Testimony of Assistant Secretary Karen S. Evans

Office of Cybersecurity, Energy Security, and Emergency Response

U.S. Department of Energy

Before the

Committee on Energy & Natural Resources

United States Senate

February 14, 2019

Introduction

Chairman Murkowski, Ranking Member Manchin, and Members of the Committee, thank you for the opportunity to discuss the continuing threats facing our national energy infrastructure. Focusing on cybersecurity, energy security, and the resilience of the Nation's energy systems is one of Secretary Rick Perry's top priorities. By the Secretary proposing and Congress affirming the Office of Cybersecurity, Energy Security, and Emergency Response (CESER), the Secretary clearly demonstrated his commitment to achieving the Administration's goal of energy security and, more broadly, national security.

Our Nation's energy infrastructure has become a primary target for hostile cyber actors, both state-sponsored and non-state sponsored. The frequency, scale, and sophistication of cyber threats have increased. Cyber incidents have the potential to disrupt energy services, damage highly specialized equipment, and even threaten human health and safety.

The Director of National Intelligence, along with several heads of the Administration's Intelligence Community agencies, recently stated in written testimony that "China has the ability to launch cyberattacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks." Russia has similar abilities with the capability to disrupt "an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016."

The release of the President's National Cyber Strategy (NCS) in September reflects the Administration's commitment to protecting America from cyber threats. The Department of Energy (DOE) plays an active role in supporting the security of our Nation's critical energy infrastructure in implementing the NCS. 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 is of utmost importance as the Assistant Secretary of CESER.

CESER and its predecessor organization have demonstrated the Emergency Response function through multiple weather events, including hurricanes, activating our Emergency Response Organization. In 2018, CESER responded to a wide range of incidents, including

six hurricanes, three wildfires, two typhoons, a cyclone, an earthquake, and a volcanic eruption. Recently, we worked closely with Federal, industry, and State partners to monitor the impacts to the energy sector from the January 2019 "arctic blast" that affected the central and eastern portions of the Nation.

However, today, I would like to focus my testimony primarily on the cybersecurity function of the office and how CESER will meet the priorities of the Administration and work in conjunction with our Federal agency, State, local, tribal and territorial government (SLTT), industry, and National Laboratory partners.

DOE FAST Act Authority

DOE's role in energy sector cybersecurity is established in statute and executive action. In 2015, Congress passed the Fixing America's Surface Transportation (FAST) Act (P.L. 114-94), codifying DOE as the Sector-Specific Agency (SSA) for cybersecurity for the energy sector, consistent with existing policy. Defined in Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, "the term 'Sector- Specific Agency' (SSA) means the Federal department or agency designated under this directive to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment." PPD-21 states that the Department of Homeland Security (DHS) will "provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure." Specific to cybersecurity, DHS has authorities that support cybersecurity assistance by the federal government to all critical infrastructure sectors, including information sharing and technical assistance. The FAST Act further mandates that the Secretary of Energy coordinates "with the Department of Homeland Security and other relevant Federal departments and agencies" and collaborates with them on, among other things, "providing, supporting, or facilitating technical assistance and consultations for the energy sector to identify vulnerabilities and help mitigate incidents, as appropriate." With the formation of CESER, the Department's role as the SSA is strengthened and has undertaken the responsibilities with the highest degree of dedication and commitment.

The FAST Act also amended the Federal Power Act to give 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, events.

CESER

The Secretary has conveyed that he has no higher priority than to support the security of our Nation's critical energy infrastructure. CESER leads the Department's efforts to secure our Nation's energy infrastructure against all hazards, reduce the risks of and impacts from cyber events and other disruptive events, and assist with restoration activities. This office works closely with the private sector, as well as Federal and SLTT government partners, to enable more coordinated preparedness and response to cyber and physical threats and natural disasters. The office enhances the Department's ability to dedicate and focus attention on DOE's SSA

responsibilities and will provide greater visibility, accountability, and flexibility to better protect our Nation's energy infrastructure and support asset owners, as well as the overall critical infrastructure response framework overseen by DHS.

The CESER office plays an active role in coordinating government and industry efforts to address energy sector threats. The office is currently composed of two divisions: Infrastructure Security and Energy Restoration and Cybersecurity for Energy Delivery Systems.

DOE's Roles and Responsibilities for Energy Sector Cybersecurity

In preparation for, and in response to, cybersecurity incidents, 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 is described as one that is "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, DOE works in collaboration with other agencies and private sector organizations, including the Federal Government's designated lead agencies for coordinating the response to significant cyber incidents: the 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 its National Cyber Investigative Joint Task Force, as well as other agencies and private sector organizations. In the event of a significant cyber incident in the energy sector, DHS and DOJ coordinates with DOE to ensure its deep expertise with the sector is appropriately leveraged.

DOE is also working with the Tri-Sector Executive Working Group (TEWG) in conjunction with Department of Treasury and DHS along with our industry partners in order to address and manage risks across the energy, telecommunications, and financial sectors. The formation of the TEWG was recommended by the President's National Infrastructure Advisory Council (NIAC) in their August 2017 report titled, "Securing Cyber Assets: Addressing Urgent Cyber to Critical Infrastructure."

