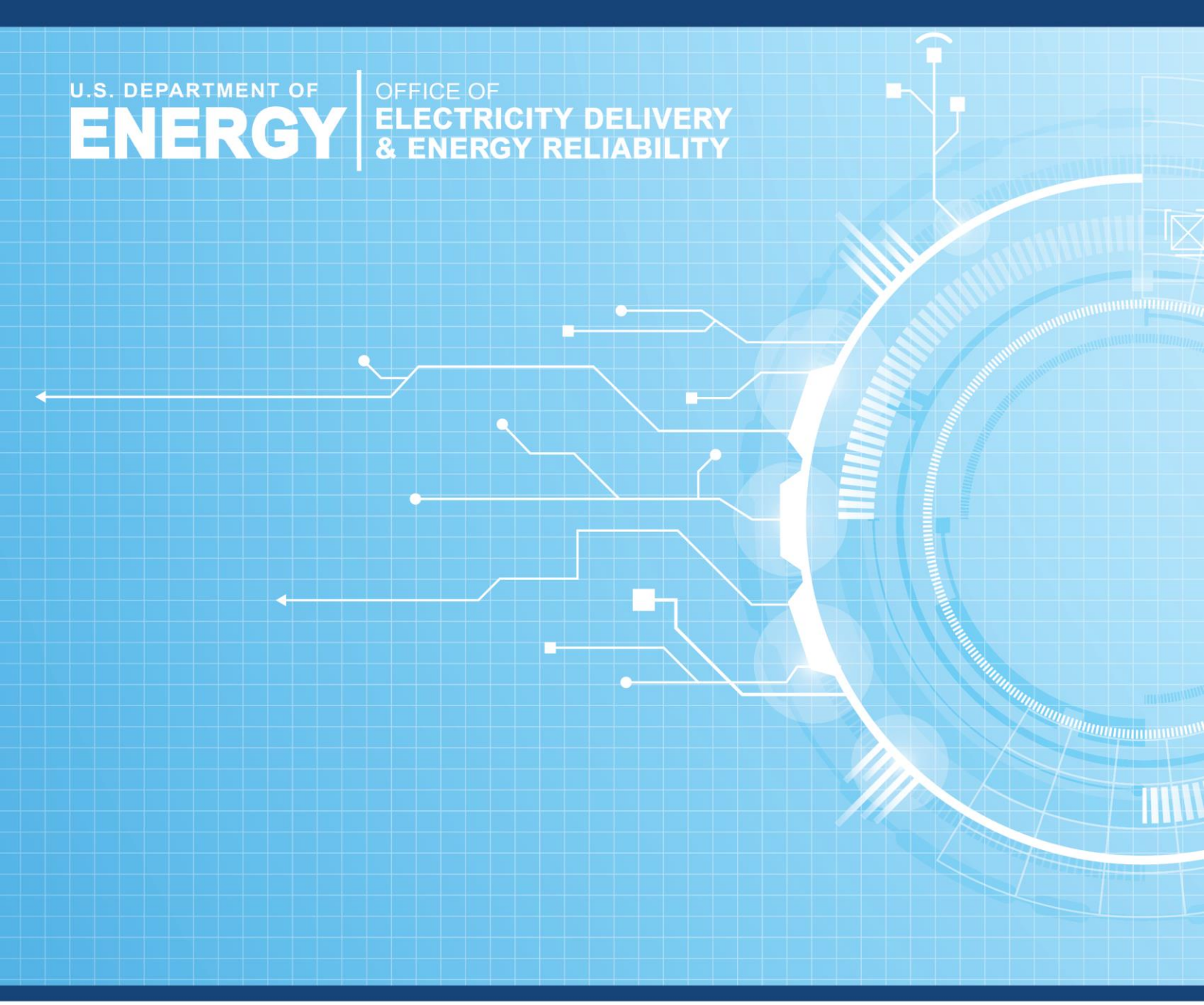


Multiyear Plan for Energy Sector Cybersecurity

MARCH 2018

Table of Contents

Letter from the Assistant Secretary

Protecting America's energy systems from cyber attacks and other risks is a top national priority. Reliable energy and power is the cornerstone of our advanced digital economy and is essential for critical operations in transportation, water, communications, finance, food and agriculture, emergency services, and more. Today, any cyber incident has the potential to disrupt energy services, damage highly specialized equipment, and threaten human health and safety. As nation-states and criminals increasingly target energy networks, the federal government must help reduce cyber risks that could trigger a large-scale or prolonged energy disruption.

The U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE OE) has prepared this ***DOE Multiyear Plan for Energy Sector Cybersecurity*** to improve cybersecurity and resilience of the nation's energy system. It lays out an integrated strategy to reduce cyber risks in the U.S. energy sector by pursuing high-priority activities that are coordinated with other DOE offices, and with the strategies, plans, and activities of the federal government and the energy sector.

This includes close alignment with the cybersecurity priorities of the 2017 *National Security Strategy* and with recommendations from private-sector executives in the National Infrastructure Advisory Council's 2017 *Securing Cyber Assets* study—both of which recognize that energy sector cybersecurity is imperative for national security and economic prosperity. The Multiyear Plan framework helps to align the efforts of government at all levels with those of energy owners and operators and key energy stakeholders in the private sector.

DOE OE recognizes that cybersecurity is a shared responsibility between the public and private sectors and has worked with the energy sector to enhance cybersecurity and resilience for more than 15 years. Our Plan priorities are guided by two industry-led efforts: the ***Roadmap to Secure Control Systems in the Energy Sector*** in 2006, and its subsequent update, the ***Roadmap to Achieve Energy Delivery Systems Cybersecurity*** in 2011. Although significant progress has been made toward Roadmap goals, much more needs to be done as new technologies are adopted and as threats to the energy sector become more sophisticated and pervasive.

The Plan identifies the goals, objectives, and activities that DOE will pursue over the next five years to reduce the risk of energy disruptions due to cyber incidents. It describes how DOE will carry out its mandated cybersecurity responsibilities as the Sector-Specific Agency and address the evolving security needs of energy owners and operators.

It establishes the guiding principles and strategic approach needed to drive both near- and long-term national cybersecurity priorities for DOE's support of the energy sector. The Plan supports implementation of Executive Order (EO) 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which directs DOE and other federal agencies to examine how federal authorities and capabilities can support cyber risk management for critical infrastructure owners and operators, and to work with the energy sector in assessing the grid's capabilities to manage and mitigate prolonged power outages resulting from cyber attack.

The Plan will provide a critical foundation to DOE's newly announced **Office of Cybersecurity, Energy Security, and Emergency Response (CESER)**, which will shift OE's cybersecurity and incident response activities to a new, dedicated office. The Plan outlines a game-changing strategy for DOE, informed by the energy industry's highest-priority needs, which can continue to be built upon by CESER leadership.

While the Plan outlines activities specifically for DOE, we look forward to conducting these efforts in close partnership with the energy industry and federal and non-federal partners throughout the nation.

Bruce J. Walker
Assistant Secretary
Office of Electricity Delivery and Energy Reliability
March 2018

Executive Summary

The nation's energy infrastructure has become a major target of cyber attacks over the past decade, with more frequent and sophisticated attacks that are increasingly launched by nation-states and cyber criminals. Despite ever-improving defenses, attackers have shifted their aim from exploitation to disruption and destruction. Today, a cyber incident has the potential to disrupt energy services, damage highly specialized equipment, and threaten human health and safety. This makes energy cybersecurity a top national priority that will require the federal government and the energy sector to work together to reduce cyber risks that could trigger a large-scale or prolonged energy disruption.

To address this priority, the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE OE) has prepared the ***DOE Multiyear Plan for Energy Sector Cybersecurity*** to improve cybersecurity and the resilience of the nation's energy system. The Plan aligns DOE's distinct roles and programs with the efforts of government, energy owners and operators, and key energy stakeholders, at all levels.

Current Situation

- Energy owners and operators have integrated advanced digital technologies to automate and control physical functions to improve performance and adjust to a rapidly changing generation mix. This has created a larger cyber attack surface and new opportunities for malicious cyber threats.
- The frequency, scale, and sophistication of cyber threats have increased, and attacks have become easier to launch. Nation-states, criminals, and terrorists regularly probe energy systems to actively exploit cyber vulnerabilities in order to compromise, disrupt, or destroy energy systems. Growing interdependence among the nation's energy systems increases the risk that disruptions might cascade across organizational and geographic boundaries.
- In response, the government and private sector continue to increase their spending on cybersecurity operations and maintenance. Despite improving defenses, it has become increasingly difficult for energy companies to keep up with growing and aggressive cyber attacks.

Critical Importance of Energy Sector Partnerships

- The public and private sectors share the responsibility to secure energy systems from cyber threats. Energy owners and operators have the primary responsibility to protect their systems from all types of risk. The federal government complements private-sector efforts to help reduce the risk that a cyber event could trigger a large-scale or prolonged energy disruption that impacts national and economic security.
- As nation-states and criminals increasingly target energy networks, the federal government provides leadership, guidance, technical expertise, and specialized information and resources to help the private sector protect its energy systems.

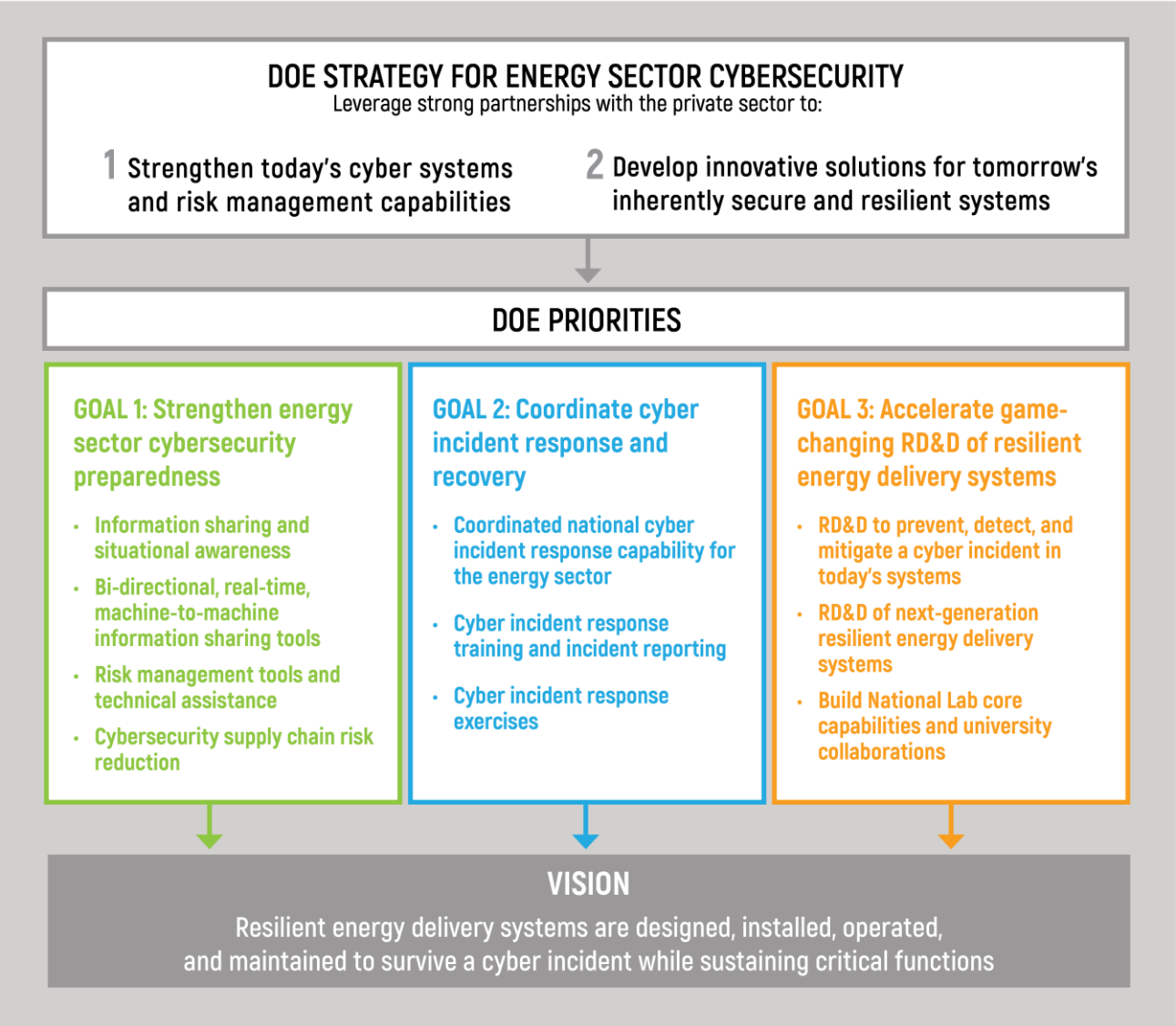
DOE's Strategy to Change the Game

- Anticipating and reacting to the latest cyber threat is a ceaseless endeavor that requires ever more resources and manpower. This approach to cybersecurity is not efficient, effective, nor sustainable in light of escalating cyber threat capabilities. We must recognize today's realities: resources are limited, and cyber threats continue to outpace our best defenses. To gain the upper hand, we need to pursue disruptive changes in cyber risk management practices.

- DOE's cyber strategy is two-fold: **strengthen today's energy delivery systems** by working with our partners to address growing threats and promote continuous improvement, and **develop game-changing solutions** that will create inherently secure, resilient, and self-defending energy systems for tomorrow.
- Meaningful public-private partnership is foundational to DOE's strategy. Facing an ever-evolving threat landscape requires a coordinated approach to improving risk management capabilities, information sharing, and incident response. The federal government has also historically funded innovative research, development, and demonstration (RD&D) that cannot be economically justified in private-sector markets. Today, this includes game-changing RD&D that will build cyber resilience into energy systems for tomorrow.

The ***DOE Multiyear Plan for Energy Sector Cybersecurity*** lays out this integrated strategy (see Figure 1) to reduce cyber risks in the U.S. energy sector. DOE's strategy aligns with Executive Order 13800, which directs federal agencies to use their authorities and capabilities to support the cyber risk management of critical infrastructure owners and operators.

Figure 1. DOE Multiyear Plan for Energy Sector Cybersecurity



The Plan is guided by the energy sector vision contained in the 2011 ***Roadmap to Achieve Energy Delivery Systems Cybersecurity***: *Resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions*. It complements the Roadmap by articulating DOE's distinct role and actions to enhance energy sector cybersecurity, working in partnership with the sector. DOE will implement the Plan in coordination with other federal agencies, state and local governments, and the private sector to unify the nation's efforts to achieve our shared vision.

OE will carry out DOE's mandated cybersecurity responsibilities and support the critical security needs of energy owners and operators by pursuing the following goals and objectives over the next five years:

Goal 1: Strengthen Energy Sector Cybersecurity Preparedness

- 1.1 **Enhance information sharing and situational awareness capabilities**: Define cyber situational awareness information needs and data; provide timely threat briefings and facilitate private-sector clearances; strengthen cyber preparedness among state/local stakeholders in energy assurance planning; and develop effective national and international partnerships.
- 1.2 **Develop and improve tools for bi-directional, real-time, machine-to-machine information sharing**: Grow energy sector participation in the Cybersecurity Risk Information Sharing Program (CRISP); expand CRISP capabilities to monitor, analyze, and share OT threat indicators; and develop a virtual crowdsourced malware forensic analysis platform.
- 1.3 **Strengthen sector risk management capabilities**: Update the Cybersecurity Capability Maturity Model (C2M2) and Risk Management Process (RMP); and work with electric cooperatives and public power utilities to foster a culture of security.
- 1.4 **Reduce critical cybersecurity supply chain vulnerabilities and risks**: Establish an energy delivery system testing and analysis capability.

Goal 2: Coordinate Cyber Incident Response and Recovery

- 2.1 **Establish a coordinated national cyber incident response capability for the energy sector**: Develop cyber incident response processes and procedures; and leverage technical capabilities to augment cyber mutual assistance.
- 2.2 **Conduct cyber incident response training and improve incident reporting**: Train emergency responders and update incident reporting processes.
- 2.3 **Exercise cybersecurity incident response processes and protocols**: Establish annual cyber incident response exercise program; and increase cyber exercises with non-federal government stakeholders.

Goal 3: Accelerate Game-Changing RD&D of Resilient EDS

- 3.1 **Research, develop, and demonstrate innovative tools and technologies to prevent, detect, and mitigate** a cyber incident in today's energy delivery systems and transition to the energy sector.
- 3.2 **Research, develop, and demonstrate game-changing cybersecurity tools and technologies** that: anticipate future energy sector attack scenarios and design cybersecurity into emerging energy delivery system devices from the start; and make future systems and components cybersecurity-aware and able to automatically prevent, detect, mitigate, and survive a cyber incident.
- 3.3 **Build strategic core capabilities** in the National Laboratories and **build university collaborations** dedicated to advancing cybersecurity for energy delivery systems.

