**Written Testimony of Acting Assistant Secretary Patricia Hoffman**

**Office of Electricity Delivery and Energy Reliability**

**U.S. Department of Energy**

**Before the**

**Subcommittee on Energy**

**Committee on Energy and Natural Resources**

**United States Senate**

**March 28, 2017**

Chairman Gardner and Ranking Member Manchin, and Members of the Subcommittee, thank you for continuing to highlight the importance of a resilient electric power grid and for the opportunity to provide the initial views of the Department of Energy (DOE) on S. 79, the Securing Energy Infrastructure Act. DOE supports the goals of S. 79, which are consistent with the Department's ongoing role in helping to ensure a resilient, reliable, and flexible electricity system in an increasingly challenging environment. DOE would like to work with the sponsor and this Committee to offer additional input on the bill as discussed later in this testimony.

Our economy, national security, and even the well-being of our citizens depend on the reliable delivery of electricity. I know the Secretary is personally engaged in the cybersecurity issues facing the energy sector. Under his leadership, the Department's role in cybersecurity is a very high priority. The mission of the Office of Electricity Delivery and Energy Reliability (DOE-OE) is to strengthen, transform, and improve energy infrastructure to ensure access to reliable and secure sources of energy. We 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 breaches.

Over the past decade, the Nation's energy infrastructure has become a major target of cyberattacks. The frequency, scale, and sophistication of cyber threats have increased and attacks have become 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.

## Importance of Cybersecurity for Energy Systems

Initial thoughts of cybersecurity often turn to computer servers and desktops, information technology (IT). Hackers target computing technology and business applications to cause disruptions – obtaining access to email accounts and personal information, data exfiltration to be released to the world at large. 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.

These cyberattacks affect not only business systems, but can also target the operating technology of energy delivery systems and other critical infrastructure as well. Electric utilities, oil and natural gas providers, hydro and nuclear facilities, along with financial, water, communications, transportation, and healthcare sectors are prime targets for 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 a power grid 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. Domestically, the 2013 cyber-attack on the Bowman Dam in Rye, New York illustrated the multitude of targets available to and being surveilled by hackers.

**The 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, local governments, and other stakeholders to quickly identify threats, develop in-depth strategies to mitigate those threats, and rapidly respond to any disruptions. The DOE National Laboratories have been the keystone in many endeavors to address new and existing cybersecurity concerns.

**Importance of Partnerships**

The U.S. 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.

The first responder when the lights go out or gasoline stops flowing in the pipelines is not immediately the state or Federal Government; rather, it is industry. 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.

Two of those partnerships are the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council, extremely strong partnerships in which DOE-OE is engaged. Each serves as a primary conduit between industry and the government to prepare for, and respond to, national-level disasters or threats to critical infrastructure. Through these relationships, cybersecurity issues can be addressed more completely and with multiple stakeholder input.

**DOE Authority in Cybersecurity**

DOE's role in energy sector cybersecurity is established in statute and executive action. In 2015, through the Fixing America's Surface Transportation Act (FAST Act), Congress assigned DOE as the lead Sector-Specific Agency (SSA) for cybersecurity for the energy sector, building upon previous Presidential Policy Directives (PPD). PPD-41 issued in July 2016, further clarified the role of DOE as a SSA during a significant cyber incident.

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 respond as needed to the threat of cyber and physical attacks on the grid. DOE is developing a proposed rule of procedure regarding this new authority.

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: providing partnership mechanisms that support collaboration and trust; developing supportive policies that encourage voluntary cybersecurity in the energy sector; developing tools and capabilities to conduct risk analysis; leveraging government capabilities to gather intelligence on threats and vulnerabilities, and share actionable intelligence with energy owners and operators in a timely manner; supporting energy sector incident coordination and response; facilitating the development of cybersecurity standards; and, promoting and supporting innovation and R&D for next-generation physical-cyber systems.

**DOE's Research and Development Activities in Cybersecurity and Resilience through the National Laboratories**

Intentional, malicious challenges to our energy systems are on the rise and we are seeing threats continually increase in number and sophistication. This evolution has profound impacts on the energy sector.

Cybersecurity for energy control systems is much different than 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. As a result, our National Laboratories conduct cybersecurity R&D taking into account these systemic characteristics.

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.

Through all of these R&D efforts, our National Laboratories have been – and continue to be – heavily engaged in their own efforts and in partnerships with academia and industry stakeholders. The following are examples of the types of cybersecurity advancements currently pursued at our National Laboratories, building off of successful cybersecurity tools and technologies already developed:

- Argonne National Laboratory is currently working on a resilient self-healing cybersecurity framework for the power grid that will leverage Wide-Area Monitoring, Protection, and Control to prevent and mitigate cyber-attacks. The project will develop tools to prevent and mitigate cyber-attacks and enhance the resilience of the bulk power system.

- Argonne is also working on a cloud and outsourcing security framework for power grid applications as well as cybersecurity for distributed energy resources (DER). This project will help ensure that implementation of cloud-based architecture and DER in the energy sector are deployed with security built-in to maintain resilience during cyber-attacks.

- An online tool being developed by Brookhaven National Laboratory will help utilities to detect, mitigate, and evaluate the potential impact of various cyberattack scenarios to reduce the risk that malicious compromise of essential forecasting data used for grid scheduling and operation might result in disruption of energy delivery.

- The Validation and Measuring Automated Response Project led by the Idaho National Laboratory is providing a cyber-incident response comparison capability and enabling industry to work towards an automated response capability to a cyber-incident and measuring the efficacy of automated response to drive future improvements.

- Lawrence Berkeley National Laboratory has an effort underway utilizing real-time micro-synchrophasor measurements and other telemetry in the distribution system to enhance identification and detection of current and future cybersecurity vulnerabilities in the power distribution grid to provide a more reliable, robust, scalable, and cost-effective means of detecting cyber-attack scenarios compared to traditional approaches.

- Pacific Northwest National Laboratory is developing visualizations that power system operators and/or cybersecurity professionals can use to make fast, accurate assessments of situations, enabling them to maintain situation awareness during unfolding events. The visualization tool will reduce the burden on the operators and enable them to make faster decisions and maintain cybersecurity situational awareness.

- Pacific Northwest National Laboratory is also working on a project evaluating existing Live Analysis monitoring and detection tools for energy delivery systems use. The research seeks to develop a tool that could provide evidence of anomalous cyber behavior on a live energy delivery system without interrupting energy delivery.

- The Artificial Diversity and Defense Security (ADDSec) project at Sandia National Laboratory is developing defensive technologies that randomly and automatically reconfigure energy delivery operational network parameters moment-by-moment to impede reconnaissance and cyber-attack planning. ADDSec will increase the security of both legacy and modern energy delivery systems by converting these traditionally static systems into moving targets.

- "Sophia" is a tool researched and developed by the Idaho National Laboratory (INL) that enhances continuous situational awareness of energy delivery control system communications and helps detect potential cybersecurity concerns. The technology helps strengthen the cybersecurity of our Nation’s energy infrastructure today and of note is the fact INL successfully transitioned this technology to commercial use through a licensing agreement.

- Similarly, Oak Ridge National Laboratory licensed the developed "Hyperion" software technology. This software can quickly recognize malicious code even if the specific program has not been previously identified as a threat and before it has a chance to execute.

- Also in the process of transitioning to commercialization is Sandia National Laboratory's "CodeSeal." CodeSeal is a cryptographically secure code obfuscation technology that prevents reverse engineering, or malicious modification of energy delivery system code, even if that code is executed on a compromised system.

**S. 79**

The U.S. Department of Energy is tremendously proud of the role our National Laboratories have played in the advancement of cybersecurity technologies for our Nation's energy infrastructure. We also appreciate the opportunity to provide technical assistance on S. 79. It appears that the intent of the legislation is to strengthen our cybersecurity posture by directing the National Laboratories to undertake a study of the systems most critical to national security and to the grid.

In considering the legislation, DOE notes that many energy sector entities already conduct such assessments to comply with mandatory Critical Infrastructure Protection standards set by the Federal Energy Regulatory Commission and the North American Electric Reliability Corporation or as part of their due diligence in ensuring their system is reliable and capable of providing uninterrupted service in the face of today's evolving cyber threat landscape.

**Conclusion**

Cyber threats to the energy sector 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 the Nation's energy infrastructure through increased resilience and flexibility.

One of the cornerstones to this ecosystem of resilience is the DOE National Laboratories and the significant contributions they provide through their cybersecurity technology advancements. 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 resilience and security, ensuring the electric power grid continues to be able to withstand and recover quickly from disasters and attacks.