven, and capable of real-time system monitoring, operation, and planning. It also requires the use of advanced sensor, communications, and data analytics technologies that allow grid operators to see, forecast, and optimize performance. The Solar Energy Technologies Office (SETO), for example, collaborated with the Hawaiian Electric Company to research potential opportunities for utilizing advanced photovoltaic (PV) inverters in high-penetration scenarios such as those seen in Hawaii. The research team developed new computer models, PV inverter testing methods, and updates to interconnection standards that helped maximize solar penetration and connect more consumers to the grid. As PV inverters offer potential new grid services, SETO is researching cybersecurity vulnerabilities of power electronics that could provide valuable insight to securing other distributed energy technologies.

Performance Targets

EERE cyber R&D success requires a holistic effort to develop cyber resilient policies, people, and technologies. This will be a continuous process, not an end state, to adapt to a complex, non-linear and evolving threats. Cyber resilient EERE technologies will be able to better identify, protect, detect, respond to, and recover from cyberattacks. Performance targets for EERE technologies critical to the renewable power, transportation, manufacturing, and buildings sectors, include but are not limited to:

- Critical function up-time improvements in cyber resilient technologies.
- Cost-reduction of cybersecurity detection and mitigation for new systems and legacy systems.
- Improved adoption rate of cybersecurity best practices and risk management as outlined in EO 13800.

EERE plans to leverage these measures of advances in cyber resilience while continuing to modernize and advance technology performance and efficiencies. EERE R&D will enhance both performance as well as the cyber resiliency of critical OT systems that incorporate power

electronics, programmable controllers, and other hardware common to EERE application sectors.

MYPP Goal 2: Increase EERE Cybersecurity Situational Awareness

EERE intends to increase stakeholder cybersecurity situational awareness to identify and protect EERE technologies from cyber threats and vulnerabilities. This work includes partnering with the private sector to conduct baselining activities for EERE technologies to help stakeholders understand the current state of their cybersecurity maturity as well as threats to their equipment and systems, publicizing existing resources to help mitigation, information sharing with other government stakeholders, and investing in new response capability research.

Common frameworks can be utilized across stakeholders to understand cybersecurity risks, vulnerabilities, and options for mitigation. Stakeholder engagement, via information resources, training, and public forums, will help improve situational awareness and enhance cybersecurity maturity among stakeholders and provide opportunities for feedback on needed EERE R&D.

Key Challenges

Variable Understanding of Vulnerabilities: EERE stakeholders need cyber assessments, tools, and training to facilitate adoption of cyber best practices to detect and respond to cyber threats. EERE stakeholders are not uniform in their understanding of the risks, so response solutions must accommodate which will require different levels of understanding.

Responding to Threats: Cyber incident response among EERE technologies may require a different set of skills, personnel, tools, and other resources than traditional energy and resource management. Incident response plans need to be regularly evaluated and updated to respond to a rapidly evolving threat. Some stakeholders may be well suited to participate in adversarial simulation activities and formal incident response exercises, but many are unaware of available resources, particularly from the broad range of Federal agencies addressing cyber issues.

Lack of EERE Stakeholder Cyber Situational Awareness: With rapid innovations in technology, there have been improvements in performance, cost, and functionality in EERE technology. However, cybersecurity awareness and preparedness have not

LAX SECURITY, REAL IMPACT

In 2016, a distributed denial of service (DDoS) attack targeted two Finnish apartment buildings' energy management systems. The attack impeded the heating controllers such that the heating never kicked in. Residents went without heat and hot water in sub-freezing conditions.

Building automation security tends to be lax or non-existent when building owners and operators are unwilling to make upfront security investments for operational technologies.

Building energy management systems are used in hospitals, commercial buildings, and Federal facilities; should someone take advantage of similarly lax cybersecurity the results could be devastating. Not only could hospital patients and caregivers be deprived of heat or hot water, but a malicious actor could potentially gain access and control of medical equipment and records, security, fire, power, and other critical networked systems.

kept pace, resulting in cybersecurity resource gaps that limit stakeholder ability to identify and respond to the evolving cyber threat.