Putting Goals and Objectives into Action

The DOE Plan is designed to achieve tangible, actionable improvements in energy sector cybersecurity where they are needed most. DOE has a robust portfolio of dozens of targeted activities and RD&D projects now underway to achieve the broad goals and objectives outlined in the Plan. Specific activities are described under each objective, and Appendix C presents past and current RD&D projects. Three selected examples below demonstrate how the Plan's goals and objectives translate into actionable projects that get results.

Goal 1: Strengthen Energy Sector Cybersecurity Preparedness

Objective 1.2: Develop and improve tools for bi-directional, real-time, machine-to-machine information sharing

CRISP (Cybersecurity Risk Information Sharing Program)

CRISP provides energy sector owners and operators with a **capability to voluntarily share cyber threat data in near-real-time, analyze this data using U.S. intelligence, and receive machine-to-machine threat alerts and mitigation measures**. Using technologies originally developed to defend DOE's networks, CRISP helps companies identify malicious traffic within their IT systems by analyzing the data streams and enhancing the analysis with classified DOE intelligence and cyber tools.

CRISP delivers cyber alerts and mitigations directly to affected companies and broadly to the energy sector. This voluntary program is now managed by the Electricity Information Sharing and Analysis Center (E-ISAC) with the goal to create a sustainable program owned and operated by the private sector enabling near real-time data sharing and analysis. **CRISP's 26 participating utilities account for 75% of U.S. electricity customers**.

This Plan includes activities to expand energy sector participation in CRISP and advance CRISP analysis capabilities through OE's Cyber Analytics Tools and Techniques (CATT) project. The Plan also seeks to expand CRISP capabilities to analyze and share threat indicators in *operational technology* systems by piloting real-time OT data sharing and analysis with four utilities in OE's Cybersecurity for the OT Environment (CYOTE) project.

Goal 2: Coordinate Cyber Incident Response and Recovery

Objective 2.1: Establish a coordinated national cyber incident response capability for the energy sector

Technical Capabilities to Augment Cyber Mutual Assistance

OE is working with the DOE National Laboratories to **develop an integrated mix of specialized cyber resources and capabilities that can be deployed during a cyber incident** to help energy companies identify and respond to a cyber attack. Each lab is expanding technical capabilities in specific topic areas to build an integrated Energy Cyber Resource Partnership. This partnership's robust incident response capability will support DOE's mandate to provide cyber-specific technical expertise and assistance to support energy sector response during a cyber incident and restore or maintain critical functions.

Goal 3: Accelerate Game-Changing RD&D of Resilient EDS

Objective 3.2: Research, develop, and demonstrate game-changing cybersecurity tools and technologies

Automated Defense Techniques for Next-Generation Systems

ABB is leading a research partnership to **enable high-voltage DC systems to detect and automatically reject commands that could destabilize the grid** if implemented. Using the physics of the grid, the capability will anticipate how the grid would react to a received command—rejecting commands that would jeopardize grid stability while executing legitimate commands in time. The project builds on a prior OE RD&D project, which successfully demonstrated the capability in transmission-level AC systems. This technology allows the grid to continue functioning during a cyber attack and prevent or limit energy disruption.

1. Introduction

Energy delivery systems form the backbone of America's infrastructure. Today's electric power grid and oil and natural gas distribution networks are tightly monitored and controlled using energy control systems to ensure reliable and continuous availability of electricity and fuels that nearly every aspect of American commerce and industry depends upon. This dependence has grown as businesses, homes, and communities increasingly integrate digital technologies and automated systems into virtually all facets of modern life.

> **"The risk is growing that some adversaries will conduct cyber attacks—such as data deletion or localized and temporary disruptions of critical infrastructure—against the United States in a crisis short of war."**
>
> — Daniel R. Coats, Director of National Intelligence, Worldwide Threat Assessment for the U.S. Intelligence Community, 2018

Energy control systems are specially designed digital systems that operate real-time physical processes by dispatching commands to millions of nodes and devices dispersed across the energy delivery infrastructure. These systems exchange massive amounts of data at high speeds over cyber networks to monitor and control physical devices such as transformers, switches, compressors, pumps, and valves. This makes data availability and integrity of paramount importance to energy operations.

Energy Control OT Systems ≠ Business IT Systems

- OT systems must be able to survive a cyber incident while sustaining critical functions. Real-time operations are imperative; latency is unacceptable.
- Power systems must operate 24/7 with high reliability and availability; no down time for patching/upgrades.
- Some OT components do not have enough computing resources to support additional cybersecurity capabilities needed for the energy OT environment.
- Energy OT components are widely dispersed and located in publicly accessible areas where they are subject to physical tampering.

Energy control systems operate within the operational technology (OT) environment. In the past, they were largely isolated from the internet and the company's information technology (IT) systems. However, in today's modern energy systems, OT and IT systems are connected, allowing cyber attacks to originate in business systems and migrate to operational systems. For example, the 2015 cyber attack on Ukrainian electric utilities originated as a spear phishing attack on utility IT systems (see box).

Energy companies increasingly integrate their physical and cyber systems and install digital devices, such as smart meters and smart sensors, throughout their infrastructure. This extensive network of new digital devices provides stronger security capabilities, but is also more accessible and exposes energy delivery systems to potential harm from accidental and malevolent cyber events. But unlike attacks on business IT systems, cyber attacks on energy control systems have the potential to disrupt power or fuel supplies, damage highly specialized equipment, and threaten human health and safety.

Cyber Attacks on the Ukrainian Power Grid

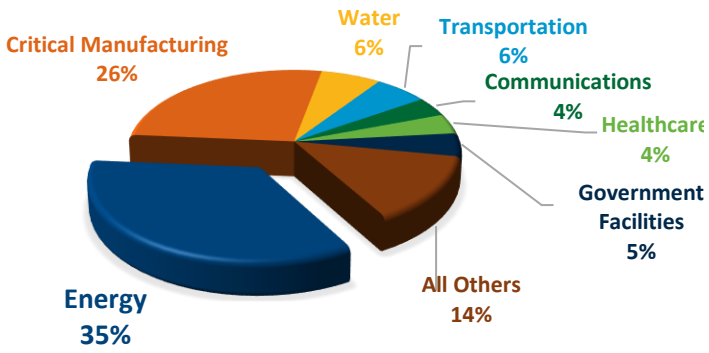
On December 23, 2015, hackers attacked three different electric utilities, resulting in power loss for 225,000 customers for several hours. Attackers used spear phishing emails to gain access to the IT networks. Once inside, they stole credentials using keystroke loggers, identified hosts and devices, and hijacked the distribution management system to systematically open breakers and cause a power outage. Attackers accessed the industrial control system (ICS) network through the virtual private network (VPN) and disabled the uninterruptible power supply, disabled operational control systems, disabled computers, and prevented infected computers from rebooting.

A year later, attackers used similar, more proficient, malware to target a remote power transmission facility and cause an outage lasting about an hour. Though relatively small in scale, these successful attacks show the attackers' ability to perform long-term reconnaissance operations needed to execute a highly synchronized, multisite attack.

The Cyber Risk Landscape

The energy sector has become a prime target for cyber attacks in recent years. Although reliable data is hard to come by, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reports that the energy sector experienced more cyber incidents than any sector from 2013 to 2015, accounting for 35% of the 796 incidents reported by critical infrastructure sectors (see Figure 2).[1] However, most cyber incidents are never reported publicly.

Figure 2. Critical Infrastructure Cyber Incidents Reported to DHS ICS-CERT (2013-2015)



Despite the sector's ever-improving defenses, the variety of threat actors and methods of attack are expanding, while the impact of incidents has evolved from exploitation to disruption to destruction. A 2015 survey of 150 IT professionals in the energy sector, conducted by Tripwire, showed that more than 75% of energy companies reported an increase in successful cyber attacks in the previous 12 months, with many reporting increases of 50% or more.[2] Yet as little as 20% of respondents reported they were confident that their organization could detect all cyber attacks, implying that many incidents go undetected. In a 2016 survey of 200 energy security professionals, Tripwire reported that more than 80% of respondents believed a cyber attack would cause physical damage to critical infrastructure in 2016.

"It's tempting to believe that this increase in attacks is horizontal across industries, but the data shows that energy organizations are experiencing a disproportionately large increase when compared to other industries."

—Tim Erlin, director of IT security and risk strategy for Tripwire, 2016

Defending against cyber risks grows more expensive each year. A 2015 study by the Ponemon Institute[3] estimates the annualized cost of cyber crime for an average energy company to be more than $27 million (see Figure 3). Estimates of control system security costs for the electric transmission and distribution equipment market range from roughly $150 million to as much as $800 million.[4] Simply put, the cost of preventing and responding to cyber incidents in the energy sector is straining the ability of companies to adequately protect their critical cyber systems.

[1] ICS-CERT, a component of the Department of Homeland Security, collects data on cyber incidents that attempt to gain access to both business and control systems infrastructure. These incidents, reported on a voluntary basis by critical infrastructure owners and operators, include unauthorized access to SCADA devices, exploitation of zero-day vulnerabilities in control systems devices and software, malware infections, SQL injection via exploitation of web application vulnerabilities, network scanning and probing, lateral movement between network nodes, targeted spear-phishing campaigns, and strategic web site compromises. Data from ICS-CERT's *Year in Review* for 2013, 2014, and 2015. The 2016 *Year in Review* reported 290 critical infrastructure incidents, but does not include a breakdown by sector.

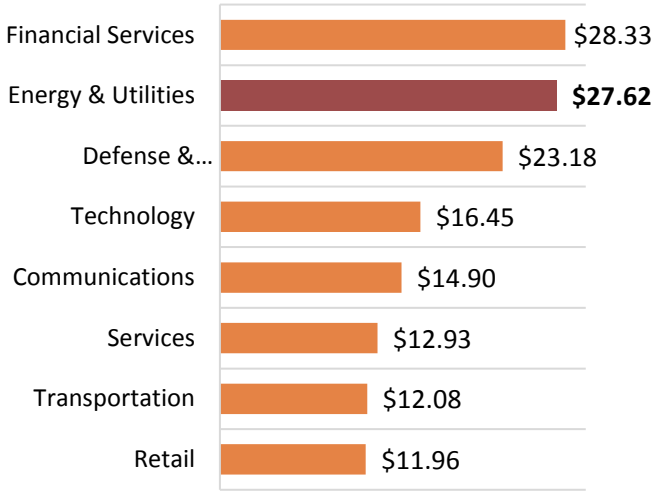
[2] Tripwire, *Energy Sector Sees Dramatic Rise in Successful Cyber Attacks*, 2016.

[3] Ponemon Institute, *2015 Cost of Cyber Crime Study: United States*, 2016.

[4] Newton-Evans Research Company, *Overview of the 2014-2016 U.S. Transmission and Distribution Equipment Market,* 2014.

The growing sophistication and effectiveness of recent intrusions mark a turning point to an era of politically motivated and nation-state-level targeting of U.S. energy infrastructure. In recent years, the energy sector has seen a dramatic increase in focused cyber probes, data exfiltration, and malware developed for potential attacks. The Director of National Intelligence reported in 2015 that security studies indicated Russian cyber actors were developing means to remotely access industrial control systems.[5] A December 2015 attack on three Ukraine power companies marked the first publicly acknowledged cyber attack to disrupt power.

Figure 3. Average Annualized Cost of Cyber Crime by Industry Sector in 2015 ($ millions)



Meanwhile, several emerging trends are rapidly re-shaping the energy sector and making digital control more complex. Utilities are rapidly modernizing the energy grid, adding advanced digital sensors and controls to operate the grid more efficiently; connect distributed energy resources ranging from electric vehicles to batteries and solar panels; increase customer participation and demand response; and integrate with other smart gas, water, and transportation infrastructure as Internet of Things technology proliferates. Electricity generation and the natural gas infrastructure also grow increasingly interdependent.

The rapid pace of technology and market changes in the energy sector make it even more challenging to secure cyber systems and ensure the reliable delivery of energy. This is particularly true in the electricity sector, which requires high-speed, accurate control of complex transmission and distribution systems. While the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) enforce mandatory reliability standards designed to improve grid reliability and resilience for the bulk power system, grid modernization brought new attention to the need for cybersecurity standards as new technologies are introduced. Advanced information and communications technologies are being developed and deployed at a rapid pace to enable new capabilities and to support the integration of variable and distributed energy resources. Continued advances in energy delivery technologies, and the utilization of legacy devices in ways not previously envisioned, are occurring as the cyber threat landscape is becoming more dynamic and challenging.

Cyber and physical components are now more interconnected, facing a multi-threat environment that includes combined cyber-physical attacks. Technologies deployed today are highly diverse and the sophistication of cybersecurity operations within energy companies ranges from very advanced to inadequate. Because threats will not diminish, future energy delivery systems must be designed and operated so they can continue to perform critical functions during and after an attack. It is also important that newly developed measures do not interfere with the energy delivery functions of the devices and components they are meant to protect. This will require the capability to identify, prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk to energy delivery operations. Government efforts are intended to support the energy sector's efforts to improve risk mitigation and resilience of energy delivery systems.

[5] Clapper, *Worldwide Threat Assessment for the U.S. Intelligence Community,* 2015.

Strategic Imperatives for Energy Sector Cybersecurity

Government, private industry, and individuals all contribute complementary expertise, resources, and functions to ensure the security and resilience of cyber systems. While their activities may be different, they follow a common set of principles that guide their respective efforts. The following principles draw from OE's experience in working collaboratively with the energy sector for more than 15 years as well as guidance provided in presidential directives.

1. **Effective cybersecurity for critical infrastructure is a shared responsibility.** Cybersecurity efforts are most effective when they leverage the distinct roles, capabilities, and resources of government and private industry. Private sector owners and operators are responsible for ensuring that their own assets are adequately protected against cyber threats. Government can support their efforts by sharing intelligence and best practices; conducting research, development, and demonstration (RD&D); leveraging its convening power to coordinate and align activities; conducting international coordination; supporting industry cyber incident response; and using law enforcement when called upon. OE and the energy sector will strengthen its productive partnerships to foster mutual trust, innovation, stewardship, and collaborative cybersecurity programs.
2. **Recognize the borderless, interconnected, and global nature of today's cyber environment.** Just as our power grid and energy pipelines extend across our borders, cyberspace is a global, interconnected system that traverses geographic borders and national jurisdictions. The United States will provide leadership to encourage the use of globally accepted standards, best practices, and assurance programs to promote security and interoperability.
3. **Adapt rapidly to emerging threats, technologies, and business models.** Many new digital technologies are helping to modernize the North American power grid, while the cyber threat landscape is changing rapidly. Cybersecurity efforts must be proactive, dynamic, and flexible to effectively leverage new technologies and business models and address new, ever-changing threats.
4. **Use risk-based methods to prioritize actions and investments.** Achieving 100% security of all systems against all threats is not possible. Resources are limited and all systems cannot and should not be protected in the same manner. DOE will use risk-based methods to make decisions and prioritize activities to support the risk management responsibilities of energy owners and operators.
5. **Enhance situational awareness.** Detecting and recognizing potential threats and identifying an attack requires continuous scanning of the operational environment and real-time intelligence of new methods and threat vectors. Timely, actionable, two-way information sharing between DOE and the private sector combines intelligence and information to improve situational awareness and accelerate mitigations.
6. **Unity of effort**. Government and energy industry partners must plan and act in a coordinated manner to optimize resources, share available risk information, and respond effectively to cyber incidents. State, local, tribal, and territorial (SLTT) governments also have responsibilities, authorities, capabilities, and resources and must be included in cybersecurity planning and response efforts.
7. **Rapid recovery from incidents**. Given the escalating capabilities of cyber attackers, ease of access to sophisticated exploitation tools, and the asymmetric advantage of threat actors, the private sector and government must be prepared to coordinate, leverage, and marshal resources to quickly respond and recover from cyber incidents.

2. DOE's Cybersecurity Partnership

OE's Partnership with the Energy Sector

The U.S. Department of Energy has collaborated with the energy sector for nearly two decades in a voluntary public-private partnership. This partnership was formalized with the designation of DOE as the Sector-Specific Agency (SSA)[6] for the energy sector, acknowledging the special security challenges of energy delivery systems and the distinct technical expertise of DOE. DOE engages energy owners and operators at all levels—technical, operational, and executive—to identify and mitigate physical and cyber risks to energy systems. This successful partnership is built on a foundation of earned trust that promotes the mutual exchange of information and resources to improve the security and resilience of critical energy infrastructures. This relationship acknowledges the special security challenges of energy delivery systems, and leverages the distinct technical expertise within industry and government to develop solutions.

