Written Statement by

Carol Hawk,
Acting Deputy Assistant Secretary
Cybersecurity for Energy Delivery Systems
Office of Cybersecurity, Energy Security, and Emergency Response

U.S. Department of Energy

at the

Federal Energy Regulatory Commission's
Reliability Technical Conference

Docket No. AD18-11-000
Tuesday, July 31, 2018

Introduction

The cybersecurity of the Nation's energy sector is a shared vital interest of sector owners, operators, and the Federal government. The Department of Energy (Department or DOE), as the Sector-Specific Agency for energy, recognizes the unique security challenges of energy delivery systems and leverages the distinct capabilities within industry and government to develop solutions. DOE serves as the day-to-day Federal interface for the prioritization and coordination of sector cybersecurity activities. The Department collaborates with the energy sector in voluntary public-private partnerships that engage energy owners, operators, and stakeholders at all levels—technical, operational, and executive—to identify and mitigate cyber risks to energy systems. The Department's cybersecurity efforts span preparedness, response, and research and development activities, following a strategic plan that is informed by input from industry and National Laboratories.

In May 2018, DOE released the Multiyear Plan for Energy Sector Cybersecurity (Multiyear Plan), which articulates a vision of resilient energy delivery systems designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions. 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. While the Multiyear Plan outlines activities specifically for DOE, efforts are conducted in close partnership with public and private stakeholders.

Anticipating and responding to the latest cyber threat is a ceaseless endeavor. It is imperative to recognize today's realities: resources are limited, and cyber threats continue to increase in frequency and sophistication. Developing cybersecurity solutions to stay ahead of the latest threat is a reactionary cycle that must be broken. Innovative research, development, and deployment (RD&D) designed 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. To gain the upper hand, innovative RD&D and disruptive changes in cyber risk management practices must be pursued.

DOE's cyber strategy is two-fold: (1) strengthen today's energy delivery systems by working with our partners to address growing threats and promote continuous improvement, and (2) develop game-changing solutions that will create inherently secure, resilient, and self-defending energy systems for tomorrow.

A1. How are current trends in cyber threats and vulnerabilities affecting the behavior of grid owners and operators?

As the President's National Security Strategy highlights, "the vulnerability of U.S. critical infrastructure to cyber, physical, and electromagnetic attacks means that adversaries could disrupt military command and control, banking and financial operations, the electric grid and means of communication."[1]

Our National Intelligence Agencies have noted the increasing number and sophistication of cyber threats. Earlier this month, the Director of National Intelligence stated that "today, the digital

[1] https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

infrastructure that serves this country is literally under attack" and that ". . . the warning lights are blinking red again."[2] Cyber attacks targeting Information Technology, or IT, including computing and business applications, are growing increasingly common, seeking to cause disruptions, obtain access to email accounts and personal information, exfiltrate data to release to the world at large, and exploit information for private gain. According to the Worldwide Threat Assessment, "the risk is growing that some adversaries will conduct cyber attacks . . . against the United States in a crisis short of war."[3] The energy sector is not immune to such attacks and, given its criticality to all other sectors, is a prime target.

Threat actors are also increasingly targeting Operational Technology (OT), the computers and networks that manage, monitor, protect, and control critical energy delivery infrastructure. For instance, OT systems can include programmable logic controllers, and their associated supervisory control and data acquisition software. The Department of Homeland Security's (DHS's) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) coordinates control systems-related security incidents and information sharing with Federal, state, and local agencies and organizations, the intelligence community, and private sector constituents. ICS-CERT responded to 295 incidents in FY 2015, of which 46 were in the energy critical infrastructure (CI) sector, and 290 incidents in FY 2016, of which 59 of the events were in the energy CI sector.[4]

Grid Owners and Operators and other energy sector stakeholders' engagement with DOE through public private partnership programs are stronger than ever. The energy sector owners and operators are responding to the changing threat landscape by strengthening their cybersecurity posture with improved processes, practices, and technologies. Examples include organizational changes that align with IT and OT security, and inclusion of cybersecurity provisions in procurement. Additionally, sector vendors and suppliers are increasingly partnering with DOE to advance the cyber-resilience of their products and cyber risk management practices.

