Testimony of Acting Assistant Secretary Patricia Hoffman

Office of Electricity Delivery and Energy Reliability

U.S. Department of Energy

Before the

Committee on Energy and Natural Resources

United States Senate

April 4, 2017

Introduction

Chairman Murkowski, Ranking Member Cantwell, and Members of the Committee, thank you for the opportunity to discuss the continuing threats facing our national energy infrastructure and the Department of Energy's role under the authorities specified in the Fixing America's Surface Transportation – or FAST – Act. At the Department of Energy (DOE), focusing on cybersecurity and the resilience of energy is one of the Secretary's top priorities.

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, including the electric power grid, from physical security events, natural and man-made disasters, and cybersecurity threats.

Over the past decade, the Nation's energy infrastructure has become a major target of both physical and cyber-attacks. The frequency, scale, and sophistication of cyber threats have increased and attacks can be easier to launch. Cyber incidents have the potential to interrupt energy services, damage highly specialized equipment, and threaten human health and safety. As a result, energy cybersecurity and resilience has emerged as one of the Nation's most important security challenges and fostering partnerships with public and private stakeholders will be of utmost importance in this work.

DOE FAST Act Authority

DOE's role in energy sector security is established in statute and executive action. In 2015, through the FAST Act, Congress assigned DOE as the lead Sector-Specific Agency (SSA) for cybersecurity for the energy sector.

The FAST Act also gave the Secretary of Energy 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

support energy sector preparations for and responses to cyber, electromagnetic pulse (EMP), geomagnetic disturbance (GMD), and physical attack threats.

EMP events are a national concern due to the potential for widespread impact and extended outages from, for example, a high-altitude nuclear burst. To promote government and industry sharing of scientific and testing results, last July, DOE and the Electric Power Research Institute (EPRI) released a Joint Electromagnetic Pulse Resilience Strategy (Joint Strategy). This Joint Strategy is intended to drive efforts to reduce EMP vulnerabilities and improve the response and recovery after EMP events, thus minimizing adverse impacts and improving grid resilience. Following development of the Joint Strategy, both DOE and EPRI committed to developing separate, but coordinated, Action Plans. EPRI's plan focused on industry actions and DOE's on departmental actions to mitigate EMP risks. Although the two Action Plans were developed independently, DOE and EPRI collaborated closely to ensure that the plans complement one another and avoid duplication of effort and implementation of both action plans are underway.

GMDs are naturally occurring phenomena relating to space weather and may have significant impacts on electrical and electronic equipment and systems, including high-frequency radio communications, global navigation satellite systems, long-haul telecommunications/internet exchange carrier lines, and electric power transmission. GMDs can have multiple effects on the electric grid, such as damaged equipment and loss of power over large areas, and can also lead to losses of communications. Significant gaps exist in the understanding of and protection against GMD effects on the electric grid, as well as in optimizing operations to limit GMD effects. Current DOE efforts relate to obtaining better data on GMDs, developing an approach to monitoring the grid and its components for GMD effects, and testing the effectiveness of blocking devices.

Importance of Cybersecurity for Energy Systems and Cybersecurity Threats

In addition to the authorities in the FAST Act related to cybersecurity, we have worked with interagency partners to ensure that our cyber response activities are consistent and integrated with broader national preparedness and incident response efforts. This allows our response to a cyber incident to seamlessly integrate with actions taken to address physical consequences caused by malicious cyber activity.

Principles of cybersecurity often start with computer servers and desktops, the heart of systems generally referred to as "information technology," or IT. As we are all aware, hackers are targeting computing technology and business applications to cause disruptions, obtaining access to email accounts and personal information, exfiltrating data to release to the world at large, and exploiting information for private gain. The energy sector is not immune to such attacks.

In the 2012 Shamoon attack, weaponized malware hit 15 state bodies and private companies in Saudi Arabia, wiping more than 35,000 hard drives of Saudi Aramco, from which the company took more than two weeks to recover. And again in January of this year, Shamoon 2 hit three state agencies and four private sector companies in Saudi Arabia, leaving them offline for at least 48 hours.

While the Shamoon and other similar-style attacks have targeted IT systems, the energy sector is also targeted because of the assets they control and the value they represent. Accordingly, this has also 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.

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. These two cyber-attacks demonstrated the real world, physical impacts that can occur through cyber means.