Figure 4. Energy Sector Continuous Risk Management Functions

Energy owners and operators have primary responsibility for continuous cybersecurity risk management functions: identify assets, protect critical systems, detect incidents, respond to incidents, and recover normal operations.

About 90% of the nation's energy infrastructure is owned and operated by the private sector. Today's cyber threats may now exceed industry's expertise, resources, and capabilities. The security and integrity of the energy infrastructure is also a federal government concern because energy underpins the operations of every other critical infrastructure, the economy, and public health and safety. Because of this**, ensuring the cybersecurity of energy systems is a shared responsibility between the private sector and all levels of government**.

The public-private partnership recognizes the distinct roles and capabilities of industry and government in managing infrastructure risks. The owners and operators of energy infrastructure have the primary responsibility for the full spectrum of cybersecurity risk management: identify assets, protect critical systems, detect incidents, respond to incidents, and recover to normal operations (see Figure 4).[7] Simply put, the government has no direct role in managing operational cyber systems to reduce risks for private-sector energy assets.

OE helps reduce cyber risks in the energy sector by supporting activities that assist owners and operators with near-term response and mitigation, and long-term solutions that build resilience into next-generation cyber-physical infrastructures. OE supports energy sector risk management functions through situational awareness, information sharing, incident coordination, and technology innovation through RD&D led by industry, academia, and National Laboratories. These activities may draw upon unique government capabilities, be inherently government functions, or are mutually shared responsibilities of industry and government.

[6] DOE was designated as the Energy SSA in 2003 under Homeland Security Presidential Directive 7; Presidential Policy Directive 21 re-affirmed this role in 2015. Congress further designated DOE as the SSA for cybersecurity for the energy sector in the energy security provision of the 2015 Fixing America's Surface Transportation Act. See DOE Roles and Authorities for Cybersecurity on page 13.

[7] DOE's 2015 *Energy Sector Cybersecurity Framework Implementation Guidance* provides guidance for implementing these core functions in the National Institute of Standards and Technology *Cybersecurity Framework*.

Energy Sector Cybersecurity Roadmaps

Since 2005, DOE has worked collaboratively with the energy sector to identify cybersecurity goals, challenges, needs, and priorities. In that year, DOE partnered with the energy sector, the U.S. Department of Homeland Security, and the Canadian government to prepare the first ***Roadmap to Secure Control Systems in the Energy Sector*** (released January 2006), an industry-led strategy that outlined goals, challenges, and priorities for securing energy control systems. Since then, DOE has helped to identify priorities for improving cybersecurity in the energy sector.

The ***Roadmap to Achieve Energy Delivery Systems Cybersecurity*** (released September 2011) updates the previous Roadmap and provides a strategic framework for designing, installing, operating, and maintaining resilient energy delivery control systems that can survive a cyber incident while sustaining critical functions. More than 80 stakeholders updated the Roadmap and identified five key strategies: 1) build a culture of security, 2) assess and monitor risk, 3) develop and implement new protective measures to reduce risk, 4) manage incidents, and 5) sustain security improvements. The Roadmap guides funding priorities within DOE and other organizations. Appendix C shows a summary of recent OE RD&D projects guided by the Roadmap.

In 2016, OE conducted the ***Roadmap Milestone Assessment***,[8] which engaged 7 National Laboratories and more than 45 industry representatives to assess progress made by both the public and private sectors since 2011 toward achieving the Roadmap milestones, and to identify continuing industry needs. See Appendix B for a brief summary of *Roadmap Assessment* findings.

OE used this Assessment to directly inform federal objectives and activities in this Plan. The Assessment shows that strong partnerships among government, National Laboratories, universities, equipment vendors, and energy operators have brought new tools, technologies, and resilient operational processes into practice within energy companies nationwide. The Assessment also revealed increased cybersecurity awareness and access to information across the industry. Past OE partnership efforts contributed to notable progress in several areas, including:

- Executive engagement and support of cyber resilience efforts—DOE's active partnership with the Electricity Subsector Coordinating Council (ESCC; described further on page 14), and the Oil and Natural Gas Subsector Council (ONGCC), has successfully engaged executive-level industry leaders to advance cyber resilience and enable an agile response to cyber threats and incidents.
- Field-proven best practices and common metrics to baseline security posture—OE worked with industry to develop the Cybersecurity Capability Maturity Models (C2M2) for the electricity and ONG subsectors, which both provide repeatable measures that baseline cybersecurity posture and promote effective resource allocation for improving cybersecurity.
- Cyber threat, vulnerability, incident, and mitigation sharing—OE's development of the Cybersecurity Risk Information Sharing Program (CRISP) was noted as a successful platform for threat identification and sharing, though it must be matured further to increase its adoption and value to industry.
- Federally funded organizations that become self-sustaining—The NESCOR organization began as a public-private partnership with DOE and became a self-sustaining entity within the Electric Power Research Institute (EPRI), working to strengthen the cybersecurity posture of the electricity sector.

OE's RD&D program was also responsible for significant strides toward several near-term and long-term milestones to advance the state of the art in control systems security, detection, and mitigation capabilities.

[8] DOE, *Strategies for Achieving Energy Delivery Systems in Cybersecurity: Milestone Assessment*, 2017.

The Assessment also identified numerous areas where continued progress is most needed to achieve milestones, including improved incident identification and reporting, common platforms to share information and lessons learned, metrics to benchmark cybersecurity capabilities, workforce training and education, secure coding, addressing supply chain risk, and developing new tools to support continuity of operations during a cyber event.

With the insights from this Assessment, the Roadmap continues to guide OE's cyber RD&D projects in this Plan. DOE's objectives and milestones aim to deliver tools and technologies that directly meet industry-defined needs—particularly those where the Assessment observed limited progress—and exhibit strong potential for rapid transition to operational environments.

Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) Partnership

The SCC-GCC Partnership is the primary means for coordinating and aligning government and industry efforts to improve the security and resilience of the energy infrastructure on a voluntary basis. The SCC concept, established under Homeland Security Presidential Directive 7, enables critical infrastructure owners and operators, their trade associations, and others to address infrastructure security issues and serve as an entry point for collaborating with DOE and the federal government. More recently, Presidential Policy Directive 21 and Section 61003 of the Fixing America's Surface Transportation (FAST) Act reaffirmed DOE's primary responsibility to lead the government's partnership with energy infrastructure owners and operators on cybersecurity issues.

Over the past decade, DOE has lead the Energy GCC and used this partnership with energy owners and operators to tackle important cybersecurity challenges. For example, DOE supported the Electricity SCC in building an executive-level membership that coordinates closely with the government on national-level threats and incidents, and has the resources and authority to direct tangible progress in improving the sector's security posture. DOE also coordinated closely with the Oil and Natural Gas SCC in strengthening the physical and cyber security of pipelines, refineries, and other critical infrastructure in the oil and natural gas subsector.

Information Sharing and Analysis Centers (ISACs)

DOE works closely with representatives from the Electricity ISAC (E-ISAC), Oil and Natural Gas ISAC (ONG-ISAC), and Downstream Natural Gas ISAC (DNG-ISAC) to ensure that information on cyber and physical threats to the energy sector is analyzed and shared efficiently and effectively between the public sector, ISACs, their membership, and other relevant stakeholders. DOE holds regularly scheduled meetings with the ISACs and DOE intelligence representatives to discuss information sharing and analysis issues, and identify and remove roadblocks to the sharing and analysis of threat information. Through this work, DOE aims to establish and adopt a set of information sharing and analysis best practices for the energy sector.

Partnerships with National Laboratories and the Research Community

The DOE National Laboratories serve as a critical strategic and technology partner, providing vital facilities, resources, and capabilities to support national security needs and conducting work that is not otherwise available from the private sector. DOE and the energy sector work with the National Laboratories on RD&D of advanced technologies, analysis of cyber security risks and threats, modeling and simulation of cyber impacts, and information sharing on evolving threats.

DOE also continues to build university collaborations dedicated to advancing cybersecurity for energy delivery systems. OE academic partners include more than 20 universities, including two multi-university collaborations that are funded together by DOE OE and the DHS Science and Technology Directorate (S&T). While conducting coordinated RD&D for cybersecurity technologies, university projects engage undergraduate and graduate

students to develop the cybersecurity workforce. Through 2016, academic partnerships have resulted in more than 80 trained cybersecurity professionals entering the workforce.

Coordination with Federal Cybersecurity Efforts

The Office of Electricity Delivery and Energy Reliability leads the Department of Energy's efforts to ensure a resilient, reliable, and flexible electricity system. OE's efforts contribute to the Science and Energy Goal in the *2014-2018 DOE Strategic Plan,* specifically Strategic Objective 2 – *Support a more economically competitive, environmentally responsible, secure and resilient U.S. energy infrastructure.* OE leads two strategies to help reduce cyber risks in the energy sector:

- Improve cybersecurity in the energy sector through effective government-industry collaboration
- Strengthen the effectiveness of DOE incident management capabilities

To implement its programs, OE coordinates and leverages capabilities across the Department:

- DOE's **Office of Intelligence and Counterintelligence (IN)** provides OE and sector partners with valuable information on emerging cyber threats facing the energy sector. This includes classified threat briefings to OE on the latest malicious cyber threats, which are communicated to energy sector partners in an unclassified format. IN also plays a major role in the CRISP program (see Figure 7, page 24), which helps utilities identify malicious activity within their IT networks. Moreover, IN coordinates across the U.S. Intelligence Community to share information and identify emerging threats.
- DOE's **Office of the Chief Information Officer (OCIO)** provides OE with expertise on tools and techniques used to monitor and protect the Department's internal IT systems.
- OE coordinates with the Department's energy programs to ensure the cybersecurity of networks and resources connected to energy delivery systems. OE is engaged in joint programs with the **Office of Energy Efficiency and Renewable Energy** on cybersecurity for grid-connected renewable resources and building systems, and with the **Office of Fossil Energy** to ensure the cybersecurity of generation sources.
- DOE's **Grid Modernization Initiative (GMI)** works across DOE to develop a modern grid that is secure and resilient. GMI supports the **Grid Modernization Lab Consortium (GMLC)**, a strategic partnership between DOE and the National Laboratories to enable more efficient use of resources; shared networks; improving learning and preservation of knowledge; enhanced lab coordination and collaboration; and relationships with local stakeholders and industry. The GMLC will lead 88 grid modernization projects over 3 years. Cybersecurity needs are integrated into this foundational RD&D.

OE also coordinates its activities across the federal government and with other nations. In particular, this Plan is aligned with two key strategies that OE participates in:

- ***Federal Cybersecurity Research and Development Strategic Plan*** is a strategy to make cyberspace inherently more secure by conducting federal cybersecurity RD&D on methods and tools for deterring, protecting, detecting, and adapting to malicious cyber activities. The plan is the most comprehensive federal cybersecurity RD&D plan to date and includes near-, mid-, and long-term goals to guide and evaluate progress. It is complemented by the Networking and Information Technology Research and Development (NITRD) Program's *Supplement to the President's Budget*.
- ***Joint United States-Canada Electric Grid Security and Resilience Strategy*** is designed to strengthen the security and resilience of the North American electricity grid by pursuing joint goals and objectives to address the vulnerabilities of the two countries' respective and shared electric grid infrastructures.

Its actions are organized around three strategic goals: 1) protect today's electric grid and enhance preparedness; 2) manage contingencies and enhance response and recovery efforts; and 3) build a more secure and resilient future electric grid.

3. DOE Roles and Authorities for Cybersecurity

DOE's role in energy sector cybersecurity is well-established in legislation, executive directives, and federal policy. In 2015, Congress assigned DOE as the Sector-Specific Agency (SSA) for cybersecurity for the energy sector, building upon previous Presidential directives. While the private sector is responsible for all aspects of cybersecurity risk management of their energy systems, DOE and the federal government play critical roles in supporting industry functions in several ways:

- Provide partnership mechanisms that support collaboration and trust.
- Develop supportive policies that encourage voluntary cybersecurity in the energy sector.
- Develop tools and capabilities to conduct risk analysis.
- Leverage government capabilities to gather intelligence on threats and vulnerabilities, and share actionable intelligence with energy owners and operators in a timely manner.
- Support energy sector incident coordination and response.
- Facilitate the development of cybersecurity standards.
- Promote and support innovation and RD&D for next-generation physical-cyber systems.

The following authorities establish and support DOE's role in cybersecurity for the energy sector.

Energy Independence and Security Act of 2007 (EISA), 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.

Presidential Policy Directive 21 (PPD-21), ***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.

Energy Security provision within the Fixing America's Surface Transportation Act (FAST Act) (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.

Presidential Policy Directive 8 **(PPD-8),** ***National Preparedness*** (March 2011), is aimed at strengthening the security and resilience of the United States through systematic preparation for major national threats, including cyber attacks. 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.

Presidential Policy Directive 41 **(PPD-41),** ***United States Cyber Incident Coordination*** (July 2016), outlines three concurrent lines of effort to respond to any cyber incident involving government or private-sector entities: threat response; asset response; and intelligence support and related activities. OE, in implementing DOE's role as the SSA for the energy sector, will coordinate federal government efforts to understand the potential business or operational impact of any cyber incident on critical infrastructure in the energy sector. If a significant incident directly impacts DOE operations, DOE OCIO will initiate a fourth line of effort to directly address the cyber attack. In addition, DOE will participate in national policy and operational coordination efforts for significant cyber incidents affecting the energy sector.

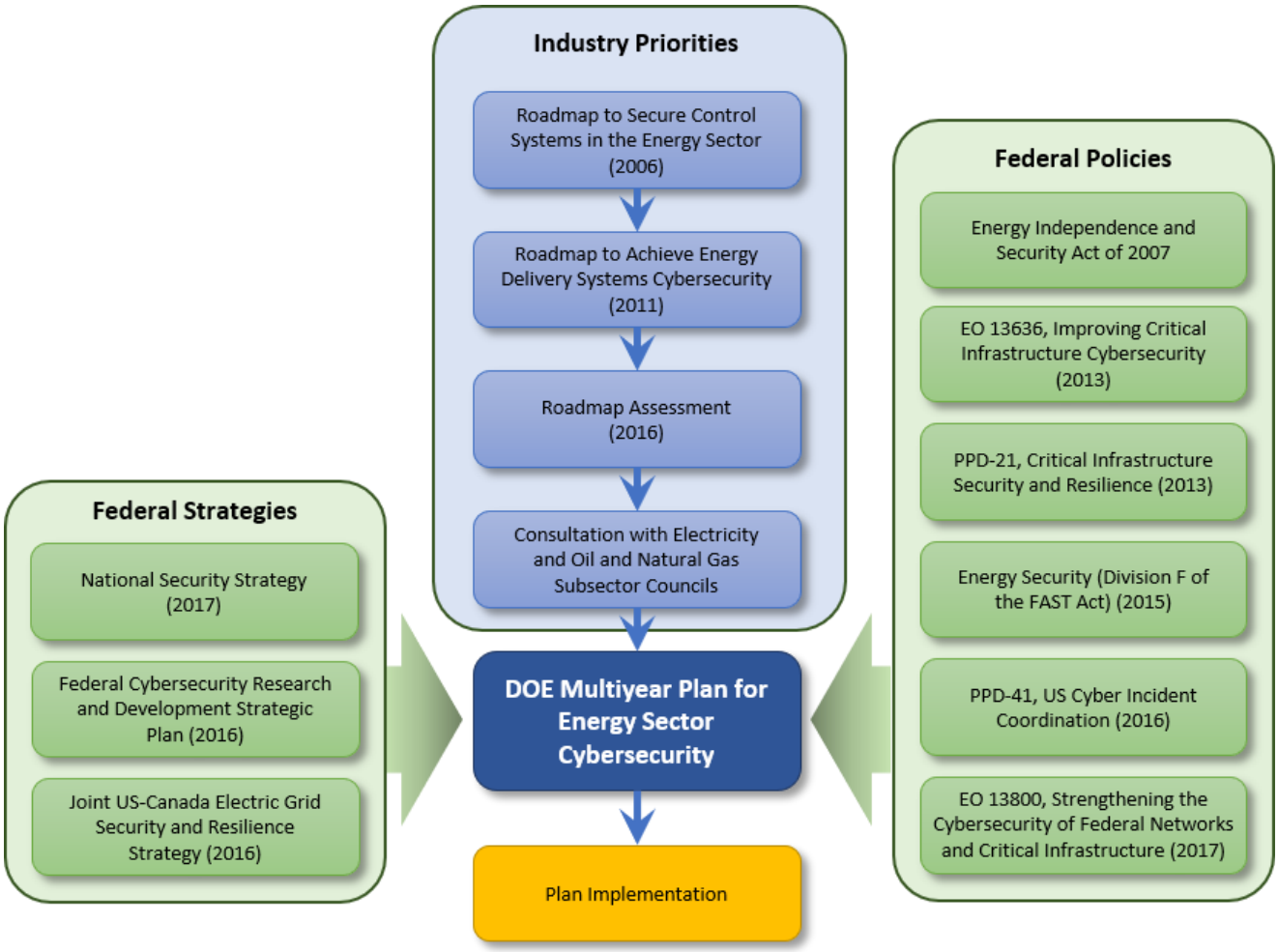
Executive Order 13636 (EO 13636), ***Improving Critical Infrastructure Cybersecurity*** (February 2013), directs the National Institute of Standards and Technology (NIST) to develop a framework to reduce cyber risks to critical infrastructure that consists of a voluntary set of standards, methodologies, procedures, and processes to address cyber risks. After the 2014 release of the *NIST Cybersecurity Framework*, DOE worked in collaboration with energy sector owners and operators to develop the *Energy Sector Cybersecurity Implementation Guidance*, 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.