Risk Evaluation and Vulnerability Assessments: EERE stakeholders need tools and resources to understand how to evaluate and prioritize vulnerabilities to cyber threats within their equipment, systems, buildings, and facilities. They need to be able to incorporate how they manage risk from cyber threats into a range of normal operating and business processes.

Objectives and Activities

Objective 2.1: Improve situational awareness

- **Improve ability to identify critical technology:** EERE proposes to collaborate with stakeholders, sharing information on methods and practices that improve the ability to identify cybersecurity vulnerabilities across critical infrastructure systems. Improved awareness should encompass common vulnerabilities across EERE sectors as well as vulnerabilities specific to focus area systems. Adversary simulation activities will identify common mode failures.
- **Develop EERE metrics:** EERE proposes to research risk measurement and consequence analysis to help quantify the associated value of cybersecurity technologies and practices and prioritize future R&D opportunities. EERE plans to partner with stakeholders to ensure metrics both strengthen EERE's cybersecurity research ecosystem and help identify and quantify sector-specific drivers for enhancing cybersecurity. Metrics should help stakeholders understand cyber risk and how solutions impact that risk.
- **Adopt cybersecurity risk management best practices:** EERE proposes to work to identify, develop, and disseminate publicly available resources to help stakeholders adopt cybersecurity risk management best practices. EERE plans to leverage existing guidance, develop new trainings, develop new guidance, and establish education and workforce development activities for EERE stakeholders and sector-specific stakeholders.

Objective 2.2: Enhance EERE technology cybersecurity maturity

- **Develop tools to protect EERE technologies:** EERE proposes to research, develop, implement, and assess best practices for implementing system and equipment protection. In coordination with stakeholders, EERE plans to identify and address gaps in EERE technology cybersecurity standards, validating and strengthening outdated, conflicting, or underdeveloped standards as appropriate. This will include research on testing frameworks and procedures to help standardize and quantify protection capabilities.
- **Develop cybersecurity maturity models:** EERE proposes to research and develop cybersecurity maturity models to help stakeholders evaluate, prioritize, and improve their cybersecurity capabilities by connecting security gaps with management actions.

EERE will leverage existing models, partner with relevant stakeholders, and customize models as necessary.

Objective 2.3: Identify opportunities for EERE stakeholder participation in cyber incident response exercises

- **Define exercise requirements:** EERE proposes to research and develop informational resources and guidance for stakeholders on when or how they should participate in formal incident response exercises, such as hack-a-thons, NERC's GridEx Security Exercise[26] or Liberty Eclipse[27].

Integrated Solutions

Controls and Communications: Control and communication systems are used across EERE technologies and represent a considerable source of vulnerability to cyberattacks. Better identifying critical communications technologies and their cyber vulnerabilities, developing network maps, and defining involved parties and best practices from other industries can help EERE understand the research needs for future sector-specific or cross-cutting communications R&D.

Best Practices: There are considerable cybersecurity resources and guidance developed across the Federal government and industry that can be leveraged for EERE stakeholders. For example, the Building Technologies Office (BTO) and FEMP jointly funded the development of the Buildings Cybersecurity Framework (BCF), which was later expanded by FEMP to become the Facilities Cybersecurity Framework (FCF)[28], to address cybersecurity in buildings across critical infrastructures by adapting the NIST Framework and other industry best practices for buildings stakeholders. The BCF and FCF provide guidance to facilitate building cybersecurity risk management efforts and increase an organization's cybersecurity posture by identifying security gaps and actionable guidance. EERE technology offices can develop similar frameworks for their specific sectors, building off the FCF model or lessons learned from its implementation. One particular area where integrated solutions can benefit all EERE offices is for coordinated vulnerability disclosures. When vulnerabilities are discovered or fixed, especially by third parties, it is important for relevant details to be shared as quickly as possible. However, which details are necessary and how to share them is equally important. Integrated development of best practices that leverages the industry specific expertise of all the EERE offices will help maximize the effectiveness of coordinated vulnerability disclosures.

