Testimony of Acting Assistant Secretary Patricia Hoffman

Office of Electricity Delivery and Energy Reliability

U.S. Department of Energy

Before the

Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection

House of Representatives

October 3, 2017

Introduction

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Subcommittee, thank you for the opportunity to discuss the continuing threats facing our national energy infrastructure and the Department of Energy's (DOE's) role in supporting the cybersecurity of the nation's energy infrastructure. C ybersecurity and the resilience of the energy sector is one of the Secretary's top priorities and a major focus of the Department.

Our economy, national security, and even the well-being of our citizens depend on the reliable delivery of electricity. The mission of the Office of Electricity Delivery and Energy Reliability (DOE-OE) – which I oversee in my roles as the Acting Under Secretary for Science and Energy and Acting Assistant Secretary for DOE-OE – is to strengthen, transform, and improve energy infrastructure to ensure access to reliable and secure sources of energy. The Secretary of Energy and DOE are committed to working with our public and private sector partners to protect the Nation's critical energy infrastructure from physical security events, natural and man-made disasters, and cybersecurity threats.

DOE's Role as the Energy Sector's "Sector Specific Agency"

In preparation for, and response to, cybersecurity threats, the Federal government's operational framework is provided by Presidential Policy Directive 41 (PPD-41). A primary purpose of PPD-41 is to clarify the roles and responsibilities of the Federal Government during a "significant cyber incident," which are described as cyber incidents that are "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."

Under the PPD-41 framework, as the Sector Specific Agency (or SSA) for cybersecurity of the energy sector, DOE works jointly with other agencies and private sector organizations, including the Federal government's designated lead agencies for coordinating the response to significant cyber incidents by protecting assets and countering threats: the Department of Homeland Security (DHS) acting through the National Cybersecurity and Communications Integration Center (NCCIC) and the Department of Justice (DOJ), acting through the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force, respectively. In the event of a cybersecurity emergency in the energy sector, closely aligning DOE's activities with those of our partners at DHS and DOJ helps to ensure that DOE's deep expertise with the sector is appropriately leveraged.

Under *Presidential Policy Directive-21 (PPD-21): Critical Infrastructure Security and Resilience*, later codified in part in the Fixing America's Surface Transportation Act, DOE is designated as the SSA for cybersecurity of the energy sector. As the SSA, DOE coordinates with DHS and other federal agencies and collaborates with industry and state, local, tribal and territorial partners on matters of cyber resilience, incident response, and planning. For any risk to the energy sector, DOE thus acts to ensure unity of effort across government, including states, and industry partners.

In addition, DOE serves as the lead agency for Emergency Support Function 12 (ESF-12) under the National Response Framework. As the lead for ESF-12, DOE is responsible for facilitating the restoration of damaged energy infrastructure. The Department works with industry and Federal, state, and local partners to facilitate response and recovery. Combining DOE roles as the SSA in cybersecurity with national response ensures incidents with both cyber and physical impacts can be coordinated for the energy sector.

In extreme cases, the Department can use its legal authorities such as those in the Federal Power Act, as amended by the Fixing America's Surface Transportation (FAST) Act, to assist in response and recovery operations. Congress enacted several important new energy security measures in the FAST Act as it relates to cybersecurity. The Secretary of Energy was provided a new authority, upon declaration of a "Grid Security Emergency" by the President, to issue emergency orders to protect or restore critical electric infrastructure or defense critical electric infrastructure. This authority allows DOE to respond as needed to the threat of cyber and physical attacks on the grid.

DOE is working to address public comments received regarding the rules of procedure to issue an order under this new authority. The Grid Security Emergency authority is unique to DOE and an important element in partnering with DHS and DOJ to fully address the cybersecurity risks to the energy sector.

The Special Nature of Energy Security Cybersecurity

Cyberattacks targeting "information technology" or IT, including computing and business applications, 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 are growing increasingly common. The energy sector is not immune to such attacks.