Executive Order 13800 (EO 13800), ***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 cyber attack and any gaps in assets or capabilities needed to mitigate potential consequences.

Drivers for the OE Multiyear Plan

Federal authorities and responsibilities help define and shape the activities contained in OE's Plan, which is also closely aligned with national-level strategies for energy sector security and critical infrastructure cybersecurity. This Plan is also largely informed by the needs of energy sector owners and operators, who have the primary responsibility for securing cyber infrastructure in the sector. Figure 5 shows the key inputs and drivers that have informed the development of this Plan.

Figure 5. Key Inputs and Drivers for the DOE Multiyear Plan for Energy Sector Cybersecurity



4. OE Cybersecurity Strategy: Winning Today and Changing the Game for Tomorrow

Owners and operators of critical infrastructure have the primary responsibility for protecting their infrastructure, assets, and systems from a variety of risks. In the energy sector, roughly 90% of all energy systems are owned and operated by the private sector, which has a long and exemplary record of ensuring the reliability and continuity of energy services in the face of routine and severe hazards. Energy companies and utilities have long been at the forefront of implementing enterprise risk management practices to anticipate and mitigate potential problems.

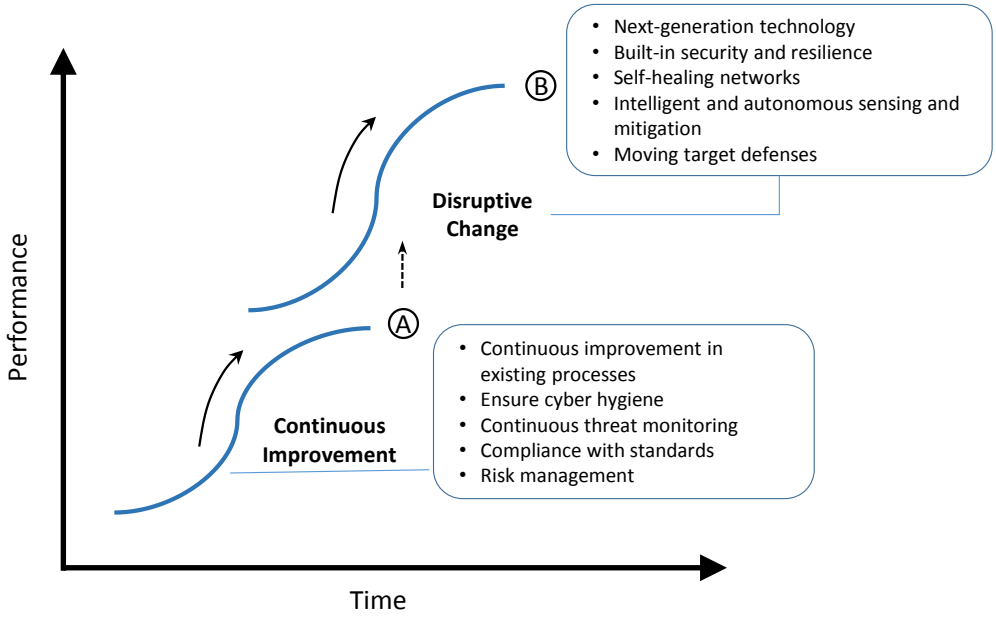
Until the September 11th attacks, the government's role in helping to ensure critical infrastructure security and resilience in the energy sector had been modest. The rapid advancement of sophisticated cyber threats and the increasing adoption of advanced energy system control technologies are changing this dynamic. Energy owners and operators have increasingly integrated digital technologies to automate and control physical devices throughout their energy systems, while malevolent actors seek to exploit cyber vulnerabilities for intentional destruction or profit. As nation-states and criminals conduct sophisticated probes and attacks on energy networks, the federal government has the responsibility to provide leadership, guidance, technical expertise, and specialized information and resources to help the private sector protect its energy systems. It is imperative that we work with our partners to address the threats of today, while working simultaneously to develop the innovative solutions for tomorrow.

> "As a nation, **we are spending more on cybersecurity today than at any time in our history**, while simultaneously continuing to witness an **increasing number of successful cyberattacks and breaches by nation states, terrorists, and hacktivists** that are stealing our intellectual property, national secrets, and private information.
>
> **The situation is not getting demonstrably better over time** and will have a debilitating long-term effect on both the economic and national security interests of the United States."
>
> — Dr. Ron Ross, NIST Fellow, speaking before the Commission on Enhancing National Cybersecurity, August 2016

The current process to identify, mitigate, and patch after the fact is not sustainable. As cyber threats become more sophisticated and frequent, the government and private sector are increasing their spending on cybersecurity operations and maintenance. At the same time, the sector continues to adopt new information and communication technologies to improve performance and adjust to a rapidly changing generation mix as well as a shift from centralized generation to distributed generation in some parts of the country. The net effect is an increasing cyber attack surface.

Any strategy to improve energy sector cybersecurity must include actions to both improve the security and resilience of today's energy systems, and to develop innovations and advanced technologies that can help build resilience into future energy systems.

Figure 6. OE's Strategic Approach Supports Both Continuous Improvement and Disruptive Change



Continuous improvements are needed and under way in existing processes, including threat monitoring, information sharing, compliance, and risk management practices, to ensure the cyber hygiene of existing energy delivery systems. Even so, many security experts have learned that anticipating and responding to the latest cyber threat is a ceaseless endeavor that requires increasingly greater resources and manpower.

That is why efforts to secure today's energy systems must also include efforts that create a disruptive change in cyber risk management. The federal government, which has historically funded innovative RD&D that cannot be justified in private-sector markets, has the additional responsibility to help develop the next generation of energy systems that are inherently self-defending and resilient, and include intelligent and autonomous sensing and mitigation (see Figure 6).

OE's Cybersecurity Plan reflects this strategic approach to continuous improvement and disruptive change. OE goals support the energy sector's risk management roles to strengthen cyber systems in operation today, and support the game-changing RD&D that will build cyber resilience into future systems. OE's activities support three strategic goals:

- **Goal 1**: Strengthen energy sector cybersecurity preparedness
- **Goal 2**: Coordinate cyber incident response and recovery
- **Goal 3**: Accelerate game-changing RD&D of resilient energy delivery systems

The following sections outline the goals in greater detail, including key challenges, objectives and activities, and milestones and performance targets through 2021.

Goal 1 Strengthen Energy Sector Cybersecurity Preparedness

DOE strives to strengthen the energy sector's cybersecurity preparedness posture and raise the maturity of its risk management capabilities through public- and private-sector partnerships that leverage DOE-supported tools, guidelines, outreach, training, and technical assistance. Reducing cyber risk to energy delivery systems requires utilities to conduct comprehensive and timely assessment of threats, identify individual system vulnerabilities and assess company practices, and analyze potential consequences to help prioritize mitigations and inform procedures. Continuous monitoring of systems, practices, and potential threats helps operators maintain situational awareness of the risk environment and enact effective risk mitigation strategies with the largest impact. DOE supports the development and adoption of industry risk management practices, including threat analysis and risk assessment tools, and shares guidance and expert analysis to support those assessments.

Timely sharing of cyber threat information across the energy sector creates the ability to identify trends specific to energy control systems that may signify a coordinated or targeted attack. In a dynamic threat environment moving at digital speed, reliable alerts about known or suspected cyber threats to energy systems can significantly limit the impact potential of an incident. To facilitate and expand efficient information sharing with the private sector, DOE leverages its: 1) unique intelligence capabilities and expertise as part of the U.S. Intelligence Community and 2) advanced threat detection technologies developed by the DOE National Laboratories.

Working on a voluntary basis with owners and operators, DOE is developing capabilities to improve the sector-wide sharing of threat indicators and analysis, allowing each energy organization to identify effective mitigations to high-priority threats. Improving the speed and accuracy of data sharing enhances the ability to identify fast-moving cyber attacks and to deploy effective mitigations before critical systems are affected.

Key Challenges

Increasing sophistication and frequency of cyber threats on a growing attack surface: The OT/ICS network environment has grown with the increased deployment of new digital devices that are sometimes located outside the physical boundary of the energy company. While these devices improve efficiency and performance, they also introduce a greater variety of cyber attack vectors. Monitoring capabilities of the critical data streams and communications pathways in OT networks must be bolstered to identify and ultimately disrupt emerging cyber attacks.

Meeting stringent privacy and security requirements while exchanging data: Real-time threat monitoring and analysis often requires exchanging extremely sensitive data from operating environments, triggering privacy and liability concerns. Real-time threat monitoring in ICS environments requires technical products and assessments that meet the requirements of OT systems and ensure protection of sensitive operational data. Pilot implementation of threat detection and analysis tools on OT systems will be required to address these challenges.

Effective assessments require specialized expertise: Effective assessment of cybersecurity risks and capabilities requires consistent, industry-accepted tools and best practices. Individual utilities, particularly smaller co-ops and public-power associations, may lack the skills and resources on staff to conduct assessments and prioritize mitigations without tools and resources. Small power suppliers also may not fall under the NERC Critical Infrastructure Protection (CIP) standards.

Information-sharing platforms require wide adoption to be most effective: Industry tools that share near-real-time threat indicators and threat analysis require wide testing with multiple industry partners and large-scale adoption by the sector to achieve their full value. Limited pilot implementations are insufficient to make a large impact on sector security or to effectively validate new tools.

Information sharing requires processes in place prior to the threat: Vital information concerning high-level cybersecurity threats and risks is often classified. This makes it difficult to distribute the information widely if partners lack clearances and if information sharing processes are not in place prior to an event or threat. More efficient processes are needed to identify and prioritize private-sector partners who have a "need to know" and grant them appropriate security clearances.

Goal 1 Objectives and Activities

Objective 1.1: Enhance information sharing and situational awareness capabilities.

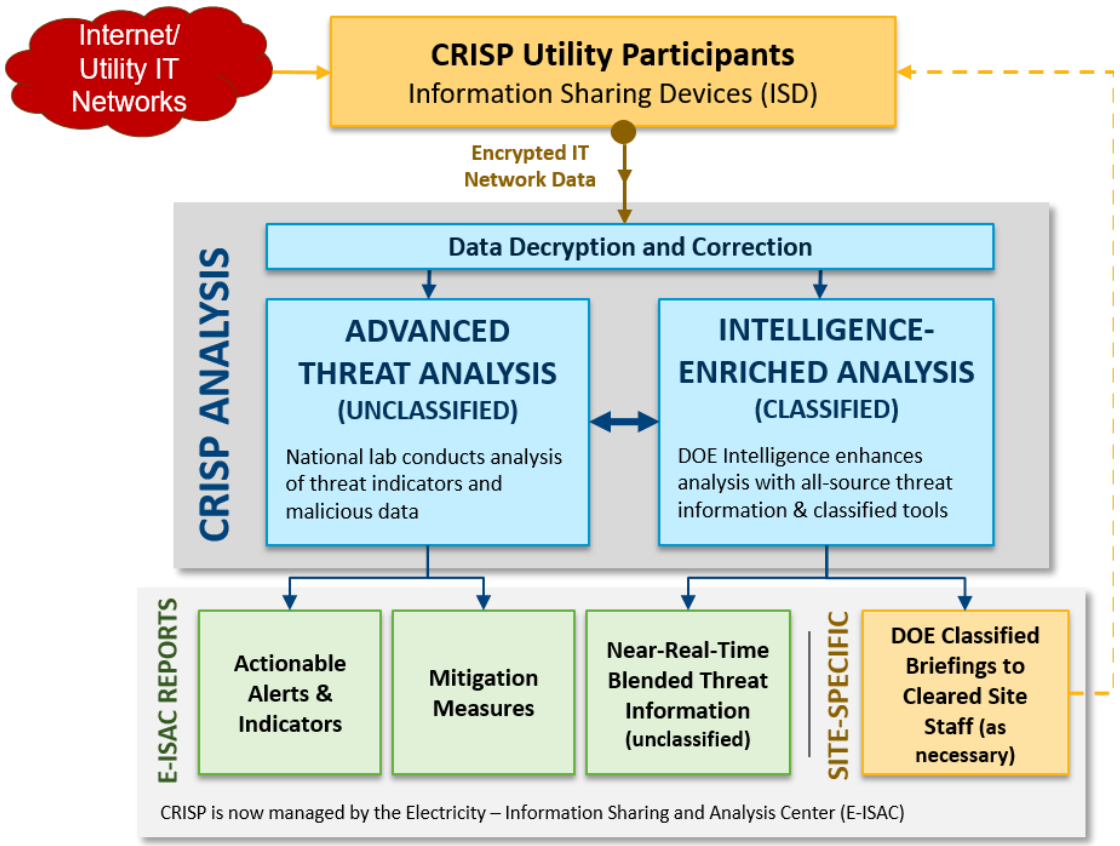
- **Define cyber situational awareness information needs and identify necessary data sources:** DOE will work with National Laboratories to develop reporting conventions and critical information requirements that facilitate the common operating picture, which internal and external federal stakeholders rely on during emergencies and steady-state operations. Timely and accurate situational awareness of incidents is necessary to set operational priorities and match federal resources to needs.
- **Provide timely cyber threat briefings to energy sector partners:** DOE will develop a targeted strategy and regularly arrange periodic threat briefings to appropriate private stakeholders to ensure timely, accurate, and actionable information sharing with energy sector partners. DOE will coordinate with the Intelligence Community, DHS, the FBI and law enforcement partners, and NERC and other industry associations to define industry cyber information needs, and ensure that threat briefings provide the appropriate technical and contextual information on emerging threats and vulnerabilities.
- **Facilitate private-sector clearances for sharing intelligence**: DOE nominates private-sector security clearances for energy sector owners and operators to facilitate sharing sensitive intelligence with those who can act on it. Cleared personnel are a prerequisite for effective information sharing.
- **Strengthen cyber preparedness among state and local stakeholders**: DOE will work with state and local energy stakeholders to ensure that state energy assurance plans and associated capabilities address state and local energy needs and are consistent with regional and federal cyber efforts. Individual states have developed state-level plans for energy distribution during emergencies; these plans are living documents that should be updated regularly to address the evolving physical and cyber risk landscape. State energy assurance plans are intended to address all hazards to the energy sector; however, the majority of existing energy assurance plans do not account for cyber incidents. Cyber incidents may introduce distinct requirements or priorities that should be considered for energy assurance.
- **Lead interagency and national policy efforts to support energy sector information sharing:** DOE programs will actively solicit feedback and address information sharing policy gaps by engaging public and private stakeholders at interagency policy committees and other forums.
- **Develop effective partnerships between cybersecurity stakeholders**: DOE will use its role as a national convener to establish effective relationships between cybersecurity stakeholders. These include asset owners and operators, ISACs, federal departments and agencies, and state, local, tribal, and territorial government stakeholders.
- **Coordinate with international partners to mitigate energy sector cyber threats and vulnerabilities in the United States:** DOE, working with interagency partners such as DHS and the FBI, will examine

international cyber incidents and share lessons learned to help the U.S. energy sector defend against cyber threats and understand vulnerabilities.

Objective 1.2: Develop and improve tools for bi-directional, real-time, machine-to-machine information sharing.