[26] NERC's GridEx Security Exercise. https://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx.
[27] Liberty Eclipse. https://www.energy.gov/articles/national-cybersecurity-awareness-month-doe-conducts-cyber-attack-exercise-electricity-oil.
[28] Facilities Cybersecurity Framework (FCF). https://facilitycyber.labworks.org/.

Performance Targets

EERE technology systems critical to operations in the renewable power, transportation, manufacturing, and buildings sectors some potential cybersecurity R&D performance targets include, but are not limited to:

- Improved data monitoring to identify and protect from cyber threat and vulnerabilities.
- Identification rate of threats and vulnerabilities for critical EERE technologies.
- Implementation rates of cyber best practices and frameworks for EERE technologies.
- Prioritization effectiveness for research and development plans for the people, policies, and EERE technologies that are integral to critical infrastructures as outlined in the EO 13800.

Increasing cybersecurity situational awareness that identifies and protects EERE technologies from cyber threats and vulnerabilities will leverage common frameworks and best practices from industry, government, and across the EERE enterprise. Where risk profiles are unique to a given sector, EERE will engage with stakeholders to develop technology application specific resources. Development of evaluation metrics for cyber resilience of EERE technology cybersecurity will enable EERE to better prioritize future investments and advance cybersecurity R&D technology resilience and competitiveness.

Current Projects

EERE has several key efforts underway that will incorporate elements of this MYPP. Some of these projects address cyber directly, while others include a cyber "layer" or aspect as EERE conducts a project which addresses other priorities. Additionally, EERE will be placing particular focus on opportunities to partner within EERE, across DOE, and across the Federal government to more effectively leverage the collective Federal investment. The Fiscal Year (FY) 2019 commitment to cybersecurity is approximately $50M of FY 2019 appropriations which includes funding for projects such as:

Current Projects

- The Solar Energy Technology Office (SETO), in collaboration with CESER, is working to develop a Hawaii Solar Distributed Generation Cybersecurity Assessment. The project will assess cybersecurity vulnerabilities and mitigations of high solar and storage penetration electric distribution scenarios for the Hawaiian Electric Company (HECO) and deliver two reports that transfer the findings. Initial work includes gathering information sources that define the distribution scenarios evaluated, such as HECO's Power Supply Improvement Plan that has been approved by the Public Utilities Commission as a guide to achieve 100% renewable energy by 2045.

- The Vehicle Technologies Office (VTO) is working to identify and assess cyber physical security vulnerabilities and threats that exist in the interfaces between vehicles, chargers, and the grid. VTO is addressing critical vulnerabilities and threats to EV charging with R&D to enhance security, detection, and mitigation. Specific work includes projects funded for FY 2018, FY 2019 and FY 2020 a multi-year effort to develop a diagnostic security module to identify and isolate cyber threats in the charging process. This work complements projects launched in FY 2019 that are developing a real-time cyberattack and mitigation system that protects EVs, chargers, and the grid as well as developing hardware and software that is both resilient and hardened from a cyber-physical standpoint. R&D efforts also include game theory based moving target approaches to provide cyber physical security for EVs, extreme fast chargers, and the grid.

- FEMP is working to help **Federal facilities actively identify, prioritize, and mitigate the risks of cyber or physical attacks on facility-related control systems** while maintaining the required level of service for efficient operations. This work includes training on Federal facility cybersecurity vulnerability assessments and risk management; developing and validating a facilities cybersecurity framework (FCF) and facilities cybersecurity maturity model (F-C2M2); developing a technical and physical cybersecurity assessment framework specifically for controls systems in DERs; and developing an interactive training game to address the NIST SP-800-53 cybersecurity framework.