However, our adversaries understand that the energy sector is a valuable target not because of its IT systems, but because of the assets that the sector controls. Accordingly, we have seen an increased interest in vulnerabilities of the "operating technology," or OT, of energy delivery systems and other critical infrastructure as well. OT systems consist of industrial control systems (or ICS), programmable logic controls, and its associated supervisory control and data acquisition software (known as SCADA). The heavy use of OT systems has made electric utilities, oil and natural gas providers, hydro and nuclear facilities, and water utilities prime targets for OT-related cyber-attacks. The disruption of any one of these is not only inherently problematic, it also hampers the ability to respond to any type of emergency event.

The Department's focus on OT systems specific to the energy sector makes our activities both distinct from, and complementary to, the activities of DHS and our other Federal agency partners. The cybersecurity of energy sector OT systems requires specific and focused attention because of their need for extremely high reliability and availability, the fact that any significant reduction in the speed of the systems is unacceptable, and because these systems are so critical to underpinning the nation's economic health, public safety, and national security.

In December 2015, the first known successful cyber-attack on power grid OT took place in Ukraine. Over 225,000 residents were left without power for several hours in the coordinated attack, and a second attack occurred in December 2016 that left portions of Kiev without electricity. More recently, publicly-available information about threats such as the Crash Override malware used in Ukraine and the nation-state activities described under the name "Dragonfly 2.0" are just two of many examples that illustrate the threat to the nation's energy infrastructure is real and growing more concerning by the day.

Importance of Partnerships

Before I describe the details of the Department's activities in support of the energy sector's cybersecurity, I must first focus on the most foundational aspect of our activities: partnerships. The Federal government does not own or operate the vast majority of the assets in the nation's energy sector, and DOE does not hold a monopoly on protecting the nation's critical infrastructure from cyber threats. As such, we cannot function effectively unless we have strong partnerships throughout the public and private sectors and with our Federal colleagues at DHS and other law enforcement- and national security-oriented agencies.

DOE has collaborated with the energy sector for nearly two decades in voluntary public-private partnerships that engage energy owners and operators at all levels – technical, operational, and executive, along with state and local governments – to identify and mitigate physical and cyber risks to energy systems.

These partnerships are 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. These relationships acknowledge the special security challenges of energy delivery systems and leverage the distinct technical expertise within industry and government to develop solutions.

The security and integrity of energy infrastructure is both a state and Federal government concern because energy underpins the operations of every other type of critical infrastructure; the economy; and public health and safety. The owners and operators of energy infrastructure, however, 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.

When the lights go out or gasoline stops flowing in pipelines, the first responder is usually not the state or Federal Government but, rather, industry or local government. This is why public-private partnerships regarding cybersecurity are paramount – they recognize the distinct roles and capabilities of industry and government in managing our critical energy infrastructure risks.

In the Energy Sector, the core of critical infrastructure partners consists of 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. The EGCC, led by DOE and co-chaired with DHS, is where the interagency partners, states, and international partners come together to discuss the important security and resilience issues for the energy sector. This forum ensures that we're working together in a whole-of-government response.

As defined in the National Infrastructure Protection Plan, the industry coordinating councils or "SCCs" are created by owners and operators and are self-organized, self-run, and self-governed, with leadership designated by the SCC membership. The SCCs serve as the principal collaboration points between the government and private sector owners and operators for critical infrastructure security and resilience coordination and planning, as well as a range of sector-specific activities and issues.

The SCCs, EGCC, and associated working groups operate under DHS's Critical Infrastructure Partnership Advisory Council (CIPAC) framework, which provides a mechanism for industry and government coordination. The public-private critical infrastructure community engages in

open dialogue to mitigate critical infrastructure vulnerabilities and to help reduce impacts from threats.

DOE's Cybersecurity Strategy for the Energy Sector

To address these challenges, it is critical for us to be proactive and cultivate what I call an ecosystem of resilience: a network of producers, distributors, regulators, vendors, and public partners, acting together to strengthen our ability to prepare, respond, and recover. We continue to partner with industry, DHS and other Federal agencies, states, local governments, and energy stakeholders broadly to quickly identify threats, develop capabilities to support mitigation strategies, and rapidly respond to any disruptions.