- **Grow energy sector participation in CRISP**: The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership to facilitate the timely sharing of cyber threat information and develop situational awareness tools to help the energy sector identify, prioritize, and coordinate the protection of its critical infrastructure (see Figure 7). CRISP provides a near-real-time capability for critical infrastructure owners and operators to voluntarily share cyber threat data, analyze this data, and receive machine-to-machine mitigation measures. DOE will work with industry partners and the Electricity Information Sharing and Analysis Center (E-ISAC) to expand energy sector participation in CRISP and work to advance CRISP analysis capabilities through OE's Cyber Analytics Tools and Techniques (CATT) project.
- **Expand CRISP capabilities to monitor, analyze, and share OT threat indicators**: The existing CRISP system analyzes energy sector data and provides alerts on potential malicious activity only in energy sector information technology (IT) environments—yet operational networks are also at risk of malicious attacks, and a successful attack on OT could create high-consequence disruptions to energy delivery. Robust security requires monitoring and securing both enterprise IT environments and operational environments. In the Cybersecurity for the OT Environment (CYOTE) project, DOE is leveraging the deep cybersecurity expertise of the National Labs to expand CRISP analytics by adding distinct OT threat analysis capabilities and evaluating OT data analysis methodologies specifically for the industrial control systems (ICS) operational environment. This will enable smarter, more targeted, and informed monitoring of critical ICS and OT networks and assets. DOE will:
    - Establish a methodology for effectively monitoring the OT environment and collecting, storing, and sharing sensitive OT data/cybersecurity threat information.
    - Employ new tools for big data analysis on existing CRISP data (from IT networks) in an effort to identify new threat knowledge and identify correlations between current and future IT and OT threat data.
    - Engage energy sector partners in an OT Pilot to identify where in the ICS environment the industry should be collectively watching for indications of intrusion, and develop data collection requirements that evaluate the feasibility and inform the design of future information-sharing devices or other data collection mechanisms.
    - Support an assessment of current OT sensor offerings to inform the development or identification of an OT sensor(s) for potential integration into electric sector cybersecurity efforts, including CRISP.

Figure 7. How CRISP Analysis Works



CRISP provides energy sector owners and operators with information sharing technologies originally developed to defend DOE's networks. The goal is to establish a sustainable program owned and operated by the private sector enabling near real-time data sharing and analysis.

Participating companies install an Information Sharing Device (ISD) on their network border, just outside the corporate firewall. The ISD collects data and sends the data in encrypted form to the CRISP Analysis Center. The Center analyzes the data it receives and, using government-furnished information, sends alerts and mitigation measures back to the participating companies about potential malicious activity. These alerts can be pulled directly into the companies' intrusion detection or intrusion prevention systems.

- **Develop and transition to practice a virtual crowdsourced malware forensic analysis platform**: DOE will establish a virtual collaborative platform for crowdsourcing and conducting advanced digital forensic analysis of untested and untrusted code, programs, and websites—without allowing the software to harm the host device. DOE will fund the design, development, testing, validation, and transition to practice of a malicious code repository that collects and catalogs malicious code artifacts from a variety of sources for research and analysis. The repository will be designed to enable multiple organizations to safely exchange large amounts of malicious files electronically and store the data for analysis. DOE will also support the initial prototyping and testing of software and systems to safely perform automatic analysis of malicious code (without running the code) and develop datasets of malware indicators that operators can ultimately use to proactively identify malware. Prototypes will also be developed and tested for tools that support manual analysis and sharing of insights. This digital

platform will support threat and attack analysis that can help identify malicious attacks and inform mitigation and response procedures.

Objective 1.3: Strengthen sector risk management capabilities through the development of tools, guidelines, outreach, training, and technical assistance.

- **Update the Cybersecurity Capability Maturity Model (C2M2) and Risk Management Process (RMP) to help stakeholders effectively evaluate cybersecurity and risk management capabilities:** DOE, in partnership with DHS, NIST, and the energy sector, developed C2M2 to encourage private-sector adoption of best practices and to help energy companies prioritize their cybersecurity investments. DOE also worked with industry to create an RMP that enables organizations to tailor and apply risk management processes to meet their individual organization's requirements. DOE will work with National Labs and the industry to update and expand the implementation of the C2M2 and RMP to address the changing technology and risk landscape.
- **Work with electric cooperatives and public power utilities to foster a culture of security and facilitate assessments:** DOE will work with cooperatives and public power utilities to evaluate emerging cybersecurity tools and cyber risk information sharing platforms, and develop case studies, reports, and briefs on the devices, tactics, and techniques best suited for different utility business models.

Objective 1.4: Reduce critical cybersecurity supply chain vulnerabilities and risks.

- **Identify actions the federal government can take to reduce supply chain risk:** DOE will work with federal partners to identify and take appropriate actions to mitigate supply chain cybersecurity risks and facilitate the building of trust between owners and operators and energy sector ICS manufacturers.
- **Develop an energy delivery systems (EDS) testing and analysis laboratory:** As threats continually evolve and new vulnerabilities are discovered and targeted by adversaries, national capabilities are needed to evaluate risk, assess alternative approaches, and engage with other government and private sector cyber analysis capabilities to quickly share actionable information. DOE will establish a robust cyber-physical testing capability at national laboratories to analyze systems and component vulnerabilities, malware threats, and impacts of zero-day threats on energy infrastructure; and to support initiatives to harden the supply chain. This will be accomplished by developing requirements and engaging the National Laboratories and private sector.

Goal 1: Strengthen Energy Sector Cybersecurity Preparedness – Milestones and Performance Targets

	FY17	FY18	FY19	FY20	FY21	Performance Target
Objective 1.1 Situational Awareness	Develop a clear definition of cyber situational awareness and the data required	Begin data collection in support of cyber situational awareness			Refresh understanding of data needs and sources; identify additional needed cyber situational awareness capabilities	Cyber situational awareness information is widely available to energy sector stakeholders.
Objective 1.1 Information Sharing	Define industry threat briefing needs and a formalized strategy for delivering timely and actionable cyber threat briefings	Provide energy sector partners with timely and actionable cyber threat briefings	Provide energy sector partners with timely and actionable cyber threat briefings	Provide energy sector partners with timely and actionable cyber threat briefings	Provide energy sector partners with timely and actionable cyber threat briefings	Energy sector partners receive the right information to make actionable decisions that reduce cyber risk.
Objective 1.1 State/Local Preparedness	Identify states that have not included cyber threats into their energy assurance plans and develop a strategy for engaging them to update their plans	25% of state energy assurance plans have been updated to include cybersecurity threats	50% of state energy assurance plans have been updated to include cybersecurity threats	75% of state energy assurance plans have been updated to include cybersecurity threats	100% of state energy assurance plans have been updated to include cybersecurity threats	Closer, more effective collaboration with state and local stakeholders to strengthen their cybersecurity energy assurance planning efforts.
Objective 1.1 Lead National Policy		In collaboration with industry, develop an understanding of energy sector information sharing policy gaps and formalize a strategy for addressing the gaps	Through interagency policy committees and other forums, ensure the energy sector is aware of, and has opportunity to inform national policies and priorities	Through interagency policy committees and other forums, ensure the energy sector is aware of, and has opportunity to inform national policies and priorities	Through interagency policy committees and other forums, ensure the energy sector is aware of, and has opportunity to inform national policies and priorities	Energy sector needs and expertise inform effective national policies and priorities.
Objective 1.2 CRISP Participation	>30 companies using CRISP	CRISP analysis migrated to use Intelligence Community advanced analysis tools	Cost of CRISP reduced by 50%		>100 utilities using CRISP	Sustainable, sector-driven CRISP program with advanced industry and government-informed analysis to identify malicious activity and mitigations in IT systems.
Objective 1.2 OT Capabilities	Methodology developed to analyze the OT environment and capture relevant cybersecurity information	OT data capture and analysis piloted at 4 utilities to evaluate feasibility of deploying ISD in specific locations within OT	OT sensor device capable of monitoring specific OT/ICS data streams	Wide-scale energy sector implementation of OT sensor and CRISP integration		Information sharing devices are installed within energy sector OT environments, and OT cyber threat analysis is integrated into the CRISP program and integrated with the E-ISAC to support OT threat mitigation.

Goal 1: Strengthen Energy Sector Cybersecurity Preparedness – Milestones and Performance Targets

	FY17	FY18	FY19	FY20	FY21	Performance Target
Objective 1.2 Malware Analysis	Validated prototypes for malicious code artifact storage and retrieval and for automated and manual code analysis	Malware analysis platform piloted and validated with energy sector partners				Distributed malware analysis platform that safely collects, stores, and enables automated and manual analysis of malicious code to share malware indicators with industry operators.
Objective 1.3 Update C2M2/RMP	Identify requirements and scope for the next version of C2M2 Develop capability to count access to/downloads of C2M2	C2M2 v2.0 updated and available to industry from DOE's website Increase energy sector use of C2M2 or other cyber maturity tools by an appropriate percentage	Requirements identified for the next version of the RMP Guideline	RMP Guideline v2.0 published	Begin refresh for the next version of the C2M2	Widely adopted and consistent approach for industry to assess its cybersecurity capabilities and prioritize risk reduction strategies.
Objective 1.3 Cooperative and Public Power Utility Engagement	Begin engagement with electric cooperatives and public power utilities to encourage them to adopt a culture that reflects the primacy of cyber threats	Implement an annual plan for engagement with electric cooperatives and public power utilities and define baseline levels of preparedness Hold the first cyber best practices information exchange workshop with electric cooperatives and public power utilities	Develop materials (e.g., educational materials, "train the facilitator" materials for C2M2) for engagement with electric cooperatives and public power utilities	Assess improvement in cyber posture of electric cooperatives and public power utilities		Improved awareness and increased adoption of cutting-edge cybersecurity technologies and tools, information-sharing platforms, and vulnerability assessment processes.
Objective 1.4 Supply Chain		Engage National Labs and private sector partners to establish an EDS testing and analysis capability	Establish a mechanism to share best practices and lessons learned to enhance supply chain cybersecurity			Energy owners and operators, cyber system manufacturers, and DOE better understand risks to the cyber supply chain.

Goal 2 Coordinate Cyber Incident Response and Recovery

DOE routinely works with the private sector and state and local entities during major energy disruptions to coordinate incident response, share real-time information, facilitate situational awareness, and provide federal assistance where necessary. Though a coordinated national response to storms and other physical security threats is well-practiced, a major cyber incident in the energy sector would require unique response capabilities and resources. DOE is working across industry and government to coordinate cyber incident response capabilities.

The FAST Act of 2015 establishes DOE as the Sector-Specific Agency for cybersecurity for the energy sector, which codifies language from PPD-21 into law specifically for cybersecurity. PPD-41 further charges DOE with synchronizing sector policy and operational coordination efforts for cyber incidents affecting the energy sector. DOE is working with the private sector 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. DOE has an important federal role to facilitate interagency collaboration during an incident and provide cyber-specific technical expertise and assistance to support energy sector response during a cyber incident and restore or maintain critical functions.

In parallel with this effort, DOE will also be working with DHS and non-federal partners to assess the nation's cyber incident response capabilities in the energy sector, as directed by EO 13800. The agencies will assess the potential scope and duration of a prolonged power outage resulting from a significant cyber incident, assess U.S. readiness in managing the consequences, and identify capability or asset gaps. This assessment will support a robust and coordinated federal cyber incident response capability to support the energy sector.

Key Challenges

Coordinating roles among many diverse stakeholders: Federal support of energy sector cybersecurity and incident response cuts across multiple government agencies and disciplines, from intelligence, to law enforcement, to emergency response. Without national leadership, this can result in conflicting roles and responsibilities and activities that are redundant or poorly aligned.

Developing flexible, adaptable procedures: Cyber threats evolve quickly and government hierarchies are traditionally not well-suited for a rapid reprioritization of activities. Continuous coordination across the federal government is required to unify national efforts and limit the strain on the private sector of partnering with multiple departments and agencies.

Coordinating geographically dispersed and diverse functional resources: Unlike many physical events, cyber events may affect energy infrastructure across a wide geographic area, and the consequences of an incident may be different for each affected system. Cyber incident response also may require a different set of resources, personnel, and skills than traditional energy disruptions. Some of these skills may not be included in traditional incident response procedures and training and may not be frequently tested.

Goal 2 Objectives and Activities

Objective 2.1: Establish a coordinated national cyber incident response capability for the energy sector.

- **Develop cyber incident response processes and procedures**: DOE will update its own internal coordination mechanisms (e.g., the Unified Coordination Structure [UCS] and the Emergency & Incident

Management Council) to reflect the principles of the National Cyber Incident Response Plan and PPD-41. DOE will also engage with private-sector partners to ensure continued synchronization with sector playbooks.

- **Leverage technical capabilities to augment Cyber Mutual Assistance:** DOE will collaborate with interagency partners and the DOE National Laboratories to develop and implement technical resources and capabilities that can augment industry-led Cyber Mutual Assistance activities during a crisis.

Objective 2.2: Conduct cyber incident response training and improve incident reporting.

- **Develop and conduct training for emergency responders:** DOE will expand its emergency responder training curriculum to include specific information about cyber attacks, what is expected of responders during a cyber incident, and the government and technical resources that can aid in recovery. The existing cadre of Emergency Support Function (ESF)-12 personnel will be trained on the additional procedures, response mechanisms, and other activities associated with a cyber incident. Training is updated and conducted regularly.
- **Update incident reporting processes:** DOE will revise the OE-417 incident reporting process in coordination with inter-agency partners to encourage energy sector partners to share cyber incident information on a near-real-time basis.

Objective 2.3: Exercise cybersecurity incident response processes and protocols with industry, federal, state, and local stakeholders.[9]

- **Establish an annual cyber incident response exercise program:** In support of the National Response Framework, DOE will develop and conduct an annual cyber incident exercise program to test and enhance coordination procedures within the energy sector. The exercises will include participation from industry, federal partners, and local, state, tribal, and territorial governments. DOE actively participates in regional and federal-level exercises such as the National-Level Exercise and the biennial GridEx exercises, which bring together government and private-sector leaders to simulate coordinated response to disruptions of the nation's energy sector. By creating and implementing a cyber-focused exercise series, DOE will strengthen interagency reporting, information sharing, technical assistance, and the energy sector's ability to address the particular attributes of cyber attacks.
- **Increase cybersecurity exercises with state, local, tribal, and territorial (SLTT) stakeholders:** DOE will put special emphasis on coordinating with SLTT partners, as response to energy emergencies is managed predominantly by state and local organizations that are not traditionally well-informed about cyber threats and mitigation capabilities. DOE will conduct regular exercises with states and local governments to educate SLTT stakeholders about federal cyber coordination capabilities, and provide a forum for improving local regulation, procedures, and legislation for cyber incidents in the energy sector.
- **Conduct Collegiate Cyber Defense Competitions to hone cyber defense skills in the next workforce:** DOE works with the National Labs and National Guard to conduct an annual competition where more than a dozen college teams defend mock utility systems from repeated cyber attacks. The competition attracts college students to cyber security careers and allows them to test skills in a real-world scenario.

[9] As part of PPD-41, U.S. Cyber Incident Coordination, DOE, as the SSA for the energy sector, must exercise the Enhanced Coordination Procedures developed per the direction of PPD-41.

Goal 2: Coordinate Cyber Incident Response and Recovery – Milestones and Performance Targets

	FY17	FY18	FY19	FY20	FY21	Performance Target
Objective 2.1 Cyber Incident Response Processes	Formalize standard operating procedures for cyber incident coordination activities	Establish National Laboratory Technical Assistance to support industry cyber mutual assistance Begin to integrate cyber incident coordination into UCS emergency response activities	Formalize approach for supporting energy sector cyber recovery activities	Cyber Incident Coordination is fully integrated with UCS emergency response activities Establish Memorandum of Understanding with interagency partner(s)	Test operational coordination with interagency partner(s)	Formalized processes, roles and responsibilities, and resources for cyber incident response and recovery that are integrated into UCS.
Objective 2.2 Cyber Response Training	Develop cyber-focused training for regional coordinators and voluntary responders	50% of ESF-12 cadre trained on cyber response procedures and activities	100% of ESF-12 cadre trained on cyber response procedures and activities	Identify continued cyber response training needs		Geographically distributed cadre of trained responders experienced in facilitating restoration during cyber incidents.
Objective 2.2 Update Reporting Process		Issue updated version of OE-417 form; make energy sector widely aware of requirements to file OE-417 forms in event of cyber attack	Begin to incorporate OE-417 cyber info in EAGLE-I situational awareness tool			Clearly defined process for private-sector partners to rapidly report cyber incidents.
Objective 2.3 Incident Response Exercises	Establish an annual exercise series, focusing on energy sector cyber threats, that will include participation of operators and SLTT partners	Host the 1st DOE cyber-focused exercise (analogous to DOE's Clear Path exercise) Engage 1X participants in this exercise	Implement the annual cybersecurity exercise plan Engage 5X participants in annual exercises	Expand and implement the annual cybersecurity exercise plan Engage 6X participants in annual exercises	Implement the annual cybersecurity exercise plan Engage 7X participants in annual exercises	Stakeholders have a clear understanding of DOE's Enhanced Coordination procedures and their role during an incident. DOE is recognized as a leader in developing and conducting cyber exercises for the energy sector.