A2. How can grid operators be better prepared to protect their systems from these threats? And A3. How do you recommend organizations mitigate cyber risks?
Drawing from DOE's experience working collaboratively with the energy sector as well as guidance provided in presidential directives, DOE's Multiyear Plan summarizes the following principles as paramount for protecting systems and mitigating risks:

1. Effective cybersecurity for critical infrastructure is a shared responsibility

[2] https://s3.amazonaws.com/media.hudson.org/files/publications/CoatsFINAL.pdf
[3] https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf
[4] DOE also collects information on electric incidents and emergencies through the Electric Emergency Incident and Disturbance Report (Form OE-417). Electric utilities that operate as Control Area Operators and/or Reliability Authorities, as well as other electric utilities as appropriate, are required to file the form whenever an electrical incident or disturbance is sufficiently large enough to cross reporting thresholds. In the case of cybersecurity, reporting is required for a cyber event that causes interruptions of electrical system operations or an event that could potentially impact electric power system adequacy or reliability. In 2016, five of the 141 events reported were cyber-related, compared with three of 150 events in 2017. However, through May of 2018, four of the 81 reported events were cyber-related. https://www.oe.netl.doe.gov/OE417_annual_summary.aspx

2. Recognize the borderless, interconnected, and global nature of today's cyber environment
3. Adapt rapidly to emerging threats, technologies, and business models
4. Use risk-based methods to prioritize actions and investments
5. Enhance situational awareness
6. Unity of effort
7. Rapid recovery from incidents

A wide range of sector neutral and sector specific frameworks and guidelines are available to organizations to help establish, evaluate, or improve their cybersecurity programs and controls.

A5. What information-sharing practices are required?
Coordination between energy sector partners and the government is necessary to share emerging threat data and vulnerability information, and to deploy advanced technology and architectures to help prevent, detect, identify, and thwart cyber-attacks more rapidly.

Subsector Coordinating Councils
In the energy sector, the core of critical infrastructure coordination is facilitated by the Electricity Subsector Coordinating Council (ESCC), the Oil and Natural Gas Subsector Coordinating Council (ONG SCC), and the Energy Government Coordinating Council (EGCC). The ESCC and ONG SCC represent the interests of their respective industries.

DOE consistently coordinates with the ESCC, the ONG SCC, and the EGCC leadership regarding research and development of new cybersecurity tools and technologies, information sharing, organizational and process level cybersecurity posture, and cyber-incident response and recovery activities. These organizations serve as the principal liaison between the Federal Government and the energy sector with the mission of coordinating efforts to prepare for and respond to national-level disasters or threats to critical infrastructure. The ESCC and the ONG SCC represent the interests of their respective industries. The EGCC, led by DOE and co-chaired with DHS, provides for a forum for interagency partners, states, and international partners to discuss the important security and resilience issues for the energy sector.

Industry Information Sharing and Analysis Organizations
Industry information sharing organizations assist owners, operators, and government with information pertaining to cyber and physical security. The Electricity Information Sharing and Analysis Center (E-ISAC), Oil & Natural Gas Information Sharing and Analysis Center, and the Downstream Natural Gas Information Sharing and Analysis Center are pivotal to communication, coordination, analysis, and reporting of threats, vulnerabilities, and incidents in the energy sector, especially at the technical level.

Critical Electric Infrastructure Information
One effort where information sharing is absolutely vital is DOE's national security responsibility to protect information under its Critical Electric Infrastructure Information (CEII) designation authority. Protection of this data is key to the safety of our systems from bad actors. DOE is currently developing new administrative procedures for CEII designation and we look forward to working with industry partners on CEII disclosure regulations that balance protection of our

critical assets with the need for certain narrow disclosures for specific regulatory and R&D needs. Completion of these procedures will allow DOE to access critical information needed to execute its responsibilities as the Sector-Specific Agency for Energy under Presidential Policy Directive 21. These proposed procedures are intended to ensure that stakeholders and the public understand how DOE would designate, protect, and share CEII.