DOE plays a critical role in supporting energy sector cybersecurity to enhance the security and resilience of the Nation's energy infrastructure. As part of a comprehensive strategy for energy resilience, the Department is focusing cyber support efforts to: enhance visibility and situational awareness of operational networks; increase alignment of cyber preparedness and planning across local, state, and Federal levels; and leverage the expertise of DOE's National Labs to drive cybersecurity innovation.

Enhance visibility and situational awareness of operational networks

It is necessary for partners in the Energy Sector and the government to share emerging threat data and vulnerability information to help prevent, detect, identify, and thwart cyber-attacks more rapidly. An example of this type of collaboration is the Cybersecurity Risk Information Sharing Program (CRISP), a voluntary public-private partnership that is primarily funded by industry, administered by the Electricity Information Sharing and Analysis Center (E-ISAC), and enhanced by DOE through intelligence analysis by DOE's Office of Intelligence and Counterintelligence. One of DOE's National Laboratories – the Pacific Northwest National Laboratory – is a key partner for the E-ISAC in accomplishing the goals of the CRISP program.

The purpose of CRISP is to share information among electricity subsector 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 the high-level cyber risks. Current CRISP participants provide power to over 75 percent of the total number of continental United States electricity customers. The Department is currently in the early stages of taking the lessons learned from CRISP and developing an analogous capability to monitor network traffic on OT networks.

If CRISP has demonstrated one finding to DOE, the E-ISAC, and our industry partners, it is that continuous monitoring of critical networks and shared situational awareness is of utmost importance in protecting against malicious cyber activities. Programs such as CRISP are critical for facilitating the identification of and response to advanced persistent threats targeting the energy sector.

Advancing this project to improve situational awareness of OT networks is a key focus of DOE's current activities. Observing anomalous traffic on networks – and having the ability to store and retrieve network traffic from the recent past – can be the first step in stopping an attack early in the cyber kill chain. Continuous monitoring of IT and OT networks, in coordination with Federal partners and industry, is a critical component of protecting the nation against cyber threats.

Increase alignment of cyber preparedness and planning across local, state, and Federal levels

As the Energy SSA, DOE works at many levels of the electricity, petroleum, and natural gas industries. We interact with numerous stakeholders and industry partners to share both classified and unclassified information, discuss coordination mechanisms, and promote scientific and technological innovation to support energy security and reliability. By partnering through working groups between government and industry at the national, regional, state, and local levels, DOE facilitates enhanced cybersecurity preparedness.

As a recent example, DOE-OE and the National Association of Regulatory Utility Commissioners (NARUC) sponsored the third edition of a cybersecurity primer for regulatory utility commissioners. This document was published in January of this year and is publicly available on the NARUC Research Lab website, benefitting not only regulators, but state officials focused on the sector as well.

The updated cyber primer provides best practices, access to industry and national standards, sample questions, and easy reference materials for Commissions in their engagements with utilities to ensure their systems are resilient to cyber threats.

We are continuing to work with the NARUC Research Lab to support regional trainings on cybersecurity throughout the year, with the goal of building commissioner and commission staff expertise on cybersecurity so they ensure cyber investments are both resilient and economically sound.

DOE also continues to work closely with our public and private partners to ensure that our response and recovery capabilities fully support and bolster the actions needed to help ensure the reliable delivery of energy. We continue to coordinate with industry through the SCCs to synchronize DOE and industry cyber incident response playbooks.

DOE-OE also engages directly with our public and private sector stakeholders to help ensure we all are prepared and coordinated in the event of a cyber incident to the industry. Innovation and preparedness are vital to grid resilience. This past December, DOE and the National Association of State Energy Officials (NASEO) co-hosted the Liberty Eclipse Exercise in Newport, Rhode Island, which focused on a hypothetical cyber incident that cascaded into the physical world, resulting in power outages and damage to oil and natural gas infrastructure. The event featured 96 participants from 13 states, and included representatives from state energy offices, emergency management departments, utility commissions, as well as Federal partners, such as FEMA, and private sector utilities and petroleum companies.