Goal 3 Accelerate Game-Changing RD&D of Resilient Energy Delivery Systems

OE's portfolio of RD&D aims to deliver game-changing tools and technologies that help utilities 1) secure today's energy infrastructure from advanced cyber threats, and 2) design next-generation future systems that are built from the start to automatically detect, reject, and withstand cyber incidents, regardless of the threat. This approach continues to advance the state of the art in today's systems, while recognizing that developing cybersecurity solutions to stay ahead of the latest threat is a reactionary cycle that must be broken. Innovative RD&D to develop trustworthy, self-defending systems can disrupt this cycle and change the game for energy delivery system cybersecurity, even as the threat advances and the attack surface increases.

Achieving this goal requires the continuous transition of long-term innovative research—from research partnerships that engage the National Laboratories, universities, suppliers, energy asset owners, operators, and utilities—into capabilities that the energy sector can put into practice today, and tomorrow, to reduce cyber risk. To date, DOE-funded cybersecurity RD&D has developed and delivered 35 tools, guidance documents, and technologies to energy sector operators—several that are now used nationwide. Many of these advanced technologies are being deployed in the nation's energy delivery systems *today* to enhance security. This history of success is due in part to OE's alignment of all RD&D activities with specific milestones in the energy sector's *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. See Appendix C for a sample of successful OE RD&D projects and their alignment with the industry's Roadmap milestones. A recent assessment of progress toward the 2011 Roadmap milestones showed clear areas where continued RD&D is needed, and OE used this input to develop Plan objectives that continue to work toward the industry vision.

Today is the time to design cybersecurity into future energy delivery systems. Grid and pipeline operations are rapidly evolving to integrate millions of new smart devices and distributed resources, and legacy devices are often being used in ways that were never envisioned. As operation of energy infrastructure becomes more complex and distributed, new energy delivery system designs with built-in cyber resilience will be essential.

Key Challenges

New solutions must support the business case: Develop cybersecurity tools and technologies that are economical, cost effective, and support operations, effectively making the energy delivery system (EDS) easier and less expensive to operate.

Cybersecurity tools and technologies that do not impede energy delivery functions: Energy delivery control systems are uniquely designed and operated to control real-time physical processes that deliver continuous and reliable power. Cybersecurity technologies for business IT computer systems and networks can inadvertently damage energy delivery control systems, which have unique performance requirements and operational needs. For example, some energy delivery system communications must be fast, such as time-critical responses of less than four milliseconds for protective relaying. In addition, they must have high availability; they cannot be patched or upgraded without extensive testing and validation, normally planned weeks or months in advance, to ensure that the change does not jeopardize power system operations. Tools and technologies must not only "not impede" critical functions, but must be able to *sustain* energy delivery functions during a cyber incident.

Diverse legacy and modern devices: Cybersecurity solutions must integrate with existing systems that often contain a mix of new and legacy devices, a mix of platforms and vendors, and devices with different levels of computational and communications resources available to support cybersecurity measures.

Solutions from diverse vendors and third-party providers must interoperate: New tools and technologies must be built to common standards to allow devices from different vendors to connect and operate without issue. Interoperable cybersecurity solutions require common standards development.

Securing devices sourced from a global supply chain: Utilities must ensure the integrity of the EDS hardware, firmware, and software components as they traverse the supply chain.

Anticipating security in the future grid: Designing future systems with built-in cyber resilience requires anticipating future grid scenarios and requirements.

Meeting the growing demand for cybersecurity professionals: To manage and defend increasingly complex and sophisticated cyber systems, universities must build the nation's cybersecurity workforce. The current workforce increasingly faces heavy workloads, a shortage of critical skills, and constantly evolving expertise needs.

OE's RD&D Approach

To ensure maximum effectiveness and impact, **OE's RD&D approach starts *with the end in mind* to ensure that RD&D results transition to practice and are scalable.** OE RD&D efforts are driven by three principles:

- ***Focus on industry needs and future innovation using a partnership approach***. DOE research partnerships develop tools and technologies that advance the milestones articulated in the energy sector's *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. These milestones reflect priorities agreed upon by representatives of diverse organizations that comprise the energy sector cybersecurity community. Alignment of RD&D activities with Roadmap milestones helps ensure DOE research partnerships are working the right problems. Research partnerships that engage asset owners and operators, suppliers, universities, and National Laboratories can best pursue approaches that yield useful results by engaging team members that integrate rigorous academic approaches with real-world expertise. DOE research partnerships do not focus solely on evolutionary RD&D; they are also looking toward future power system components and architectures to design strong cybersecurity in at the beginning phases, integrated within new energy delivery system and component product lines and demonstrating interoperability across diverse vendors.

- ***Ensure cybersecurity tools and technologies do not impede energy delivery functions***. To be useful—and used—an advanced cybersecurity technology must not interfere with the function of the power system device the technology is intended to protect. For instance, where latency is a consideration, the cybersecurity technology must not slow the system down. DOE research partnerships often conclude in a demonstration of the developed technology at an asset owner or operator research partner site to help build confidence that the developed product will support, not impede, energy delivery functions.

- ***Ensure cybersecurity tools and technologies are scalable and cost effective to accelerate wide adoption throughout the energy sector***. A robust business case is needed if a cybersecurity technology is to be widely adopted throughout the energy sector. Cost-effective technologies, for instance, technologies that strengthen cybersecurity while easing the cost of operations and maintenance, offer a strong business case that heightens the chance of wide adoption. DOE research partnerships are advancing technologies that help prevent unexpected cyber-activity while improving operational network performance with faster heal times; that provide global, real-time cybersecurity situational awareness of distributed power system cyber-assets, from a central location; and that help protect grid assets from intentional misuse by a malicious insider, while at the same time helping to prevent accidental misconfiguration.

Key Successes to Date: OE's Approach to RD&D Has Supported Successful Transition to Practice

Over the past decade, OE-funded cybersecurity RD&D has transitioned 35 tools and technologies to the private sector using a partnership-focused approach. Sample projects exemplify this success:

INDUSTRY-LED PROJECT EXAMPLES

Commercialization of Software Defined Networking (SDN) for Energy Delivery Systems – Schweitzer Engineering Laboratories (SEL) led the Watchdog and SDN projects, which resulted in the world's first OT software-defined networking solution. Partnership with a national lab and demonstration in a utility environment resulted in an innovative, market-ready solution. Commercialized in a suite of SEL hardware, the SDN capability monitors network traffic using a whitelist approach, quarantines unauthorized or suspicious traffic, and pre-engineers network communication paths, allowing the network to dynamically reconfigure to thwart attacks or reconnaissance.

Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF) – CODEF detects insider attacks, spoofed power system data, malicious commands or configuration set points by anticipating their effect on power grid operations. ABB developed and then demonstrated the cybersecurity technology at the transmission level at Bonneville Power Administration (BPA), ensuring the use of this technology did not impede energy delivery functions.

Cybersecurity Intrusion Detection and Monitoring for Field Area Networks – Vencore Labs (formerly Applied Communication Sciences) worked with several utilities to demonstrate its anomaly and intrusion detection technologies for smart grid wireless mesh networks that support advanced metering infrastructure (AMI) and distribution automation. Several major utilities are now using SecureSmart™ to achieve greater visibility into these critical smart grid networks and provide security, operations, engineering, and field staff with actionable intelligence and continuous feedback. This intelligence provides utility personnel with better information to recognize an emerging threat and develop a real-time response.

NATIONAL LABORATORY-LED PROJECT EXAMPLES

Quantum Security Modules for the Smart Grid – Quantum key distribution encrypts critical network traffic with a unique advantage: operators can detect when an adversary attempts to intercept the key (causing an unavoidable distortion of the received quantum signal). Los Alamos National Laboratory recently used field trials of its hybrid classical/quantum communication system to improve polarization tracking of the photon that carries the key information over optical fibers and increase encryption speed.

Sophia – Idaho National Laboratory's patent-pending Sophia tool passively monitors communications between control system components to detect anomalies and intruders. The tool conducts a week's worth of monitoring in only four hours, and was beta-tested by 70 organizations. NexDefense acquired rights to release Sophia commercially and continues to upgrade the tool.

Hyperion – Oak Ridge National Laboratory's Hyperion tool can examine how an executable file will operate—without running the file—to detect malicious code or unexpected functions. The tool reduces supply chain risks by allowing operators to examine all new software and detect tampering or zero-day threats. Hyperion was licensed to R&K Cyber Solutions LLC in 2015.

UNIVERSITY-LED PROJECT EXAMPLES

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) – TCIPG was OE's first collaborative RD&D center, made up of five universities that worked with industry, National Labs, and academia to study control systems and design tools that embed security into grid operations. Research has resulted in multiple new tools now available to the energy sector, including **Autoscopy Jr.**, a host-based intrusion detection system for remotely deployed smart grid devices, which cannot support internal detection systems nor constantly update malware signatures; the **Amilyzer** sensor that monitors traffic among smart meters and grid access points to detect when any device deviates from the specified security policy; and **NP-View**, which performs a comprehensive network path analysis from firewall and router configurations to identify misconfigurations or deviation from security policies.

Goal 3 Objectives and Activities

Objective 3.1: Research, develop, and demonstrate tools and technologies that can be transitioned to the energy sector to prevent, detect, and mitigate cyber incidents in today's energy delivery systems.

- **Research, develop and demonstrate tools and technologies to help *prevent* a cyber incident:** Tools and technologies aim to decrease the cyber attack surface, protect what remains, and protect the supply chain to prevent the introduction of new vulnerabilities:
  - ***Decrease the cyber attack surface of energy delivery systems and components***. DOE research partnerships are advancing tools and technologies that anticipate ways a cyber attack might attempt to misuse an EDS, and that strengthen the EDS against these scenarios; that integrate "designed-in" cybersecurity within the power system component itself; and that have been strengthened through "red teaming" techniques developed specifically for novel EDS cybersecurity technologies.
  - ***Block attempted misuse of the EDS at every level***. DOE research partnerships are advancing tools and technologies that deny any unexpected cyber activity from taking place on an EDS, which is designed to perform a well-defined, limited operational function and must do nothing else, and in particular, nothing unexpected; that help impede attack planning, for instance by changing the configuration of the control system moment-by-moment, creating a "moving target" that helps prevent reconnaissance, thereby impeding this necessary first step of attack planning; that limit access to EDS components to the least needed to perform the operations or maintenance task at hand, tailored to the organizational roles of energy infrastructure operators, and tailored to different operating modes such as start-up, shut-down, normal and emergency that may change the access requirements of an EDS component.
  - ***Decrease the risk posed by malicious functionality that could be inserted as components and systems traverse the supply chain***. DOE research partnerships are advancing tools and technologies that help identify undesired, potentially malicious, functionality that may have been inserted in hardware, firmware or software of EDS components as they traverse the supply chain; that offer guidance on procurement language that purchasers and suppliers of EDS can use as a starting point to discuss needed cybersecurity measures during the EDS process; and that help ensure the integrity of patches and upgrades.

Technology Pathways to Help Prevent Cyber Incidents in Today's EDS

- Qubitekk is leading a research partnership that will help prevent cyber incidents by **decreasing the cyber attack surface through quantum key distribution** (QKD) for the energy sector. QKD enables secure exchange of cryptographic keys to prevent compromise of critical energy sector data, and detects attempted eavesdropping in real-time.
- Iowa State is leading a research partnership to **develop algorithms that continuously, and autonomously, assess and reduce the cyber attack surface**, helping prevent a cyber incident across the EDS architecture, spanning substations, the control center, and the SCADA network.

- **Research, develop and demonstrate tools and technologies to help *detect* a cyber incident:** Cyber incidents typically aim to misuse EDS functionality by forcing the system to do something it should never do, or do something it should sometimes do, but never under the prevailing operating conditions. Tools and technologies aim to rapidly identify incorrect or misused functions:
  - ***Provide for real-time continuous cybersecurity situational awareness at all EDS levels***. DOE research partnerships are advancing tools and technologies for all EDS levels (generation, transmission, and distribution) that are constantly looking for indications of an emerging cyber incident; that help power plants detect patterns of operation indicative of a cyber incident; that help detect spoofed GPS-signals that could compromise the wide-area situational awareness provided by synchrophasor data; and that help reveal the presence of an adversary in the mesh networks often found in the Advanced Metering Infrastructure (AMI) or distribution automation (DA).
  - ***Detect attempts to execute unwanted functionality that the EDS was not designed to support***. DOE research partnerships are advancing tools and technologies that help identify unexpected, and consequently undesired, cyber-activity; that help detect intrusion in energy delivery networks and computational platforms; and that help identify anomalous operational behavior that could indicate an emerging cyber incident.
  - ***Detect attempts to misuse an EDS functionality that should never be executed under the immediate circumstances***. DOE research partnerships are advancing tools and technologies that help protective relays recognize malicious commands that if implemented could jeopardize grid stability; that help power system applications such as wide area management protection and control (WAMPAC), or state estimation (SE) recognize data of compromised integrity meant to mislead operators or disrupt energy delivery; and that help identify malicious cyber activity by revealing its physical consequence for grid operations through integrated cyber-physical models, such as cyber-physical contingency analysis.

Technology Pathways to Help Detect Cyber Incidents in Today's EDS

- NRECA is leading a research partnership to develop technology to **rapidly identify anomalies in utility control communications** that can serve as indicators of a cyber compromise and support utility operators in expedited mitigation.
- Schweitzer Engineering Laboratories, Inc. (SEL) is leading a research partnership to **detect spoofing of the precise, synchronized GPS time signals that are typically used for synchrophasor data** to provide unprecedented visibility of grid operations across wide geographic regions. The partnership will also develop potential mitigations, such as shifting to an alternative precise timing source.
- Likewise, Texas A&M University Engineering Experiment Station will develop algorithms to **detect the compromise of precise synchronized timing signals** throughout the power grid architecture.

- **Research, develop and demonstrate tools and technologies to help *mitigate* a cyber incident:** Mitigating an incident requires tools and technologies to distinguish an incident, characterize it, and respond with the right actions to isolate and eliminate it:
  - ***Distinguish a disruption of energy delivery resulting from a cyber incident, from a disruption resulting from a different cause***. DOE research partnerships are advancing tools and technologies that perform advanced analytics on operational data to help distinguish a disruption of energy delivery that is caused by a cyber incident, from a failure resulting from a different cause. This rapid recognition of an emerging cyber incident is needed to help speed mitigation efforts.
  - ***Characterize the extent and consequences of a cyber incident to support response actions***. DOE research partnerships are advancing tools and technologies that help characterize changes in the trustworthiness of EDS systems and components; that anticipate consequences of a cyber incident using faster than real-time integrated cyber-physical models; and that seek ways to actively map operational networks without interrupting the function of EDS devices, recognizing that this technique is traditionally avoided as some legacy devices may in certain cases react unpredictably to today's active mapping techniques.
  - ***Provide for automated response to a cyber incident***. DOE research partnerships are advancing tools and technologies that pre-engineer alternative operational network paths that can be used automatically to help sustain critical functions in the event of a cyber incident; that help anticipate the physical consequences to power system operations if a received command is executed, and reject commands that could jeopardize grid stability; and that help tailor access controls to immediate circumstances, such as restricting access to cyber-assets in the case that physical intrusion is detected.

Technology Pathways to Help Mitigate Cyber Incidents in Today's EDS

- ABB will lead a research partnership to **enable high-voltage DC systems to detect commands that could destabilize the grid** if implemented, and mitigate the effects of these commands, preventing a cyber attack from resulting in energy delivery disruption.
- The Cyber Resilient Energy Delivery Consortium (CREDC) will **formally model risk assessment and network diversity** to assess the resilience of EDS against zero-day attacks. The risk assessment model can be used to classify attacks based on potential impacts and select a resilient mitigation approach.

Objective 3.2: Research, develop, and demonstrate tools and technologies that can be transitioned to the energy sector to change the game so that tomorrow's resilient energy delivery systems can survive a cyber incident.

- **Research, develop and demonstrate cybersecurity tools and technologies that anticipate future grid scenarios and design cybersecurity into emerging power system devices from the start:** DOE research partnerships are advancing tools and technologies that will be needed by tomorrow's power systems. For instance, increasing use of the cloud for more cost-effective operation of the grid through "big data" analytics will bring with it the need for strengthened cybersecurity between the cloud and grid-edge devices. Increasing integration of distributed energy resources will bring with it the need for strengthened cybersecurity of distribution-level energy management systems, including those that coordinate microgrid operations. In another example, today synchrophasor data are used for wide-area situational awareness across extensive geographic regions, not typically for control, of grid operations.

However, the future grid may increasingly rely on synchrophasor data for control as well as for situational awareness. Hence, DOE research partnerships are developing technologies that strengthen cybersecurity of the distributed, synchronized precise timing signals, often obtained through GPS that are used to time-align synchrophasor data.