In the energy sector, the core of critical infrastructure partners are represented by 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 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 we are working together in a whole-of-government response.

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 Activities for the Energy Sector

DOE plays a critical role in supporting energy sector cybersecurity by enhancing the security and resilience of the Nation's critical energy infrastructure. To address these challenges, it is critical for us to be proactive and cultivate a secure energy network of producers, distributors, regulators, vendors, and public partners, acting together to strengthen our ability to prepare, respond, and recover.

The Department is focusing cyber support efforts to strengthen energy sector cybersecurity preparedness, coordinate cyber incident response and recovery, and accelerate game-changing research, development, and deployment (RD&D) of resilient energy delivery systems.

Strengthening Energy Cybersecurity Preparedness

It is necessary for partners in the energy sector and the government to share meaningful and timely emerging threat data and vulnerability information to help prevent, detect, identify, and thwart cyberattacks 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, as well as the broader U.S. intelligence community.

Current CRISP participants provide power to more than 75 percent of continental United States electricity customers. CRISP has clearly demonstrated 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.

The CRISP program is an example of how DOE, as the Sector-Specific Agency for energy, integrates additional efforts, including information from other public-private cybersecurity programs, such as DHS's Automated Indicator Sharing (AIS). The AIS program also allows for the bidirectional sharing of observed cyber threat indicators amongst DHS and participating companies. Those cyber treat indicators are incorporated into the CRISP analytics.

Advancing the ability to improve situational awareness of Operational Technology (OT) networks is a key focus of DOE's current activities. The Department is currently taking the lessons learned from CRISP and developing an analogous capability to monitor traffic on OT networks via the Cybersecurity for the Operational Technology Environment (CyOTE) pilot project. Observing anomalous traffic on networks can be the first step in stopping an attack in its early stages.

Cybersecurity vulnerabilities of key control systems and operational technology are an increasing concern for the Nation's critical energy infrastructure owners and operators. The Cyber Testing for Resilience of the Industrial Control Systems (CyTRICS) program will serve as a central capability for DOE's efforts to increase energy sector cybersecurity and reliability through testing and enumeration of critical electrical components. Further, analysis of test results will identify both systemic and supply chain risks and vulnerabilities to the sector by

correlating collected test data and enriching it with other data sources and methods. Through CyTRICS, DOE will collaborate with government, National Laboratories, and industry to identify key energy sector industrial control systems components and apply a targeted, prioritized, and collaborative approach to these efforts.

DOE is also establishing the Clean Energy Manufacturing Innovation Institute: Cybersecurity in Energy Efficient Manufacturing, led by the Office of Energy Efficiency and Renewable Energy in collaboration with CESER, to enhance the cybersecurity of energy-efficient manufacturing processes and accelerate the adoption of these technologies in the marketplace. The Institute will focus on cybersecurity in manufacturing, including understanding the evolving cybersecurity threats to greater energy efficiency in manufacturing industries, developing new cybersecurity technologies and methods, and sharing information and expertise with the broader community of U.S. manufacturers. The initiative will develop and leverage innovative solutions in two technical areas, securing automation and securing the supply chain, in order to address current and future challenges.

Facilitating Cyber Incident Response and Recovery

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.

Last year, DOE and the National Association of Regulatory Utility Commissioners (NARUC) released the third edition of a cybersecurity primer for regulatory utility commissioners. The updated primer provides best practices, access to industry and national standards, and clearly written reference materials for state commissions in their engagements with utilities to ensure their systems are secure from cyber threats. This document is publicly available on the NARUC website, benefitting not only regulators, but other State officials as well.

We are continuing to work with NARUC to support regional trainings on cybersecurity, with the goal of building commission expertise on cybersecurity, so they ensure cyber investments are both secure and economically viable.

DOE also continues to work closely with our public and private partners with the goal of fully supporting and bolstering the actions needed to help ensure the reliable delivery of energy. We continue to coordinate with industry through the Sector Coordinating Councils (SCCs) to synchronize government and industry cyber incident response playbooks.

CESER engages directly with our government and industry partners to help ensure we all are prepared and coordinated in the event of a cyber incident to the industry. The 2018 iteration of DOE's cybersecurity-focused exercise, Liberty Eclipse, included two phases. Phase I was a tabletop exercise focusing on the roles, responsibilities, and authorities, of Federal, State, and energy industry partners in response to a significant cyberattack on energy infrastructure. Phase II included a seven-day operations-based exercise conducted on Plum Island in New York.

During Phase II, DOE worked with the Defense Advanced Research Projects Agency (DARPA), who tested and evaluated technologies that could enable the blackstart recovery of the power grid during a cyberattack in an isolated and controlled environment with first responders and power engineers on hand.

In 2017, DOE participated in Clear Path V, an annual exercise led by the North American Electric Reliability Corporation (NERC) that was designed to simulate a cyber and physical attack on electric and other critical infrastructures across North America. Clear Path V, which took place in Houston, Texas, focused on the cross-sector response to a hurricane impacting the Gulf Coast, with particular attention to the interdependencies of the electricity, oil and natural gas, and communications sectors. This exercise was cited by participants from multiple sectors as crucial to preparing for a nearly-identical real-world event only a few months later Hurricane Harvey. This and other similar large scale exercises continue to highlight the interdependencies between our Nation's energy infrastructure and other sectors.

DOE's most recent exercise, Clear Path VI, took place near Washington, D.C., in May 2018. Clear Path VI built on the successful implementation of the regionally-focused Clear Path IV exercise, and addressed the desire to conduct more issue-focused exercises that explore coordination between industry, State, and Federal partners in managing interdependencies within and between infrastructure sectors. This iteration focused on the challenges that the sector may face during a major hurricane impacting the mid-Atlantic region.

Clear Path VII, scheduled for May 2019, will return to examining the impacts of a catastrophic earthquake, this time focusing on the New Madrid Seismic Zone. As a result of the lessons-learned identified from Clear Path IV, improvements have been implemented regarding the Department's response communications and coordination structures.

It is critical that the results of the exercises inform our response plans on a continuous basis to close identified gaps in coordination with our industry and government partners through the associated coordinating councils. Communication capabilities that are survivable, reliable, and accessible, by both industry and government, will be key to coordinating various efforts showcased in the exercise, including unity of messaging required to recover from a real-life version of the exercise scenario.

In preparation for any future grid security emergency, it is critical that we continue working with our government and industry partners to further shape the types of orders that may be executed under current authorities, while also clarifying how we communicate and coordinate the operational implementation of these orders. Continued coordination with Federal, SLTT, and industry partners and participation in preparedness activities like Liberty Eclipse enable DOE to identify gaps and develop capabilities to support cyber response.

Accelerating Breakthrough RD&D of Resilient Energy Delivery Systems

Cybersecurity for energy control and OT systems is vastly different from typical IT systems. OT 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 often be difficult.

CESER's Cybersecurity for Energy Delivery Systems (CEDS) R&D program is designed to assist energy sector asset owners by developing cybersecurity solutions for energy delivery systems through a focused, early-stage research and development effort. CESER co-funds industry-led, National Laboratory-led, and university-led projects with SLTT and 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. In a demonstration of our coordination with other federal agencies, two of the university-led collaborations are funded in partnership with DHS Science and Technology.

To select cybersecurity R&D projects, DOE constantly examines the 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 any commands would result in damage to the system or have 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.

The Energy Sector Security Appliances in a System for Intelligent Learning Network Configuration Management and Monitoring project, otherwise known as *Essence*, is a CEDS-funded endeavor involving the National Rural Electric Cooperative Association (NRECA). *Essence* started as a concept to build a system that passively monitors all network traffic within an electric utility, and to use machine learning to develop a model of what "normal" is, so that deviations indicative of cyber compromise could be detected instantly and acted on quickly. The envisioned system was built and successfully demonstrated in the first project. Work since then has focused on extending a solid technical prototype into commercially deployable products with solid, committed technical partners with an established presence in the utility market. To date, NRECA has engaged with four partners to offer commercial products based on *Essence*.

DOE is also working in conjunction with NRECA and the American Public Power Association (APPA) to help further enhance the culture of security within their utility members' organizations. With more than a quarter of the Nation's electricity customers served by municipal public power providers and rural electric cooperatives, it is critical that they have the tools and resources needed to address security challenges. To address risks and manage the risks to an acceptable level, APPA and NRECA are developing security tools, educational resources,

updated guidelines, and training on common strategies that can be used by their members to improve their cyber and physical security postures. Exercises, utility site assessments, and a comprehensive range of information sharing with their members will all be used to bolster their security capabilities.

Strengthening our Workforce Development

The final area I would like to highlight is one that is truly foundational in nature, cybersecurity workforce development. It is also a national priority outlined in the President's National Cyber Strategy. Through our SLTT workforce development efforts with state organizations like the National Association of State Energy Officials (NASEO), we are developing a multifaceted approach including online trainings, playbooks, workshops, and guidance to build capacity throughout the sector and guarantee that the State energy officials that we engage with regularly have the necessary and current skills and resources needed to prepare for and respond to energy disruptions of significance, including cyber emergencies.

DOE is also continuing and expanding our annual collegiate-level cyber defense competition. In 2018, DOE held two competitions to help develop the next generation of cybersecurity professionals to help secure our Nation's critical energy infrastructure. DOE's third Cyber Defense Competition (CDC) took place in April, with 25 college and university teams competing at three National Laboratories. DOE's 2018 CyberForce Competition™ followed in late November-December, with 64 college and university teams from 24 states and Puerto Rico competing at seven National Laboratories across the Nation.

Conclusion

Establishing CESER is the result of the Administration's commitment to and prioritization of energy security and national security. Our long-term approach strengthens our national security and positively impacts our economy. As CESER moves forward, we are taking the first steps in the transformational change necessary to achieve the Secretary's priority of emergency preparedness and rapid, coordinated response to disruptions in the energy sector.

I appreciate the opportunity to appear before this Committee to discuss cybersecurity in the energy sector, and I applaud your leadership. I look forward to working with you and your respective staffs to continue to address cyber and physical security challenges.