Ecosystem of Resilience

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, Federal agencies, states, local governments, and other stakeholders to quickly identify threats, develop in-depth strategies to mitigate those threats, and rapidly respond to any disruptions.

DOE plays a critical role in supporting industry functions in several ways: providing partnership mechanisms that support collaboration and trust; leveraging government capabilities to gather intelligence on threats and vulnerabilities, and share actionable intelligence with energy owners and operators in a timely manner; developing supportive tools that encourage cybersecurity best practices in the energy sector; developing tools and capabilities to conduct risk analysis; supporting energy sector incident coordination and response; and, supporting innovation and R&D for next-generation physical-cyber systems.

Importance of Partnerships

The Department of Energy 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, 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 the Department of Homeland Security'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.

Strengthening Energy Sector Cybersecurity Preparedness

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 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.

Cybersecurity Risk Information Sharing Program

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 funded by industry, administered by the Energy Sector Information Sharing and Analysis Center (E-ISAC), and supported by DOE in both intelligence analysis through DOE's Office of Intelligence and Counterintelligence and from an R&D standpoint by DOE-OE. 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 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 the high-level cyber risks. Current CRISP participants provide power to over 75 percent of the total number of continental United States electricity customers.

Cybersecurity Capability Maturity Model

Another example of how DOE supports the cyber posture of the energy industry is DOE-OE's Electricity Subsector Cybersecurity Capability Maturity Model (C2M2) to help private sector owners and operators better evaluate their cybersecurity capabilities. The C2M2 evaluation allows organizations – regardless of size, type, or industry – to evaluate, prioritize, and improve their own cybersecurity capabilities.

DOE and the oil and natural gas (ONG) subsector collaborated extensively to develop a C2M2 version specifically for them. The model was tested and refined for the subsector through pilot evaluations across upstream, midstream, and downstream ONG companies.

Owners and operators across the subsector are utilizing these best practices. The C2M2 evaluation workshops facilitated by the American Gas Association are a strong example of their use.

Since the C2M2 program's inception in June 2012, more than 1,100 C2M2 toolkits have been distributed, many to domestic energy sector companies. The tool enables voluntary, consistent measurement of the maturity of an organization's cybersecurity capabilities. This is a comprehensive and credible approach that energy sector companies can use to improve their cybersecurity posture. In addition to the electricity and ONG versions, a sector agnostic C2M2 version has been created for industry at large.

As we move forward, we continue to engage stakeholders from both the electricity and ONG subsectors to leverage insights gathered from industry to further enhance the C2M2 model.

National Association of Regulatory Utility Commissioners Primer

DOE-OE also works to provide guidance to the Nation's policy makers on improving their cybersecurity. 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.

Coordinating Cyber Incident Response and Recovery

Cyber Incident Coordination

The emergency authorities established under the FAST Act enable the Secretary to undertake certain actions within the context of a Grid Security Emergency. These actions require a swift and coordinated response in collaboration with industry partners to secure critical energy infrastructure and to support response and restoration efforts.

In the event of a significant cyber incident, a national Cyber Unified Coordination Group (UCG) would be activated. The Department of Homeland Security's National Cybersecurity and Communications Integration Center, or NCCIC, would be designated as the Asset Response Lead, the National Cyber Investigative Joint Task Force, or NCIJTF, would be designated as the Threat Response Lead and the Cyber Threat Intelligence Integration Center, or CTIIC, would be responsible for leading intelligence support. Under the UCG, DOE, in its role as the energy sector SSA, would be responsible for leading sector coordination and enabling sector specific technical assessments and assistance.

We continue 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 the SCCs to synchronize DOE and industry cyber incident response playbooks.

Cyber Exercises

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 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 addition to building up participant knowledge of the cyber threat and the roles and responsibilities of the government in a cyber incident, it brought stakeholders from all aspects of the energy emergency management spectrum together to further build relationships and share expertise.

As a result of this event, a number of states are now looking to update their energy assurance and incident response plans to include more robust coordination of cyber incidents in the energy sector.

Accelerating Game-Changing Cyber Research, Development, and Deployment

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.

DOE-OE's Cybersecurity for Energy Delivery Systems (CEDS) R&D program aligns activities with Federal and private sector priorities, envisioning resilient energy delivery control systems designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

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.

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.

Closing

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 disaster 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 fostering these relationships and investing in technologies to enhance security and resilience, ensuring the electric power grid continues to be able to withstand, respond, and recover quickly from all threats and hazards.