- **Research, develop and demonstrate tools and technologies that make future power systems and components cybersecurity-aware and able to automatically prevent, detect, mitigate, and survive a cyber incident:** Tomorrow's trustworthy, cyber-resilient EDS will be able to recognize and reject a cyber attack automatically, adjusting as needed to keep the lights on while isolating, encapsulating and removing the cyber incident. These future EDS will recognize and refuse to take any action that does not support grid stability, and will only perform the well-defined functions for which they are designed.

  DOE research partnerships are working to design power systems and components to automatically recognize, and reject, attempted misuse. Research is now advancing tools and technologies that bring awareness of cybersecurity into the power system applications and devices themselves. For instance, cyber-physical state estimators that integrate the cyber and the physical infrastructure to anticipate, and automatically mitigate, cyber-physical contingencies, that is, help predict and prevent the physical consequence of a cyber incident. In another example, protection and control equipment that can check that a received command supports grid stability, given the current operational circumstances. If the received command instead jeopardizes grid stability, it can be considered malicious and automatically rejected. Likewise, operational networks that dynamically reconfigure to route around a cyber incident, while sustaining critical functions.

Industry-Led Technology Pathways to Better Secure Tomorrow's EDS

Industry-led OE projects are advancing future energy delivery systems that can survive a cyber incident while sustaining critical functions. Example projects include:

- Intel is leading a research partnership that will help **secure the cyber interaction of grid-edge devices with the cloud**. More efficient and economical grid operations are expected from future architectures that increasingly use the cloud for "big data" analytics to process new data streams from an increasing number of grid-edge devices.
- The future grid is expected to enable dynamic load management to enhance grid reliability and provide energy consumers with more, and better-informed, control over energy usage choices. United Technologies Research Center (UTRC) is leading a research partnership that will allow building management systems that interact with the building's energy provider to recognize a cyber incident that could impact the grid, and **switch to a more secure platform that may have limited functionality, but is better able to survive the incident**.
- ABB is leading a research partnership that will **develop a cyber-physical control and protection architecture for the secure integration of multi-microgrid systems**, enabling stable performance during a cyber attack. Future grid architectures may rely on microgrids, and systems of microgrids, for increased grid reliability, allowing for the creation of intentional electrical islands when this could benefit grid operations.
- SEL is leading a research partnership that will **develop resilient operational networking technology** that provides an automated response to a cyber incident, and survives without disruption of energy delivery.

Objective 3.3: Advance the nation's cyber expertise by building core capabilities in the National Labs and building dedicated university collaborations.

- **Build strategic core capabilities in the National Laboratories:** The DOE National Laboratories are engaged in bringing cyber-resilience to the nation's energy infrastructure, with an eye toward the future. OE supports RD&D at 10 National Laboratories that are working in partnership with each other, with academia, and with the energy sector, to advance cybersecurity of both the future power grid and the oil and natural gas infrastructure. OE's National Lab RD&D is designed to foster a strategic mix of core capabilities among the National Labs to strengthen the next generation of energy delivery systems.

  National Laboratory Core Capabilities to Better Secure Tomorrow's EDS

  Example national laboratory research areas include:

  - **Argonne National Laboratory** (ANL) — applications and devices that are cyber aware, such as cyber-physical state estimators that anticipate and automatically mitigate physical consequences of a cyber incident.
  - **Brookhaven National Laboratory** (BNL) — sophisticated capabilities to forecast cyber attack impacts.
  - **Idaho National Laboratory** (INL) — threat-informed control systems cybersecurity validation and demonstration; cyber-informed development and engineering for next generation resilient energy delivery systems.
  - **Los Alamos National Laboratory** (LANL) — quantum key distribution technologies that use quantum physics principles to reveal when adversaries attempt to intercept data.
  - **Lawrence Berkeley National Laboratory** (LBNL) — cyber-attack signatures in distribution level systems, where new sensors and devices are increasing cyber connections.
  - **Lawrence Livermore National Laboratory** (LLNL) — technologies that can actively map the grid's 24/7 operational networks without disrupting them.
  - **National Renewable Energy Laboratory** (NREL) — outreach to the energy sector to raise awareness of energy delivery system cybersecurity best practices.
  - **Oak Ridge National Laboratory** (ORNL) — techniques to detect when applications are compromised—either in the supply chain before deployment or during operation.
  - **Pacific Northwest National Laboratory** (PNNL) — advanced blockchain technologies and cognitive system engineering techniques to identify the information operators need to respond under multiple circumstances.
  - **Sandia National Laboratories** (SNL) — capabilities for operational network configurations to dynamically reconfigure, both to limit an adversary's reconnaissance and to sustain critical functions during an attack.

- **Build university collaborations dedicated to advancing cybersecurity for energy delivery systems:** OE academic partners include more than 20 universities, including two multi-university collaborations that are funded together by DOE OE and the DHS Science and Technology Directorate (S&T). Each academic project and university collaboration works closely with the energy sector to develop tools and technologies that will bring cyber resilience to the future power grid. University teams identify the energy sector's highest priority cybersecurity needs, research novel solutions, develop technologies and techniques that are interoperable with energy delivery infrastructure, and verify and validate product

efficacy in existing university and industry test beds. The hallmark of academic partnerships is the high degree of active engagement and outreach with stakeholders, including asset owners and operators, solution providers/vendors, and other government agencies.

These academic partnerships help develop and train the next generation of cybersecurity professionals for the energy sector. Through 2016, academic partnerships have resulted in more than 80 trained cybersecurity professionals entering the workforce, the release of more than 370 papers and publications based on cybersecurity research, and more than 600 industry-relevant presentations delivered at conferences and through webinars.

Academic Collaborations to Better Secure Tomorrow's EDS

OE builds academic partnerships by funding individual research projects led by universities, and by co-funding two large academic collaborations with DHS S&T:

- **The Cyber Resilient Energy Delivery Consortium (CREDC)** is led by the University of Illinois at Urbana-Champaign, in partnership with nine other universities and two National Laboratories. CREDC research engages an industry advisory board that helps identify research priorities, facilitating the transition of new, needed cybersecurity technologies into real-world energy delivery systems. CREDC research themes include real-time cyber event detection and situational awareness, protective and cyber-resilient architectures and technologies, and designing cyber-resilience into emerging power system devices for the future grid, and oil and natural gas infrastructure.

  Partner universities include: Arizona State University, Dartmouth College, Massachusetts Institute of Technology, Old Dominion University, Oregon State University, Rutgers University, Tennessee State University, University of Houston, and Washington State University
  Partner National Laboratories include: Argonne National Laboratory and Pacific Northwest National Laboratory

- **The Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS)** is led by the University of Arkansas, in partnership with five other universities and one electric cooperative. SEEDS research also engages an industry advisory board to help determine research priorities, provide input toward ongoing research, and ensure that activities are likely to be useful and used by the energy sector. SEEDS research themes include detecting malicious data input to power system applications such as automatic generation control, moving target defense, detecting supply chain cybersecurity compromise of smart grid devices, optimization of cybersecurity resources, and cybersecurity for time-critical communications necessary for energy delivery system operations. SEEDS is advancing cybersecurity for the power grid, as well as the oil and natural gas infrastructure.

  Partner universities include: Carnegie Mellon University, Florida International University, Lehigh University, Massachusetts Institute of Technology, and the University of Arkansas at Little Rock
  Partner electric cooperative: Arkansas Electric Cooperative Corporation

Goal 3: Accelerate Game-Changing RD&D of Resilient EDS – Milestones and Performance Targets

OE's portfolio includes technologies at all stages of development. Milestones may be met by different projects, not one project in continuous development.

	FY17	FY18	FY19	FY20	FY21	Performance Target
Objective 3.1 Prevent Today	Build research partnership to develop a tool or technology that decreases the cyber attack surface	Complete preliminary design of a tool or technology to block attempted misuse	Complete prototype of a tool or technology that reduces the risk of malicious functionality being inserted along the supply chain	Test-bed demonstrate a tool or technology that helps prevent a cyber incident in energy delivery systems	Field-test a tool or technology that helps prevent a cyber incident in energy delivery systems	Energy sector partners can access a tool or technology that helps prevent a cyber incident in energy delivery systems.
Objective 3.1 Detect Today	Build research partnership to develop a tool or technology for real-time, continuous cybersecurity situational awareness	Complete preliminary design of tool or technology to detect an action that is unexpected and ought never to be performed, regardless of operational context	Complete prototype of a tool or technology to detect an action that is expected at times, but never in the immediate operational context	Test-bed demonstrate a tool or technology that helps detect a cyber incident in energy delivery systems	Field-test a tool or technology that helps detect a cyber incident in energy delivery systems	Energy sector partners can access a tool or technology that helps detect a cyber incident in energy delivery systems.
Objective 3.1 Mitigate Today	Build research partnership to develop a tool or technology that helps distinguish a cyber incident from a disruption resulting from a different cause	Complete preliminary design of a tool or technology that characterizes the extent and consequence of a cyber incident	Complete prototype of a tool or technology that supports an automated response	Test-bed demonstrate a tool or technology that helps mitigate a cyber incident in energy delivery systems	Field-test a tool or technology that helps mitigate a cyber incident in energy delivery systems	Energy sector partners can access a tool or technology that helps mitigate a cyber incident in energy delivery systems.
Objective 3.2 Cyber Resilience Tomorrow	Build research partnership to develop a tool or technology for next-generation energy delivery systems to recognize malicious compromise of data or algorithms	Complete preliminary design of a tool or technology for next-generation energy delivery systems to adapt and survive malicious compromise of data or algorithms	Complete prototype of a tool or technology for next-generation energy delivery systems to isolate, encapsulate and reject data or algorithms subjected to malicious compromise	Test-bed demonstrate a tool or technology for next-generation energy delivery systems to survive a cyber incident	Field-test a tool or technology for next-generation energy delivery systems to survive a cyber incident	Energy sector partners can access a tool or technology for next-generation energy delivery systems to survive a cyber incident.

Goal 3: Accelerate Game-Changing RD&D of Resilient EDS – Milestones and Performance Targets

OE's portfolio includes technologies at all stages of development. Milestones may be met by different projects, not one project in continuous development.

	FY17	FY18	FY19	FY20	FY21	Performance Target
Objective 3.2 National Lab Core Capabilities	Build research partnerships that strengthen the strategic mix of core capabilities in the National Laboratories to develop a tool or technology for next-generation energy delivery systems	Complete preliminary design of a tool or technology for next-generation energy delivery systems to enable the automatic detection and rejection of cyber intruders, dynamically heal, and maintain critical operations while under attack	Complete prototype of a tool or technology to change traditionally static control systems into moving targets for the next-generation energy delivery systems	Test-bed demonstrate a tool or technology that detects intrusion in real time for next-generation energy delivery systems	Field-test a tool or technology that automates a response to a cyber incident for next-generation energy delivery systems	Energy sector partners can access a tool or technology for next-generation energy delivery systems by leveraging the core competencies at the National Laboratories.
Objective 3.2 Academic Collaboration	Build research partnerships that advance and promote the collaborative atmosphere of academic partnerships to develop a tool or technology for next-generation energy delivery systems	Complete preliminary design of a tool or technology for next-generation energy delivery systems that prevents cyber incidents	Complete prototype of a tool or technology that detects a cyber incident in next-generation energy delivery systems	Test-bed demonstrate a tool or technology that mitigates the consequences of a cyber incident in next-generation energy delivery systems	Field-test a tool or technology for next-generation energy delivery systems to automatically respond and survive a cyber incident	Energy sector partners can access a tool or technology for next-generation energy delivery systems by leveraging academic core capabilities.

Appendix A: References

Coats, Daniel R., *Worldwide Threat Assessment of the U.S. Intelligence Community, Statement for the Record*, Office of the Director of National Intelligence (Prepared for the Senate Armed Services Committee), February 13, 2018, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

Coats, Daniel R., *Worldwide Threat Assessment of the U.S. Intelligence Community, Statement for the Record*, Office of the Director of National Intelligence (Prepared for the Senate Armed Services Committee), May 23, 2017, https://www.dni.gov/files/documents/Newsroom/Testimonies/SASC%202017%20ATA%20SFR%20-%20FINAL.PDF.

Clapper, James R., 2016, *Worldwide Threat Assessment of the U.S. Intelligence Community, Statement for the Record,* Office of the Director of National Intelligence (Prepared for the Senate Armed Services Committee), February 9, 2016, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

Clapper, James R., 2015, *Worldwide Threat Assessment of the U.S. Intelligence Community, Statement for the Record,* Office of the Director of National Intelligence (Prepared for the Senate Armed Services Committee), February 26, 2015, https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy*, December 1, 2016, https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

Commission on Enhancing National Cybersecurity, "Panelist and Speaker Statements," from the Meeting of the Commission on Enhancing National Cybersecurity, August 23, 2016, https://www.nist.gov/sites/default/files/documents/2016/08/25/august23_panelist_statements.pdf.

Executive Office of the President, *National Security Strategy of the United States of America*, December 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017, https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

Fixing America's Surface Transportation (FAST) Act, Pub. L. 114-94, December 4, 2015, https://www.congress.gov/114/bills/hr22/BILLS-114hr22enr.pdf.

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), *ICS-CERT Year in Review*, 2015, https://ics-cert.us-cert.gov/Year-Review-2015.

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), *ICS-CERT Year in Review*, 2014, https://ics-cert.us-cert.gov/Year-Review-2014.

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), *ICS-CERT Year in Review*, 2013, https://ics-cert.us-cert.gov/Year-Review-2013.

Infosecurity, "Attackers Ramp Up Threats to the Energy Sector," *Infosecurity Magazine*, October 30, 2013, http://www.infosecurity-magazine.com/news/attackers-ramp-up-threats-to-the-energy-sector/.

National Infrastructure Advisory Council (NIAC), *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*, August 2017, https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf.

National Science and Technology Council, *Federal Cybersecurity Research and Development Strategic Plan: Ensuring Prosperity and National Security*, Executive Office of the President, February 2016, https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf.

Newton-Evans Research Company, *Overview of the 2014-2016 U.S. Transmission and Distribution Equipment Market, Control Systems Series CS10: Cyber Security Software for Control Systems,* July 14, 2014.

Ponemon Institute, *2015 Cost of Cyber Crime Study: United States*, October 2016, http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states.

Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience*, February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Presidential Policy Directive (PPD) 8, *National Preparedness*, March 30, 2011, http://www.dhs.gov/presidential-policy-directive-8-national-preparedness.

Tripwire, *Tripwire Study: Energy Sector Sees Dramatic Rise in Successful Cyber Attacks,* April 7, 2016, http://www.businesswire.com/news/home/20160407005104/en/Tripwire-Study-Energy-Sector-Sees-Dramatic-Rise.

United States and Canada, *Joint United States–Canada Electric Grid Security and Resilience Strategy*, December 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint_US_Canada_Grid_Strategy_06Dec2016.pdf.

U.S. Department of Energy and the Energy Sector Control Systems Working Group, *Roadmap to Achieve Energy Delivery Systems Cybersecurity,* September 2011, http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf.

U.S. Department of Energy, "Awards Selection for the Development of Next Generation Cybersecurity Technologies and Tools," August 2016, https://www.energy.gov/oe/downloads/award-selections-development-next-generation-cybersecurity-technologies-and-tools-fact.

U.S. Department of Energy, *Cybersecurity Capability Maturity Model (C2M2), Version 1.1,* February 2014, https://energy.gov/oe/downloads/cybersecurity-capability-maturity-model-february-2014.

U.S. Department of Energy, *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1*, February 2014, http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

U.S. Department of Energy, *Energy Sector Cybersecurity Framework Implementation Guidance,* January 2015, http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

U.S. Department of Energy, *Strategies for Achieving Energy Delivery Systems in Cybersecurity: Milestone Assessment*, 2017.

U.S. Department of Energy, *Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure*, April 2015, http://energy.gov/sites/prod/files/2015/04/f22/QER-ALL%20FINAL_0.pdf.

U.S. Department of Energy, *Quadrennial Technology Review: An Assessment of Energy Technologies and Research Opportunities,* September 2015, http://energy.gov/sites/prod/files/2015/09/f26/Quadrennial-Technology-Review-2015_0.pdf.

Appendix B: Energy Sector Cybersecurity Roadmap Assessment

In 2016, OE tasked 7 National Laboratories to assess the energy sector's progress in both the public and private sectors toward the 5 strategies and 28 milestones in the 2011 *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. The National Labs formed Industry Advisory Boards—including 45 total energy sector asset owners, vendors, and energy organizations—to assess progress and identify continuing industry needs. OE used this input to directly inform the objectives in this Plan.

Several of the milestones in 2011 Roadmap remain out-year milestones, with a target completion by 2020. Rather than assess each of the 28 milestones as met or unmet, the resulting *Roadmap Assessment* provides evidence of progress and recommendations for future action for each milestone, regardless of target completion date. Each milestone was also evaluated on two metrics: the number of activities working toward the milestone and the number of available tools that address it. While these are not perfect metrics of progress, milestones with higher levels of associated activities and tools were generally closer to achievement.

