Testimony of 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

July 12, 2016

Chairman Risch 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. 3018, the Securing Energy Infrastructure Act. DOE supports the goals of S. 3018, 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 health and safety of our citizens depend on the reliable delivery of electricity. 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, secure, and clean 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

There are plenty of risks beyond cyber, including physical, severe weather, natural disasters, electromagnetic pulses (EMPs), aging infrastructure, and infrastructure interdependencies. In the face of these diverse threats, we can help ensure that the grid is poised to recover quickly following an incident. Fostering partnerships with public and private stakeholders plays a critical and necessary role in this work.

THE ECOSYSTEM OF RESILIENCE

A crucial factor to meeting these challenges is 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, other 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.

Our resilience efforts are further bolstered by our broader grid modernization activities, including our support of the research, development, and demonstration of advanced technologies and our work with state, local, tribal, and territorial stakeholders to help them improve their local

resilience and energy emergency response capabilities. Of the $4.5 billion that we invested in grid modernization through the American Recovery and Reinvestment Act (ARRA), $3.4 billion was used to help industry accelerate the deployment of advanced technologies that are now reducing costs and keeping the lights on more reliably and efficiently. This smarter grid is helping to prevent outages, reduce storm impacts, and restore service faster when outages occur.

Our model is partnerships first. We are all in this together. It is through working together that we continue to strengthen our ability to bounce back following an event.

PARTNERSHIPS FOR READINESS

DOE-OE has been working with utility owners and operators, regulators, and state and local officials across the country concerning threats to cybersecurity and other risks. Through these partnerships, we are providing tools, best practices, new technologies, and funds to support their many ongoing efforts.

We directly support preparedness efforts at the community level, in part through products and tools produced by our Infrastructure Security and Energy Restoration (ISER) division, to inform and educate state and local officials in their energy emergency preparedness activities. This is done through forums, training, and tabletop exercises for Federal, state, and local energy officials.

Cybersecurity and Resilience

Intentional, malicious challenges to our energy systems are on the rise. We are seeing threats continually increase in numbers and sophistication. This evolution has profound impacts on this sector, which is why we've made cybersecurity one of our highest priorities at DOE.

As there has been an increase in malicious cyber activity, we work closely with the energy sector to share cyber threat information. Since 2010, DOE-OE has invested more than $210 million in cybersecurity research, development and demonstration projects that are led by industry, universities and National Labs. Since then, more than 20 new technologies that our investments helped support are now being used to further advance the resilience of the Nation's energy delivery systems. For example, SecureSmart helps keep Smart Grid networks secure, and Hyperion helps keep power system applications secure.

All of OE's cybersecurity research initiatives are based upon industry involvement, joint funding through matching funds, and development with an end goal of practical use.

There are several examples of DOE-OE supported cybersecurity technologies tailored to respect the stringent operational requirements of the power grid, and to advantageously use the physics of energy delivery. One example is an industry-led research project that helps protection and control equipment check received commands to ensure these commands support the stability of grid operations and do not jeopardize grid stability[i]. Another example is DOE National Laboratory-led research that is designing cybersecurity awareness into the power system applications so malicious, adversarial manipulation of power system devices and applications can be identified and mitigated automatically.[ii]

The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership, co-funded by DOE-OE and industry that also focuses on building sector resilience. The purpose of CRISP is to collaborate with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information and to develop situational awareness tools that 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 National 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 U.S. electricity subsector customers.

Cybersecurity preparedness was part of the Smart Grid Investment Grants (SGIG) awarded by OE through American Recovery and Reinvestment Act. Each of the 99 projects that received funding was required to develop a cybersecurity plan. Participants included investor owned utilities, public power utilities, and cooperatives. This process truly raised the bar of awareness of cybersecurity risks and jumpstarted progress in cybersecurity protection actions and best practices.

Further, as part of the Administration's efforts to improve electricity subsector cybersecurity capabilities, DOE-OE and industry partners developed the Electricity Subsector Cybersecurity Capability Maturity Model (C2M2) to help private sector owners and operators better evaluate their cybersecurity capabilities. The C2M2 evaluation helps organizations prioritize and improve cybersecurity activities.

Since the C2M2 program's inception in June 2012, more than 900 C2M2 toolkits have been distributed, and industry adoption of the C2M2 is growing steadily. This is a comprehensive and credible approach that all energy sector companies can use to improve their cybersecurity posture. DOE-OE also released versions of the C2M2 for the oil and natural gas sector and for industry at large.

PARTNERSHIPS FOR RESPONSE

Our partnerships with private and public stakeholders also focus on quickly identifying threats, developing in-depth strategies to mitigate them and rapidly responding to any disruptions. With 90 percent of the Nation's power infrastructure privately held, coordinating and aligning efforts between the government and the private sector is the only viable path to success.

Under Presidential Policy Directive-21: Critical Infrastructure Security and Resilience and the Fixing America's Surface Transportation (FAST) Act (P.L. No. 114-94), DOE is the Sector-Specific Agency (SSA) for electrical infrastructure. The SSA plays the pivotal role of ensuring unity of effort and message across government partners, including the Department of Homeland Security, the Department of Defense, and DOE offices.

As the Energy SSA we also serve as the day-to-day Federal interface for the prioritization and coordination of activities to strengthen the security and resilience of critical infrastructure in the electricity subsector. This involves building, maintaining, and advancing our relationships and collaborative efforts with the energy sector. We have invested in public/private partnership

programs and initiatives that involve sharing real time information, assessing vulnerabilities, clarifying responsibilities, and engaging in training and exercises.

In addition, the Department of Energy serves as the lead agency for Emergency Support Function 12 (ESF-12) under the National Response Framework. As the lead for ESF-12, the DOE is responsible for facilitating the restoration of damaged energy infrastructure. During a response operation, the Department works with industry and Federal/state/local partners to:

- Assess disaster impacts on local and regional energy infrastructure;
- Coordinate asset delivery to repair damaged infrastructure;
- Monitor and report on restoration efforts; and
- Provide regular situational awareness updates to key decision makers in the Administration and our interagency partners.

To achieve these operational priorities, the Department deploys responders who work directly with the affected utilities and local officials on the ground during a disaster. The responders provide expertise on a variety of energy issues, and have direct access to our subject matter experts in Washington, DC who work with our interagency partners to coordinate the appropriate waivers, when needed, to further speed restoration efforts. In extreme cases, the Department can use its legal authorities under the Federal Power Act, Defense Production Act, and other statutes to assist in response and recovery operations.

Threats ranging from a fallen tree to a dedicated hacker from overseas can threaten the broader transmission system and the distribution system. When the power goes out, the local utility is the first responder. Should any threat or emergency exceed local public or private resources or require a full-blown national response, a utility CEO, a representative trade association member of the Electricity Subsector Coordinating Council (ESCC), the Electricity Information Sharing and Analysis Center (E-ISAC), or the Federal Government can request what is called a Crisis State Activity. Crisis State Activities are coordinated through the ESCC because, as with preparedness, we respond through partnerships. The ESCC is a group of leaders from across the electricity subsector that meet regularly with government to coordinate and share information. Together, we work toward collective actions to address the threat or risk.

Congress enacted several important new energy security measures in the FAST Act. 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 issue rules of procedure regarding this new authority.

PARTNERSHIPS FOR INNOVATION

Innovation and preparedness are vital to grid resilience. In January 2016, the DOE built upon its Grid Modernization Initiative – an ongoing effort that reflects the Obama Administration's commitment to improving the resiliency, reliability, and security of the Nation's electricity delivery system – by releasing a comprehensive new Grid Modernization Multi-Year Program Plan (MYPP). The MYPP, developed in close collaboration with a wide range of key external partners, lays out a blueprint for DOE's research, development, and demonstration agenda to

enable a modernized grid, building on concepts and recommendations from the first installment of the Quadrennial Energy Review (QER) and Quadrennial Technology Review (QTR).

For example, large power transformers are critical to grid resilience, and are ripe for innovation. These important grid assets can weigh hundreds of tons, are expensive, and are typically custom made with procurement lead times of a year or more. A significant number of damaged transformers from any type of hazard could result in a long-term impact on the overall resilience of the grid. The QER recognized the risks associated with the loss of large power transformers. The QER recommended that DOE work with other Federal agencies, states, and industry on an initiative to mitigate these risks. Approaches envisioned in the QER include the development of one or more strategic transformer reserves through a staged process, beginning with an assessment of technical specifications and whether new Federal regulatory authorities or cost-share are necessary and appropriate.

Secretary Moniz also announced last January an award of up to $220 million over three years, subject to congressional appropriations, to DOE's National Laboratories and partners to support critical research and development in advanced storage systems, clean energy integration, standards and test procedures, and a number of other key grid modernization areas. This Grid Modernization Laboratory Consortium effort recognizes regional differences and will strengthen regional strategies while defining a diverse and balanced national strategy. In addition to projects that address the needs of incorporating individual grid technologies like solar or energy storage, DOE is also developing crosscutting projects that have impact across multiple technologies. As Secretary Moniz said at the announcement, "Modernizing the U.S. electrical grid is essential to reducing carbon emissions, creating safeguards against attacks on our infrastructure, and keeping the lights on."

Energy storage is another key technology for whole-grid resilience. Energy storage fundamentally changes the relationship between when energy is produced and when it is consumed. The President's FY 2017 Budget Request supports OE's work on materials research, device development, demonstrations, and grid analysis to help transition selected energy storage technologies from R&D to industrially relevant scales with improved safety, industry acceptance, and reduced cost. Improved energy storage technologies will enable the stability, resiliency, and reliability of the future electric utility grid, as well as increased deployment of variable renewable energy resources.

We have been proactive in advancing technologies to modernize and make our grids smarter and more adaptive to the challenges posed by threats to the grid. For example, DOE-OE has made key investments in the area of synchrophasor technology, which reduces grid vulnerabilities by providing timely and accurate power outage information and better self-healing capabilities, and has also invested in microgrids, which keep local communities up and running during regional and other outages and help supply power to affected areas.

Many of these projects are working in local jurisdictions throughout the United States. Supporting the research, development, and deployment of next-generation technologies enhances the grid's ability to recover quickly from disruptions.

S. 3018

Thank you for the opportunity to provide technical assistance on S. 3018. It appears that the intent of S. 3018 is to strengthen the cybersecurity posture by allowing DOE National Laboratories to study the systems most critical to national security to the grid.. Yet, many energy sector entities already conduct such assessments to comply with mandatory Critical Infrastructure Protection (CIP) standards set by the North American Electric Reliability Corporation (NERC) 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.

There may still be a gap where the DOE National Laboratories could be of value to the Nation. Given that the National Laboratories are able to address complex system vulnerabilities, S. 3018 could provide an opportunity for the National Laboratories to not only identify complex system vulnerabilities, but do the research and development to mitigate these risks.

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 disaster and threat exercises.

Building an ecosystem of resilience is—by definition— a shared endeavor, and keeping a focus on local communities remains an imperative. Because DOE has spent decades building—and continues to build—local partnerships and investing in technologies to enhance resilience, the grid is better able to withstand and recover quickly from disasters and attacks.

---

[i] Led by ABB, with partners University of Illinois at Urbana Champaign and Bonneville Power Administration.
[ii] Led by Argonne National Laboratory, with partners Idaho National Laboratory, State University of New York-Buffalo, Illinois Institute of Technology, Commonwealth Edison, and PJM.