In November, we are looking forward to participating in GridEx IV, which is the biennial exercise lead by the North American Electric Reliability Corporation (NERC) and is designed to simulate a cyber and physical attack on electric and other critical infrastructures across North America. Coordination with Federal partners and participation in preparedness activities enable DOE to identify gaps and develop capabilities to support cyber response as the SSA.

Leverage the expertise of DOE's National Labs to drive cybersecurity innovation

Beyond providing guidance and technical support to the energy sector, DOE-OE also supports an R&D portfolio designed to develop advanced tools and techniques to provide enhanced cyber protection for key energy systems. Intentional, malicious cyber threat challenges to our energy systems are on the rise in both number and sophistication. This evolution has profound impacts on the energy sector.

Cybersecurity for energy control and OT systems is much different than that of typical IT systems. Power systems must operate continuously with high reliability and availability. Upgrades and patches can be difficult and time consuming, with components dispersed over wide geographic regions. Further, many assets are in publicly accessible areas where they can be subject to physical tampering. Real time operations are imperative and latency is unacceptable for many applications. Immediate emergency response capability is mandatory and active scanning of the network can be difficult.

The CEDS R&D program is designed to assist the energy sector asset owners by developing cybersecurity solutions for energy delivery systems through a focused research and development effort. DOE-OE co-funds projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems. These research partnerships are helping to detect, prevent, and mitigate the consequences of a cyber-incident for our present and future energy delivery systems. Of course, our National Laboratories are critical partners in executing this work.

To select cybersecurity R&D projects, DOE constantly examines today's threat landscape and coordinates with partners, like DHS, to provide the most value to the energy sector while minimizing overlap with existing projects. For example, the Artificial Diversity and Defense Security (ADDSec) project will develop solutions to protect control system networks by constantly changing a network's virtual configuration, much like military communications systems that rapidly change frequencies to avoid interception and jamming. As a result, ADDSec can harden networks against the mapping and reconnaissance activities that are the typical precursors to a cyberattack.

Another project, the Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF), is designed to anticipate the impact a command will have on a control system environment. If the commands would result in damage to the system or other negative consequences, CODEF will have the ability to prevent their execution. This type of solution is especially intriguing as it can detect malicious activity regardless of the source, be it an insider threat or an external actor.

Since 2010, DOE-OE has invested more than $210 million in cybersecurity research, development, and demonstration projects that are led by industry, universities, and the National Laboratories. These investments have resulted in more than 35 new tools and technologies that are now being used to further advance the resilience of the Nation's energy delivery systems.

Conclusion

Threats continue to evolve, and DOE is working diligently to stay ahead of the curve. The solution is an ecosystem of resilience that works in partnership with local, state, and industry stakeholders to help provide the methods, strategies, and tools needed to help protect local communities through increased resilience and flexibility. To accomplish this, we must accelerate information sharing to inform better local investment decisions, encourage innovation and the use of best practices to help raise the energy sector's security maturity, and strengthen local incident response and recovery capabilities, especially through participation in training programs and preparedness exercises.

Building an ecosystem of resilience is – by definition – a shared endeavor, and keeping a focus on partnerships remains an imperative. DOE will continue its years of work coordinating with DHS and fostering vital energy sector relationships and investing in technologies to enhance security and resilience in order to support industry efforts to respond to, and recover quickly from all threats and hazards.

I appreciate the opportunity to appear before the Subcommittee to discuss the cybersecurity of the energy sector. I would, however, be remiss if I did not take a moment to stress that the interdependent nature of our infrastructure requires that all sectors be constantly focused on

improving their cybersecurity posture. Collaboration among DOE, DHS, and the rest of the Federal family is absolutely critical to ensuring that we remain both ahead of the curve and resilient to any potential cyberattack. DOE, as always, looks forward to our continued partnership to share best practices, collaborating where appropriate and possible, and helping to protect our civilian infrastructure from the nation's cyber adversaries.