Refer to the milestone chart in Appendix C for a full list of Roadmap milestones.

Key Findings

The Assessment shows that strong partnerships among government, National Laboratories, universities, equipment vendors, and energy operators have brought new tools, technologies, and resilient operational processes into practice within energy companies nationwide. The Assessment revealed increased cybersecurity awareness and access to threat information across the industry since 2011.

Yet the Assessment also found that the sector-wide impact of new tools and technology advancements was often limited by lack of awareness. Outreach was a key barrier to wider adoption of cybersecurity tools or participation in partnership activities.

The Roadmap identified a step-wise approach over a 10-year timeframe, with 8 near-term, 11 mid-term, and 9 long-term milestones. As expected, there was often more clear progress toward near- or mid-term milestones, but also a host of remaining needs: to mature new technologies, to continue RD&D to advance emerging capabilities, or to fund new research for long-term milestones that represent a future state.

Select Examples of Notable Progress

The following are select examples of notable progress toward several milestones (noted in parentheses), though more work remains in each area:

- **Executive engagement and support of cyber resilience efforts** (1.1)—The Electricity Subsector Coordinating Council (ESCC) has engaged executive-level industry leaders to coordinate with government counterparts to advance cyber resilience and enable an agile response to cyber threats and incidents. The ONG subsector reported the prevalence of executive and senior management engagement, responsibility, and support of cyber resilience efforts within the organization.
- **Field-proven best practices and resources** (1.4)—Federally funded resources and tools—such as C2M2 or Procurement Language for EDS—are valuable to several utilities; however, the degree of penetration across the energy sector is still relatively limited, and guidelines may not be appropriately scaled for small utilities. In the ONG subsector, required standards and guides have resulted in nearly universal implementation of best practices.

- **Common metrics to baseline and benchmark security posture** (Milestone 2.1, 2.2)—The Cybersecurity Capability Maturity Models (C2M2) for the electricity and ONG subsectors both provide repeatable measures that baseline cybersecurity posture and promote effective resource allocation. Yet companies still cannot adequately compare their security posture, and smaller companies have not widely adopted these and other tools.
- **Cyber threat, vulnerability, incident, and mitigation sharing** (5.1, 5.3, 4.6)—Industry partners noted substantial progress on information sharing, particularly through ICS-CERT, the ISACs, EPRI, and CRISP, and especially regarding accessible and actionable information following the 2015 attack on the Ukrainian grid. Yet more work is needed to make these mature, proactive processes. Companies still rarely voluntarily report incident information, and collection of lessons learned is fragmented.
- **Cyber event detection tools that evolve with the dynamic threat landscape** (4.1, 4.5)—While the maturity of cyber event detection tools has dramatically improved, few are specifically tailored to OT or able to evolve to address new threats. OE supports RD&D to develop technologies that anticipate cyber-physical contingencies, and implement mitigations before the contingency arises.
- **Incident reporting guidelines** (4.3)—Incident reporting is well implemented for electricity—through NERC CIP, DOE, and E-ISAC requirements—and for ONG through their regulatory bodies. Yet current processes are driven by compliance more than process improvement, and coordination among reporting mechanisms could be valuable.
- **Federally funded organizations that become self-sustaining** (5.4)—While there are few fully self-sustaining cybersecurity organizations, the NESCOR organization began as a public-private partnership with DOE and became a self-sustaining entity within the Electric Power Research Institute (EPRI), working to strengthen the cybersecurity posture of the electricity sector. Despite this success, few industry members knew of or had engaged with NESCOR.

Continuing Industry Needs

Several areas require continued advances and new capabilities—even where substantial progress has been made to date—reflecting the dynamic character of advancing power system technologies and a rapidly evolving threat environment. Many of the milestones referenced below are long-term milestones, targeted for achievement by 2020. The assessment confirmed that many of these out-year targets remain relevant priorities today and should receive continued focus. Select examples of continuing needs (in addition to those noted above) include:

- **Secure code development and software quality assurance** (1.2 and 1.3): Secure and safe coding practices can be implemented on new products, but high cost, conflicts with legacy products, and lack of demand remain key barriers. Significant work is needed in awareness and workforce training. Supply chain risk remains a key issue.
- **Real-time security state monitoring and risk assessment** (2.3)—A multitude of tools and vendor products for monitoring were noted, yet real-time monitoring of OT systems is still a challenge, and no tools can assess new risks in real time.
- **Workforce training and education** (1.6): Despite new courses and university curricula, the shortage of qualified cybersecurity professionals remains severe.

- **Secure serial and routable communications and secure wireless communications** (3.3, 3.6): Substantial work is underway to develop new security protocols and test new approaches on OT systems. Implementation across entire systems presents many challenges. Emerging technologies, like SDN, have yet to make a significant impact.
- **Self-configuring EDS network architectures and continued operation during a cyber attack** (3.4, 3.5): Self-configuring and self-defending architectures largely remain a future state where additional RD&D is needed. OE continues to support RD&D to develop and transition technologies that adapt operational network pathways to route around disruptions, and technologies that identify compromised power system devices, then adapt to their loss by changing how the remaining, uncompromised devices are used.
- **Real-time forensics capabilities** (4.4)—Forensics for OT is still largely a black box activity for post-event analysis. Large technology gaps remain for conducting forensics and sharing data.
- **Automated response to cyber incidents** (4.7)—There is a significant gap between the state of the art and this milestone. New technologies can automatically identify a cyber incident, but substantial RD&D is needed to design systems that can automatically respond or reconfigure.
- **Mature platforms for information sharing** (5.6)— Users find it difficult to keep up with the data and alerts, and need machine-to-machine information sharing to speed response.

With the insights from this Assessment, the Roadmap continues to guide OE's cyber RD&D projects in this Plan to deliver tools and technologies that directly meet industry-defined needs and exhibit strong potential for rapid transition to operational environments.

Appendix C: Industry Needs Drive OE-Funded Cybersecurity RD&D (Goal 3)

Since its first release in 2006, OE has used the cybersecurity needs identified by the energy sector in the *Roadmap to Achieve Energy Delivery Systems Cybersecurity* to drive a wide portfolio of RD&D efforts with industry, universities, and National Laboratories. More than 80 industry representatives developed the 2011 Roadmap and identified five core Roadmap strategies and 28 specific milestones (see Table 1).

The last decade of OE-funded projects fully transitioned 35 tools and technologies to the industry marketplace, while building a foundation of new capabilities that current projects can build upon. OE continues to align its RD&D projects directly to the industry needs in the Roadmap, and the objectives identified under Plan Goal 3 reflect this alignment. OE's strategy of funding public-private partnerships and cost-sharing research accelerates leap-ahead technology advancements and speeds market adoption. Table 2 shows how ongoing and completed projects from OE's RD&D portfolio support several of the Roadmap milestones.

Table 1. Roadmap Strategies, Milestones, and Goals

	1. Assess and Monitor Risk	2. Manage Incidents	3. Develop and Implement New Protective Measures to Reduce Risk	4. Manage Incidents	5. Sustain Security Improvements
Near-term Milestones (By 2013)	**1.1** Executive Engagement and support of cyber resilience efforts **1.2** Industry-driven safe code development and software assurance awareness workforce training campaign launched	**2.1** Common terms and measures specific to each energy subsector available for baselining security posture in operational settings	**3.1** Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes commercially available	**4.1** Tools to identify cyber events across all levels of energy delivery system networks commercially available **4.2** Tools to support and implement cyber-attack response decision making for the human operator commercially available	**5.1** Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders **5.2** Federal and state incentives available to accelerate investment in and adoption of resilient energy delivery systems
Mid-term Milestones (By 2017)	**1.3** Vendor systems and components using sophisticated secure coding and software assurance practices widely available **1.4** Field-proven best practices for energy delivery systems security widely employed **1.5** Compelling business case developed for investment in energy delivery systems security	**2.2** Majority of asset owners baselining their security posture using energy subsector specific metrics	**3.2** Scalable access control for all energy delivery system devices available **3.3** Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented	**4.3** Incident reporting guidelines accepted and implemented by each energy subsector **4.4** Real-time forensics capabilities commercially available **4.5** Cyber event detection tools that evolve with the dynamic threat landscape commercially available	**5.3** Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners **5.4** Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining
Long-term Milestones (By 2020)	**1.6** Significant increase in the number of workers skilled in energy delivery, information systems, and cybersecurity employed by industry	**2.3** Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available	**3.4** Self-configuring energy delivery system network architectures widely available **3.5** Capabilities that enable security solutions to continue operation during a cyber-attack available as upgrades and built-in to new security solutions **3.6** Next-generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented	**4.6** Lessons learned from cyber incidents shared and implemented throughout the energy sector **4.7** Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available	**5.5** Private-sector investment surpasses federal investment in developing cybersecurity solutions for energy delivery systems **5.6** Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector
Goals	**Continuous security state monitoring of all energy delivery system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators**	**Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment**	**Next-generation energy delivery system architectures provide "defense in depth" and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident**	**Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment**	**Collaboration between industry, academia, and government maintains cybersecurity advances**

Table 2. Alignment of OE RD&D Portfolio (to Address Goal 3) with Industry Needs

OE-Funded RD&D Portfolio	Industry-Defined Roadmap Milestones																										
ONGOING PROJECTS TO ADDRESS GOAL 3	1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	3.1	3.2	3.3	3.4	3.5	3.6	4.1	4.2	4.3	4.4	4.5	4.6	4.7	5.1	5.2	5.3	5.4	5.5	5.6
ABB, Inc.: "Cyber Attack Resilient HVDC System"									•					•		•	•			•		•						
ABB, Inc.: "Multi-layered Resilient Microgrid Networks"										•		•	•	•	•													
Argonne National Laboratory (ANL): "A Resilient and Trustworthy Cloud and Outsourcing Security Framework for Power Grid Applications"										•				•		•												
Brookhaven National Laboratory: "AIERCI Tool to Ensure Uninterrupted Energy Flow from Cyber Attacks Targeting Essential Forecasting Data for Grid Operations"									•					•		•	•			•								
GE Global Research: "Cyber Attack Detection and Accommodation for Energy Delivery Systems"									•	•			•	•			•			•		•						
Intel Federal, LLC: "Enhanced Security for the Power System Edge"									•		•	•			•	•				•								
Iowa State University of Science and Technology: "Autonomous Tools for Attack Surface Reduction"									•	•			•	•			•					•						
Lawrence Berkeley National Laboratory: "Detecting Differences between Real-Time Micro-synchrophasor Measurements and Cyber-Reported SCADA"									•	•						•				•								
Lawrence Livermore National Laboratory (LLNL): "GMLC: Threat Detection and Response with Data Analytics"									•	•				•		•				•								
Qubitekk, Inc.: "A Scalable Quantum Cryptography Network for Protected Automation Communications"										•	•	•				•				•								
Schweitzer Engineering Laboratories, Inc. (SEL): "Chess Master"									•	•	•	•	•	•		•				•		•						
Schweitzer Engineering Laboratories, Inc. (SEL): "Tempus Project"									•					•		•				•								
Texas A&M Engineering Experiment Station: "Timing Intrusion Management Ensuring Resilience (TIMER)"									•	•				•		•				•		•						

OE-Funded RD&D Portfolio	Industry-Defined Roadmap Milestones																											
ONGOING PROJECTS TO ADDRESS GOAL 3	1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	3.1	3.2	3.3	3.4	3.5	3.6	4.1	4.2	4.3	4.4	4.5	4.6	4.7	5.1	5.2	5.3	5.4	5.5	5.6
United Technologies Research Center: "INGRESS: Integration of Green Renewable Energy Sources Securely with Buildings and Electric Power"									•	•			•									•						
University of Arkansas: "Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS)"									•	•						•												
University of Arkansas: "Detecting Compromised Devices"									•							•				•								
University of Arkansas: "Detecting Time Synchronization Attack (TSA) in PMU Data"									•							•				•								
University of Arkansas: "Mitigating Data Falsification Attacks in Automatic Generation Control (AGC)"									•	•				•						•								
University of Illinois at Urbana-Champaign: "Continuous Security Monitoring Protocols and Architectures for Energy Delivery Systems"									•	•						•				•								
University of Illinois at Urbana-Champaign: "Cyber-Physical Intrusion Detection Incorporating Micro PMU Measurements"									•	•				•						•								
University of Illinois at Urbana-Champaign: "Cyber Resilient Energy Delivery Consortium (CREDC)"									•	•	•	•	•	•	•	•	•											
University of Illinois at Urbana-Champaign: "Forecasting Cybersecurity Incidents in Energy Delivery Systems"									•	•				•						•								
University of Illinois at Urbana-Champaign: "Robust and Scalable Security Monitoring and Compliance Management for Dynamic Energy Delivery Systems"									•	•						•				•								
University of Illinois: "Cyber-Physical Modeling and Analysis for Cyber-Induced Cascading Failure Risk Assessment"									•	•						•				•								
University of Illinois: "Modeling Security Risk to and Resiliency of EDS Using Software-Defined Networks and Robust Networked Control Systems"									•			•	•	•						•		•						
University of Illinois: "Robust and Secure GPS-Based Timing for Power Systems"									•							•				•								
University of Illinois: "Secure, Dynamic Interoperability of Microgrid Assets"									•	•				•	•					•		•						

OE-Funded RD&D Portfolio	Industry-Defined Roadmap Milestones																													
COMPLETED FOUNDATIONAL PROJECTS (GOAL 3 SUCCESSES)	1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	3.1	3.2	3.3	3.4	3.5	3.6	4.1	4.2	4.3	4.4	4.5	4.6	4.7	5.1	5.2	5.3	5.4	5.5	5.6
Siemens Energy Automation: "Situational Awareness of Physical/ Cybersecurity Posture"									•							•	•											
ViaSat Inc.: "Cyber-Intrusion Auto-Response Policy and Management System (CAPMS)"			•						•		•	•		•		•	•		•	•	•	•	•		•			•
Grid Protection Alliance: "ARMORE: Applied Resiliency for More Trustworthy Grid Operation"									•			•				•	•											
Schweitzer Engineering Laboratories Inc.: "Secure Software Defined Radio"											•				•													
Schweitzer Engineering Laboratories Inc.: "Software Defined Networking (SDN) Project"											•	•	•	•														
Schweitzer Engineering Laboratories Inc.: "Alliance Project"											•																	
Foxguard Solutions Inc.: "Patch and Update Management Program for Energy Delivery Systems"			•							•													•		•			
Vencore Labs, Inc.: "Cybersecurity Intrusion Detection and Monitoring for Field Area Networks"									•							•	•		•	•								
National Rural Electric Cooperative Association (NRECA): "Energy Sector Security Appliances in a System for Intelligent, Learning Network Configuration Management and Monitoring"									•							•	•		•	•								
Digital Bond: "Bandolier"									•	•			•															
Digital Bond: "Portaledge"									•							•												
Argonne National Laboratory (ANL): "A Resilient Self-Healing Cyber Security Framework for Power Grid"				•		•			•				•		•					•			•					
Idaho National Laboratory (INL): "Control System Situational Awareness Technology"									•			•		•		•	•											
Oak Ridge National Laboratory (ORNL): "Automated Vulnerability Detection for Compiled Smart Grid Software"			•							•																		

OE-Funded RD&D Portfolio	Industry-Defined Roadmap Milestones																											
COMPLETED FOUNDATIONAL PROJECTS (GOAL 3 SUCCESSES)	1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	3.1	3.2	3.3	3.4	3.5	3.6	4.1	4.2	4.3	4.4	4.5	4.6	4.7	5.1	5.2	5.3	5.4	5.5	5.6
Oak Ridge National Laboratory (ORNL): "Next-Generation Secure, Scalable Communication Network for the Smart Grid"													•	•	•													
Oak Ridge National Laboratory (ORNL): "Practical Quantum Security for Grid Automation"												•																
Pacific Northwest National Laboratory (PNNL): "Bio-Inspired Technologies for Enhancing Cyber Security in the Energy Sector"									•							•	•											
Pacific Northwest National Laboratory (PNNL): "Supply Chain Integration for Integrity (SCI-FI)"			•	•					•		•																	
Pacific Northwest National Laboratory (PNNL): "Understanding the Special Case of Digital Forensics in Energy Delivery Systems"																			•	•								
Sandia National Laboratory (SNL): "Artificial Diversity and Defense Security (ADDSec)"									•				•	•	•					•		•						
Idaho National Laboratory (INL): "High Level Language Microcontroller"			•								•																	
Sandia National Laboratory: "Trust Anchor/CodeSeal"									•			•				•	•											

U.S. DEPARTMENT OF ENERGY

OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY