Testimony of Patricia A. Hoffman

Assistant Secretary for Office of Electricity Delivery and Energy Reliability

U.S. Department of Energy

Before the

Committee on Transportation and Infrastructure

Subcommittee on Economic Development, Public Buildings, and Emergency Management

U.S. House of Representatives

April 14, 2016

Chairman Barletta, Ranking Member Carson, and Members of the Subcommittee, thank you for focusing attention on the importance of a resilient electrical grid, and for the opportunity to discuss the Department of Energy's role in helping to ensure a resilient, reliable, and flexible electricity system in an increasingly challenging environment.

Our economy, national security and even the health and safety of 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 disruptions caused by natural and manmade events, such as severe weather, physical attacks, and cyber-attacks.

The electrical grid is more than just infrastructure. It is an ecosystem of asset owners, manufacturers, service providers, and government officials at Federal, state, and local levels, all working together to run one of the most reliable power grids in the world. Ninety percent of the nation's energy infrastructure is in private hands, and 3,306 electricity providers serve approximately 148 million people[1] through a network of 450,000 miles of high-voltage transmission lines.

There are plenty of risks beyond cyber, including physical, severe weather, natural disasters, aging infrastructure, and infrastructure interdependencies. My testimony today will focus on how, in the face of these diverse threats, we can help ensure that the grid is poised to recover quickly following an incident and how partnerships with public and private stakeholders play 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

[1] Energy Information Administration Forms EIA-861 and 861S, 2013. Does not include U.S. territories.

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, for instance our support of the research, development and deployment 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 cyber-security and other risks. Through these partnerships, we are providing tools, best practices, new technologies, and matching 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, which 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.

In early February, DOE Secretary Ernest Moniz signed an updated Energy Emergency Assurance Coordinators (EEAC) Agreement with the National Association of State Energy Officials (NASEO), National Association of Regulatory Utility Commissioners (NARUC), National Governors Association (NGA), and National Emergency Management Association (NEMA). This updated EEAC Agreement lays out concrete items to improve our collective ability to share information, which is essential for making sound response and restoration decisions during emergencies. To support this effort, DOE and state officials will develop information-sharing protocols and processes to streamline response operations. We will also test these processes and information-sharing mechanisms through routine drills and exercises.

The President's FY 2017 Budget includes a request for $15 million for a State Energy Assurance program to foster regional hazard preparedness. This program would focus on providing state, local, tribal, and territorial governments with analysis, training, and exercising of shared regional risk factors where entities depend on each other for energy supplies and must work together to resolve energy disruptions to restore energy infrastructure.

This new program would be facilitated through competitive regional cooperative assistance awards to state and local partners. As needed, DOE, including our National Laboratory expertise and capability, would be available to the awardees to enhance preparation and allow for real-world energy emergency support. Lessons learned will be shared with other communities to leverage the program across the nation and help improve resiliency planning.

DOE-OE also focuses on enabling our state, local, and utility partners with information. EAGLE-I (Environment for Analysis of Geo-Located Energy Information), for example, is a DOE-designed and operated web tool that automatically gathers electrical grid service status data from company websites every 15 minutes, and organizes it into an easy to read picture of electrical service status nationwide. Now covering 75 percent of all U.S. electricity customers, it provides real-time information about the grid – what is up, what is down, the number and location of outages, when service is restored – to DOE and, through our information-sharing efforts, with other Federal agencies.

Cyber-security 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 cyber-security 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 $180 million in cyber-security 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 is a capability to identify bad actors on networks and Hyperion is a capability to evaluate and expose malicious content and third-party software.

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

The Cyber-security Risk Information Sharing Program (CRISP) is a public-private partnership, co-funded by DOE-OE and industry. 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 50 percent of the total number of continental U.S. Electricity Subsector customers.

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

As part of the Administration's efforts to improve electricity subsector cyber-security capabilities, DOE-OE and industry partners developed the Electricity Subsector Cyber-security Capability Maturity Model (C2M2) to improve cyber-security capabilities and to help private sector owners and operators better assess cyber-security posture of the energy sector. The C2M2 provides an evaluation tool that helps organizations evaluate, prioritize and improve cyber-security capabilities.

Since the C2M2 program's inception in June 2012, more than 750 organizations have requested and received the C2M2 toolkit, including more than 400 electricity subsector organizations, and the number of participants is growing steadily. This is a comprehensive and credible approach that all energy sector companies can use to improve their cyber-security posture. DOE-OE also released versions of the C2M2 for the oil and natural gas sector and for industry at large.

Preparedness Exercises

DOE leads preparedness exercises at the local, state, and national levels. In November 2015, for example, DOE led the Federal participation in the North American Electric Reliability Corporation's Grid Ex III, the largest electricity sector crisis response exercise ever. More than 350 government and industry organizations, as well as 4,500 participants played a role in testing and shaping the national response plan.

In April, DOE will lead Clear Path IV in Portland, Oregon and Washington, DC. Clear Path IV is an interagency exercise focused on testing and evaluating energy sector roles and responsibilities within response plans utilized for a Cascadia Subduction Zone (CSZ) 9.0 earthquake and tsunami. Clear Path IV includes representation from 10 Federal agencies, seven states, five local governments, 15 oil and natural gas companies, 18 electric utilities, six trade associations, and four state associations with more than 175 participants.

Through this broad range of activities with our private and public partners, we are continuing to make good progress in creating a comprehensive ecosystem of resilience.

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, 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 White House, the Department of Homeland Security, the Department of Defense and other Offices within DOE.

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 energy sector. 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 the impacts of a disaster on the local and regional energy infrastructure;
- Coordinate the delivery of assets to repair that 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. They provide expertise on a variety of energy issues, and have direct access to subject matter experts back at our headquarters in Washington, DC. These experts 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, the Defense Production Act, and the recently-passed FAST Act (Fixing America's Surface Transportation Act, P.L. 114-94) to assist in response and recovery operations.

The national electricity infrastructure spans 19,000 power plants, 450,000 miles of transmission lines, 55,000 substations, and 6 million miles of distribution lines. The grid is truly a national system of complex systems, where small variations in power output or quality can be felt almost instantly several states away. That said, every piece of that infrastructure is local.

A fallen tree or 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, or a representative trade association member of the Electricity Subsector Coordinating Council (ESCC) member, 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. The ESCC is the strategic communication and coordination mechanism of industry and government for collective actions toward national critical infrastructure security and resilience.

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 and will continue its partnership with the energy sector to ensure the maximum effectiveness of this authority.

The FAST Act also codifies DOE's role as the lead SSA for energy sector cyber incident coordination. These actions provide a central point of action for the energy sector and can expedite recovery from cyber and physical incidents.

The FAST Act protections afforded to critical electric infrastructure information provide essential information-sharing tools to enhance the Federal Government's situational awareness while assuring the private sector that sensitive information on vulnerabilities will be safeguarded.

DOE looks forward to consulting in depth with FERC on the forthcoming critical electric infrastructure information rulemaking.

The FAST Act will enable a more robust response for energy incidents, and DOE is on track to implement the energy security provisions.

PARTNERSHIPS FOR INNOVATION

The myth that older infrastructure is more resilient because it is safe from cyber-attack is just that – a myth. In some cases the aging infrastructure of the grid itself can be a liability or risk. This infrastructure is less sophisticated, less stable, less tolerant to heat and cold, and less able to absorb voltage and frequency variations.

The keys to strengthening resilience are not only better threat insight and response, but also innovation and preparedness. 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 recent Quadrennial Energy Review (QER 1.0) and Quadrennial Technology Review (QTR).

One technology ripe for innovation is large power transformers. These important grid assets can weigh hundreds of tons, are expensive, and are typically custom made with procurement lead times of 1 year or more. Significant numbers of damaged transformers from any type of hazard, can result in a long-term impact on the overall resilience of the grid. The first installment of the QER 1.0 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.

The Transformer Resilience and Advanced Components (TRAC) program also includes a number of R&D activities to improve the resilience of transformers. Replacing aging grid assets with long-lived outdated technology will lead to infrastructure lock-in that increases the total cost of grid modernization. The average lead time between a large power transformer order and the date of delivery ranges from five to 12 months for domestic producers and six to 16 months for producers outside the United States. However, this lead time could extend beyond 20 months and up to five years in extreme cases if the manufacturer has difficulties obtaining any key inputs, such as bushings and other key raw materials. The President's FY 2017 budget request included $15 million for TRAC to develop cost-effective, next generation components that are inherently more resilient.

The FAST Act also addressed this issue and required DOE to submit a plan to Congress evaluating the feasibility of establishing a Strategic Transformer Reserve for the storage, in strategically-located facilities, of spare large power transformers in sufficient numbers to

temporarily replace critically damaged large power transformers. In January, DOE-OE awarded this analysis project to a team led by the Oak Ridge National Laboratory. The project team includes researchers from the University of Tennessee-Knoxville, Sandia National Laboratory, the Electric Power Research Institute, and Dominion Virginia Power.

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 would support 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 increase the deployment of variable renewable energy resources. All of these advances will strengthen resilience.

We have been proactive in advancing technologies to modernize and make our grids "smarter" and therefore more adaptive to the challenges that various threats pose 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 effected 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.

CONCLUDING STATEMENT

Threats will 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 sector's cyber-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, of which keeping a focus on local communities remains a top imperative. Because DOE has spent decades building—and continue to build— local partnerships and investing in technologies to enhance resilience, the grid is better able to withstand and recover quickly from a disaster or attack.