- Building on previous work to develop automated fault detection and diagnostics of building operations, in FY 2020 BTO funded research on **adaptive building controls as a use case for cybersecurity.** R&D activities include developing methods to evaluate effectiveness of building fault detection and diagnostic algorithms. Additionally, BTO seeks to develop and integrate threat detection capabilities of adaptive control algorithms into building automation systems.

- The Advanced Manufacturing Office (AMO) established a **Clean Energy Manufacturing Innovation Institute:[29] Cybersecurity in Energy Efficient Manufacturing**. This is the sixth Clean Energy Manufacturing Innovation Institute established by DOE. This effort, started in FY 2019, funds research to better understand the evolving cybersecurity threats to greater energy efficiency in manufacturing industries, developing new cybersecurity technologies and methods, and sharing information and expertise to the broader community of U.S. manufacturers. This will be complemented by the planned work on the cybersecurity of smart manufacturing systems, AMO's work to develop a manufacturing-specific cybersecurity maturity model, and manufacturing workforce development activities.

- GMI involves all the applied energy offices and focuses on working with public and private partners to develop new tools and technologies that measure, analyze, predict, protect, and control the grid of the future. In the **FY 19 GMI Lab Call**, DOE offices funded up to $40 million of research across five topic areas: resilience modeling; advanced sensors; energy storage; cybersecurity; and institutional support.

- FY 2019 funded projects from SETO Advanced Systems Integration for Solar Technologies (ASSIST) FOA (DE-FOA-0001987) aim to address the cybersecurity challenges from the integration solar photovoltaic (PV) systems. These projects will focus on the situational awareness of solar PV systems in strategic locations with considerations of cyber and physical vectors to ensure the electric power grid provides continuity of service to critical infrastructures in the face of wide spread and coordinated threats.

EERE Cybersecurity MYPP Milestones

The following milestones demonstrate the path forward and how EERE intends to measure progress in implementation of this MYPP. All milestones listed below are fully funded with FY 2020 and prior appropriations. Noted fiscal years report when a milestone is anticipated to be achieved. Additional milestones may be added pending future appropriations.

[29] Clean Energy Manufacturing Innovation Institute. https://www.energy.gov/eere/cemi/clean-energy-manufacturing-initiative-current-activities.

Objective 1.1: Improve cybersecurity defenses

- Milestone 1.1.1: Characterize vulnerabilities based in hardware components common to EERE technologies. (FY 2019)
- Milestone 1.1.2: Develop common components to real-time intrusion detection and mitigation tools for EERE technologies. (FY 2020)
- Milestone 1.1.3: Develop and validate real-time intrusion detection and mitigation tools for electric vehicle charging and solar arrays. (FY 2021)

Objective 1.2: Mitigate vulnerability

- Milestone 1.2.1: Quantify the potential vulnerabilities and threats for equipment and system technologies designed to deliver energy services in buildings. (FY 2019)
- Milestone 1.2.2: Complete end-to-end threat informed and consequence driven vulnerability assessment of electric vehicle/charging/grid interactions. (FY 2020)
- Milestone 1.2.3: Develop test method to evaluate effectiveness of building fault detection and diagnostic algorithms. (FY 2020)
- Milestone 1.2.4: Develop novel techniques that analyze anomalous network behavior or physical system responses to properly identify faults originating from a cyber-attack or malicious activity in order to properly isolate the fault and respond to an attack. (FY 2021)

Objective 1.3: Next-generation cyber resilient technologies

- Milestone 1.3.1: Demonstrate and integrate threat detection capabilities of adaptive control algorithms on building automation systems. (FY 2019)
- Milestone 1.3.2: Develop optimization-based control strategies that incorporate information on cyber-related faults, attack strategies, and vulnerabilities that can maintain continuity of operations with limited impact on energy efficiency and learn from faults to anticipate future attacks and responses. (FY 2020)
- Milestone 1.3.4: Develop deceptive capabilities that can mislead the attacker and reveal its presence to the control system to learn from and thwart off future attacks. (FY 2021)
- Milestone 1.3.5: Based on the results of the end-to-end vulnerability assessment (milestone 1.2.2), develop and evaluate cyber enhanced hardware and firmware for lectric vehicle charging systems. (FY 2021)

Objective 2.1: Improve situational awareness

- Milestone 2.1.1: Identify the potential vulnerabilities and threats for equipment and system technologies designed to deliver energy savings in buildings. (FY 2019)
- Milestone 2.2.2: Complete IAC assessments and reports including cybersecurity components. (FY 2019)

- Milestone 2.1.3: Identify current state-of-the-art best practices for implementing cybersecurity solutions through stakeholder engagement with building owners and energy managers. (FY 2020)
- Milestone 2.1.4: Provide technical assistance for validation of cybersecurity solutions applicable to legacy systems. (FY 2021)

Objective 2.2: Enhance EERE technology cybersecurity maturity

- Milestone 2.2.1: Define framework for hardware component cybersecurity reference architecture. (FY 2020)
- Milestone 2.2.3: Working with industry advisory groups, develop cybersecurity reference architecture for common hardware components and associated general systems. (FY 2020)
- Milestone 2.2.3: Working with industry advisory groups, develop and release cybersecurity reference architectures for electric vehicle charging, solar arrays, and interactions with the grid. (FY 2021)

Objective 2.3: Identify opportunities for EERE stakeholder participation in cyber incident response exercises

- Milestone 2.3.1: Define shared interests in cybersecurity of hardware components among EERE technology offices with other DOE offices, including CESER and OE. (FY 2019)
- Milestone 2.3.2: Develop draft standard for cyber incident response exercises based on common hardware components. (FY 2020)
- Milestone 2.3.3: Report on cyber incident response exercises utilizing draft standard. (FY 2021)

The below table illustrates how these projects map to the relevant MYPP objectives being accomplished. It is not intended to be a comprehensive portrayal of EERE's cybersecurity R&D portfolio.

Activity or Project	Goal 1: Accelerate R&D of EERE Cybersecurity Operational Technologies			Goal 2: Increase EERE Cybersecurity Situational Awareness		
	Obj. 1.1	*Obj. 1.2*	*Obj. 1.3*	*Obj. 2.1*	*Obj. 2.2*	*Obj. 2.3*
Opportunistic hybrid communications for distributed PV coordination	✓	✓	✓		✓	
R&D on tools, technologies, and techniques to secure, protect, detect, and mitigate cyber physical intrusions in the EV/EVSE/grid ecosystem guided by consequence driven threat assessments			✓			
Federal facility-related control system cybersecurity		✓		✓	✓	
Building fault detection and diagnostics for cyber intrusion, adaptive building controls for cybersecurity	✓	✓	✓			✓
Cybersecurity in energy efficient manufacturing, smart manufacturing systems, and manufacturing workforce development			✓	✓	✓	
Grid Modernization Initiative FY 2019 Lab Call: Cyber R&D topic area			✓			

Conclusion

Cyber threats targeting EERE technologies present an immediate risk to the integrity and availability of energy infrastructure critical to the Nation's economy, security and well-being. EERE technologies use common technologies and systems, such as power electronics and advanced communications, but their risk profiles can vary depending on the sector (renewable power, transportation, manufacturing, and buildings). The goals, objectives, and activities laid out here will help EERE and its stakeholders address a dynamic and evolving cyber threat.