Cybersecurity Risk Information Sharing Program
Another example of DOE-industry collaboration is the Cybersecurity Risk Information Sharing Program (CRISP), a voluntary public-private partnership that is funded by industry, administered by the E-ISAC, and supported by DOE. DOE's Office of Intelligence and Counterintelligence provides analytic support and DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is advancing research and development (R&D) of information sharing capabilities.

The purpose of CRISP is to share information among electricity sector partners, DOE, and the Intelligence Community to facilitate the timely bi-directional sharing of unclassified and classified threat information to enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources.

CRISP leverages advanced sensors and threat analysis techniques developed by DOE along with DOE's expertise as part of the Intelligence Community to better inform the energy sector of cyber risks. Current CRISP participants provide power to over 75 percent of the total number of continental United States electricity customers.

Cybersecurity for the Operational Technology Environment
While the CRISP program is designed to support analysis of energy sector IT networks, Cybersecurity for the Operational Technology Environment (CYOTE) is focused on cyber threats in operational technology, or OT networks, which manage and control the energy delivery system infrastructure and could pose an attack vector for energy disruptions.

The Department is working with several utilities to design an approach for appropriately sharing OT data—one that allows operators to elicit special insights from the U.S. intelligence community and the expertise of DOE national laboratories to deliver actionable information.

A6. How are best practices developed, applied, and improved?
DOE leverages public private partnerships to support the development of best practices. Stakeholder engagement ensures a better product with stronger adoption. Over the past several years, DOE and other government stakeholders in partnership with industry have developed and supported numerous cybersecurity guidance documents.

Cybersecurity Capability Maturity Model (C2M2)
DOE's Cybersecurity Capability Maturity Model (C2M2) program helps companies evaluate the cybersecurity posture of the grid, allowing them—regardless of size, type, or industry—to improve the cybersecurity of their operations and information technologies. In addition to the

electricity and oil and natural gas versions, a sector-agnostic C2M2 version has been created for industry at large.

Since the inception of the C2M2 program in June 2012, more than 1,100 C2M2 toolkits have been distributed, many to domestic energy sector companies. The Department is currently working with industry to update the model.

Energy Sector - Cybersecurity Framework Implementation Guidance
Executive Order 13636, Improving Critical Infrastructure Cybersecurity (February 2013), directed 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 Framework 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.

B1. How can changing technology (e.g., cloud computing, virtualization, "Internet of Things," "Industrial Internet of Things") introduce new vulnerabilities that may impact the security of the Bulk-Power System? And B2. How could cloud computing, virtualization, and other technologies be deployed securely to help manage the emerging grid?
Emerging technologies designed or deployed without security and resilience requirements may introduce vulnerabilities. Digitalization and cybersecurity must move forward in unity. The Department's cyber research and development efforts include a focus on secure and resilient design for emerging technologies, and exploring architecture redesign alternatives for existing technologies so energy delivery systems can adapt to survive while sustaining critical functions.

DOE is partnering with the energy sector to strengthen cybersecurity between the cloud and grid-edge devices. Additionally, DOE supports research partnerships that explore the use of virtualization to rapidly isolate and mitigate a cyber attack against power system applications while sustaining critical functions.

C1. The Commission engages with other agencies and industry in mitigating the risk posed by cyber threats – including promoting information sharing, identifying and assessing threats, sharing lessons learned and best practices. How can we improve these efforts?
Office of Cybersecurity, Energy Security, and Emergency Response
Recognizing the importance of cybersecurity to national security, DOE recently announced the standup of the Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

CESER is comprised of two former Office of Electricity Delivery and Energy Reliability (OE-predecessor) divisions, Infrastructure Security and Energy Restoration (ISER) and Cybersecurity for Energy Delivery Systems (CEDS). This reorganization allows the Department to provide greater visibility, accountability, and flexibility in safeguarding our energy infrastructure.

CESER is designed to elevate coordinated preparedness and response with our partners in the private sector, as well as government at every level, including the Commission.

Prepare. Respond. Recover.
The ISER Division coordinates a national effort to secure U.S. energy infrastructure against all hazards, reduce impacts from disruptive events, and assist industry with restoration activities. ISER works closely with the electricity and oil and natural gas industries, other Federal agencies, and State, Local, Tribal, and Territorial communities to advance national energy security and prepare for, respond to, and recover from evolving threats.