This holistic plan guides EERE program offices and entities to accelerate cybersecurity R&D to strengthen technologies that are critical to our Nation's most critical infrastructures, transportation, buildings, renewable energy, and manufacturing. EERE's cybersecurity strategy aims to systematically research, develop, coordinate, and validate the tools and technologies necessary to reduce vulnerabilities and enhance the sector's overall cybersecurity posture and impose costs on our adversaries. As cyber threats evolve, this MYPP supports EERE programs' and sectors' review of new threats and vulnerabilities and incorporating them into early-stage R&D as appropriate. Achievement of the goals of the MYPP is a continuous process that aims for resilience against all hazards and requires extensive interaction with industry, academic, and government stakeholders.

Appendix A: References

Energy Futures Initiative and National Association of State Energy Officials. May 2018. "U.S. Energy and Employment Report." Accessed January 30, 2019: https://static1.squarespace.com/static/5a98cf80ec4eb7c5cd928c61/t/5afb0ce4575d1f3cdf9ebe36/1526402279839/2018+U.S.+Energy+and+Employment+Report.pdf

E.O. 13800, 82 FR 22391 (2017). "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Accessed November 1, 2018: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

U.S. Department of Energy. EERE FEMP Facilities Cybersecurity Maturity Model. Retrieved on February 12, 2019 at https://facilitycyber.labworks.org/fc2m2.html

Greenberg, Andy. June 28, 2017. "Researchers Found They Could Hack Entire Windfarms." *Wired*. Accessed November 28, 2018: https://www.wired.com/story/wind-turbine-hack/

International Information System Security Certification Consortium $(ISC)^2$. 2018. "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens." Accessed January 30, 2019: https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

Mylrea, M., & Gourisetti, S. N. G. (2017). Cybersecurity and Optimization in Smart "Autonomous" Buildings. In *Autonomy and Artificial Intelligence: A Threat or Savior?* (pp. 263-294). Springer, Cham.

National Institute of Standards and Technology. April 2018. "Cybersecurity Framework Version 1.1." Accessed December 1, 2018: https://www.nist.gov/cyberframework

National Institute of Standards and Technology. September 2012. "Guide for Conducting Risk Assessments." NIST Special Publication 800-30 Rev. 1.

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

North American Electric Reliability Corporation. "GridEx." Accessed January 14, 2019: https://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx

Stagg, Jason. July 26, 2017. "Adventures in Attacking Wind Farm Control Networks." Presented at *Black Hat USA 2017*. Accessed December 3, 2018: https://www.blackhat.com/docs/us-17/wednesday/us-17-Staggs-Adventures-In-Attacking-Wind-Farm-Control-Networks.pdf

U.S. Department of Defense, Defense Science Board. February 2018. "Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence." Accessed January 28, 2019: https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf

U.S. Department of Energy, Federal Energy Management Program. "EERE FEMP Facilities Cybersecurity Maturity Model." Accessed February 12, 2019: https://facilitycyber.labworks.org/fc2m2.html

U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability. March 2018. "Multiyear Program Plan for Energy Sector Cybersecurity." Accessed October 30, 2018: https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

U.S. Department of Energy, Wind Energy Technologies Office. August 2018. "2017 Wind Technologies Market Report." DOE/EE-1798. Accessed February 25, 2019: https://www.energy.gov/sites/prod/files/2018/08/f54/2017_wind_technologies_market_report_8.15.18.v2.pdf

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Agency. "Critical Infrastructure Sectors." Accessed November 1, 2018: https://www.dhs.gov/cisa/critical-infrastructure-sectors

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Agency. "Alert (ICS-ALERT-18-011-01) Meltdown and Spectre Vulnerabilities." Accessed February 13, 2019: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-18-011-01

U.S. Energy Information Administration. "What is U.S. electricity generation by source?" Accessed February 12, 2019: https://www.eia.gov/tools/faqs/faq.php?id=427&t=3

Appendix B: Statutory and Executive Authorities for Cybersecurity

In 2015, Congress assigned DOE as the Sector-Specific Agency (SSA) for cybersecurity for the energy sector, building upon previous Presidential directives. Within DOE, the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is the designated lead on cybersecurity. The following authorities establish and support DOE's role in cybersecurity for the energy sector:

Executive Order 13800 (EO 13800)[30], ***Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*** (May 2017), directs DOE and other Sector-Specific Agencies to examine how Federal authorities and capabilities can be better used to support the cybersecurity risk management efforts of critical infrastructure entities, particularly those assets designated at greatest risk under Section 9 of EO 13636. The order also directs DOE to work with DHS, the Director of National Intelligence, and other partners to assess U.S. readiness to manage a prolonged power outage due to cyberattack, and any gaps in assets or capabilities needed to mitigate potential consequences.

Energy Security provision within the Fixing America's Surface Transportation Act (FAST Act)[31] (December 2015) designates DOE as the SSA for cybersecurity for the energy sector and directs the Department to coordinate and collaborate with the U.S. Department of Homeland Security (DHS), other Federal agencies and departments, and owners and operators of critical electric infrastructure to carry out its SSA duties. The Act also amends the Federal Power Act to give the Secretary of Energy specific legislative authority to take emergency measures to protect or restore the reliability of critical electric infrastructure or defense critical electric infrastructure if the President identifies a grid security emergency. The Act also directs the Secretary to develop and adopt procedures to enhance communication and coordination between the public and private sectors to improve emergency preparedness, response, and recovery.[32]

Executive Order 13636 (EO 13636)[33], ***Improving Critical Infrastructure Cybersecurity*** (February 2013), directs the National Institute of Standards and Technology (NIST) to develop a framework to reduce cyber risks to critical infrastructure that consists of a voluntary set of standards, methodologies, procedures, and processes to address cyber risks. After the 2014

[30] Executive Order 13800. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.
[31] Energy Security provision within the Fixing America's Surface Transportation Act (FAST Act). https://www.govinfo.gov/content/pkg/PLAW-114publ94/pdf/PLAW-114publ94.pdf.
[32] DOE established the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to lead emergency preparedness and coordinated response to disruptions of the energy sector, including physical and cyberattacks, natural disasters, and man-made events.
[33] Executive Order 13636. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

release of the *NIST Cybersecurity Framework*[34], DOE worked in collaboration with energy sector owners and operators to develop the *Energy Sector Cybersecurity Implementation Guidance*[35], designed to help the energy sector establish or align existing cybersecurity risk management programs to meet the objectives of the NIST Cybersecurity Framework. Section 9 of the executive order also directs SSAs to designate critical infrastructure at greatest risk within each sector. DOE meets regularly with these designated energy entities to align and prioritize Federal cybersecurity capabilities and roles.

Presidential Policy Directive 21 (PPD-21)[36], ***Critical Infrastructure Security and Resilience (February 2013)***, designates DOE as the SSA for the energy sector and directs the Department to serve as the day-to-day Federal interface for energy infrastructure security and resilience, including dynamic prioritization and coordination of sector-specific activities; carrying out incident coordination responsibilities consistent with statutory authority, policies, directives, or regulations; and provide technical assistance and consultations to the sector to identify vulnerabilities and help prevent or mitigate the effects of incidents.

Presidential Policy Directive 8 (PPD-8)[37], ***National Preparedness*** (March 2011), is aimed at strengthening the security and resilience of the United States through systematic preparation for major national threats, including cyberattacks. PPD-8 builds on the National Response Framework (NRF), which describes how Federal support efforts are to be coordinated during emergencies. Emergency Support Function #12 – Energy Annex to the NRF (ESF-12), designates DOE as the lead Federal coordinator to facilitate the reestablishment of damaged energy systems and components for incidents requiring a coordinated Federal response.

Energy Independence and Security Act of 2007 (EISA)[38], Section 1301, establishes national policy for grid modernization to maintain a reliable and secure electricity infrastructure to meet future demand growth. The Act outlines cybersecurity requirements for the smart grid, including increased use of digital information and control technology to improve reliability, security, and efficiency; and the dynamic optimization of grid operations and resources with full cybersecurity. The Act also states that the smart grid shall have the ability to detect, prevent, communicate with regard to, respond to, or recover from system security threats, including cybersecurity threats and terrorism, using digital information, media, and devices.

[34] NIST Cybersecurity Framework. https://www.nist.gov/cyberframework.
[35] Energy Sector Cybersecurity Implementation Guidance. https://www.energy.gov/sites/prod/files/2015/01/f19/Energy Sector Cybersecurity Framework Implementation Guidance_FINAL_01-05-15.pdf.
[36] Presidential Policy Directive 21 (PPD-21). https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[37] Presidential Policy Directive 8 (PPD-8). https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.
[38] Energy Independence and Security Act of 2007 (EISA). https://www.congress.gov/bill/110th-congress/house-bill/6.

Appendix C: Cybersecurity Focus Areas by EERE Office

Office	2019 Cyber Focus Area
Geothermal Technologies Office	Research capabilities of increased rotor stability on a geothermal turbine to mitigate impacts of cyber and other incidents on a thermal energy storage system.
Solar Energy Technologies Office	R&D to protect solar assets, including developing technologies with protective measures that automatically recognize and warn operators of security breaches. Support the development and harmonization of cybersecure interconnection standards.
Water Power Technologies Office	Hydropower cybersecurity R&D targeted towards codifying non-standardized cyber systems (legacy electronics and diverse industrial control systems) and articulating the diverse set of cyberattack implications (agricultural, energy, flooding, municipal water supply). Marine and Hydrokinetic (MHK) R&D focused on providing actionable, industry-focused cybersecurity guidance on MHK cybersecurity (design cycle integration and desired security metrics) and documenting cyberattack ramifications as the industry matures into different markets (energy generation, power at sea, and resilient coastal communities).
Wind Energy Technologies Office	R&D for cyber-physical detection, response, and recovery for wind energy technologies, including vulnerability analysis and tools to improve cybersecurity defense and resilience for wind.
Bioenergy Technologies Office	Protect against sabotage of cyber communications and systems integrated throughout the operations of chemical facilities.
Fuel Cell Technologies Office	Identify and manage risks in power and fuel generation, fuel distribution, storage, and consumption.
Vehicle Technologies Office	R&D to detect, deter, protect, and prevent cyber threats to Electric Vehicles (EVs), Electric Vehicle Supply Equipment (EVSE), charging operators, and utility assets. This encompasses activities ranging from exhaustive assessment of possible threats to software and hardware-based hardening of EV infrastructure.
Advanced Manufacturing Office	R&D of new energy efficient technologies and practices for manufacturers to increase their cybersecurity capabilities, including precision manufacturing, cybersecurity gaps across EERE-relevant supply chains, and cybersecurity embedded in automation.

Building Technologies Office	R&D of network-connected control systems to develop optimization-based control solutions that integrate knowledge on cyber-related faults, cyberattack strategies, and vulnerabilities that can maintain continuity of energy efficient operations and are cyber-aware with deceptive capabilities to thwart future attacks.
Federal Energy Management Program	Improve Federal facility cybersecurity posture via tools, training, and technical expertise to actively identify, prioritize, and mitigate risks of cyber or physical attacks on facility-related control systems while maintaining required level of service for efficient operations.
Weatherization and Intergovernmental Programs Office	Raise awareness of cyberattacks with state and local partners, incorporating cybersecurity provisions in energy emergency assurance and response plans and comprehensive energy plans.

Appendix D: Converged Cyber and Physical Devices

EERE technologies converge cyber and physical devices, IT and OT from a wide range of systems that are increasingly integral to our Nation's electricity infrastructure, transportation systems and other critical infrastructures that underpin and support our economy, national security and well-being.