Prepare.
Emerging threats make energy infrastructure security a constantly evolving challenge. ISER's programs help the energy sector understand and prepare for a range of potential risks. Energy sector exercises bring together stakeholders at the national, regional, and local level to identify gaps in energy assurance planning, better understand interdependencies between energy and other sectors, and build and strengthen networks across the energy emergency response community.

Respond.
ISER plays a pivotal role in responding to severe incidents that affect the energy sector. From Superstorm Sandy to threats posed by electromagnetic pulses and cyber intrusions, ISER addresses a full range of hazards in close coordination with infrastructure owners and operators, state and local government, and our Federal partners. During a Presidentially declared energy sector emergency related to cyber, ISER facilitates the Secretary of Energy's authorities to direct actions to protect the safety and well-being of the American people.

Recover.
In a landscape of ever-evolving threats, education, diligence, and innovation are vital. ISER illuminates risks to critical energy infrastructure by working with key stakeholders to characterize potential threats and hazards and explore mitigation strategies. ISER works with DOE's National Laboratories, industry groups, and other Federal agencies to understand the most critical vulnerabilities of the electricity and oil and natural gas industries, and where and how the Federal Government can engage most effectively to enhance preparedness and response capabilities.

Research and Development
For more than a decade, DOE, through its CEDS Program, has partnered with the energy sector to advance cybersecurity R&D specifically designed to reduce cyber risks to energy delivery infrastructure. The CEDS program cost-shares the earlier stage, high-risk/high-reward research for which a business case may not be readily apparent but can lead to advanced cyber resilience technologies imperative for national security.

CESER's cybersecurity R&D program aligns activities with Federal priorities as well as the strategy and milestones articulated in the Multiyear Plan, which envisions resilient energy delivery control systems designed, installed, operated, and maintained to survive a cyber incident and sustain critical functions.

The CESER cybersecurity R&D program was designed to assist energy sector asset owners by developing cybersecurity solutions for energy delivery systems through a focused research and development effort. CESER co-funds projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems. These research partnerships are helping to prevent, detect, and mitigate the consequences of a cyber-incident for the energy delivery systems of today and tomorrow.

Examples:

- *Prevent attempted misuse of the Energy Delivery System (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.
- *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.
- *Mitigate the extent and consequences of a cyber incident.* DOE research partnerships are advancing tools and technologies that help power plants detect patterns of operation indicative of a cyber incident and accommodate to continue providing power while the cyber-attack is isolated and eradicated.

D1. How can cyber incident response plans be improved to address the evolving cyber threat landscape? For example, when a cyber system is compromised, antimalware software may not identify the system as compromised, and the only indicator may be the system's abnormal behavior.

Incident Response plans are evolving documents that are constantly improved, especially after incidents or exercises. The DOE hosts and supports many energy sector and cross-sector cybersecurity exercises, e.g., GridEx, CyberStorm, and Liberty Eclipse. These exercises provide an opportunity for owners, operators, regulators, ISACs, and government stakeholders to practice, test, and improve incident response plans, processes, and procedures.

CESER's research and development is working on technology solutions to prevent execution of commands with potential negative operational consequences. CESER also supports research partnerships that are developing technologies to detect deviations from normal, expected operating behavior, to determine if this abnormal behavior is a result of a malicious cyber attempt and mitigate the attempt before the disruption of energy delivery.

E2. What role can the voluntary development, application, and sharing of best practices play?

Voluntary best practices developed with public and private sector collaboration help improve the security posture of the entire ecosystem. While regulations provide an essential baseline for regulated entities, voluntary partnerships can help both regulated and nonregulated organizations share best practices that address the rapidly changing threat landscape in accordance with their risk management approach.

Conclusion

Cyber threats continue to evolve and DOE is working diligently to eliminate and mitigate the potential consequences of these threats. Our multiple efforts, including DOE's establishment of the CESER office, advance the vision of resilient energy delivery systems designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions. DOE's long-term cybersecurity vision will positively impact our national security as we continue to meet the ever changing cyber landscape as highlighted by our National Intelligence Agencies.