Testimony of Assistant Secretary Karen Evans

Office of Cybersecurity, Energy Security, and Emergency Response

U.S. Department of Energy

Before the

Committee on Energy and Commerce

United States House of Representatives

September 27, 2018

Introduction

Chairman Upton, Ranking Member Rush, 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 the Secretary's top priorities. By creating the Office of Cybersecurity, Energy Security, and Emergency Response (CESER), the Secretary clearly demonstrated his priorities and his commitment to achieving the Administration's goal to 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 private groups. 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. The recent release of the President's National Cyber Strategy (NCS) reflects the Administration's commitment to protecting America from cyber threats. The Department of Energy (DOE) plays a vital role in supporting the security of our Nation's critical energy infrastructure. 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 for me as the Assistant Secretary of CESER.

Recently, CESER demonstrated the Emergency Response function through multiple weather events—with the hurricanes activating our Emergency Response Plan while we also, working with federal and industry partners through the Oil and Natural Gas Subsector Coordinating Council, helped addressed the over pressurization of a Columbia Gas natural gas pipeline that caused multiple explosions and fires at residential locations in Massachusetts.

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 agencies, state, local and tribal governments, our industry partners and our national laboratories.

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), specifically naming DOE as the Sector-Specific Agency (SSA) for cybersecurity for the energy sector. As set forth in P.L. 114-94, Congress designated DOE as the SSA for cybersecurity for the energy sector. Defined in Presidential Policy Directive 21 (PPD-21), "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 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." 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 collaborating with, among other things, on "providing, supporting, or facilitating technical assistance and consultations for the energy sector to identify vulnerabilities and help mitigate incidents, as appropriate". By creating CESER, the Department's role as this SSA will be strengthened. The Department takes this responsibility seriously.

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 natural, physical and logistical events.

CESER

The creation of CESER elevates the Department's focus on energy infrastructure protection and will enable more coordinated preparedness and response to cyber and physical threats and natural disasters with the private sector, as well as federal, state and local government partners. This includes electricity transmission and delivery, oil and natural gas infrastructure, and all forms of generation. The Secretary has conveyed that he has no higher priority than to support the security of our Nation's critical energy infrastructure. The formation of the CESER 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 the Department of Homeland Security (DHS).

The CESER office plays an essential 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 (ISER) and Cybersecurity for Energy Delivery Systems (CEDS).

DOE's Roles and Responsibilities for Energy Sector Cybersecurity

In preparation for, and in response to, cybersecurity threats, 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 a cyber incident 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 the National Cyber Investigative Joint Task Force, respectively. In the event of a cybersecurity emergency in the energy sector, closely aligning DOE's activities with those of our partners at DHS and DOJ ensures DOE's deep expertise with the sector is appropriately leveraged.

DOE is also working with the recently established 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 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 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 that 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 to enhance 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 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.

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 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 US intelligence community.

The purpose of CRISP is to share information among electricity subsector partners, DOE, DHS, DOJ, 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 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.

DOE's 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.

Advancing the ability to improve situational awareness of OT networks is a key focus of DOE's current activities. The Department is currently in the early stages of 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 – and having the ability to store and retrieve network traffic from the recent past – 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. DOE will collaborate with government, National Laboratories, and industry to identify key energy sector industrial control systems components and apply a targeted, collaborative approach to these efforts.

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's Office of Electricity (OE) 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 resilient to cyber threats. This document is publicly available on the NARUC Research Lab website, benefitting not only regulators, but state officials as well.

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.

DOE also continues to work closely with our public and private partners so 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 industry through the SCCs to synchronize government and industry cyber incident response playbooks.

CESER engages directly with our federal, state, local, tribal, and territorial (SLTT) government partners, as well as 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. DOE and the National Association of State Energy Officials (NASEO) 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 the NCCIC and FEMA, and private sector utilities and petroleum companies.

And late last year DOE participated in GridEx IV, a biennial 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. This and other similar

large scale exercises continue to highlight the interdependencies between our Nation's energy infrastructure and other sectors.

While the after-action report has yet to be released, during GridEx IV it was clear that collaboration between industry and the federal government has strengthened greatly since Superstorm Sandy and GridEx III. The executed coordination in response to this year's hurricane season also is evidence of this strengthening. 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 industry, Federal, and SLTT 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 GridEx enables DOE to identify gaps and develop capabilities to support cyber response as the SSA.

Accelerating breakthrough RD&D of resilient energy delivery systems

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.

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 today's 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.

Conclusion

Establishing CESER is the result of the Administration's prioritization of electric grid security and national security. Our long-term vision will positively impact our national security and economy. As CESER addresses all areas of responsibilities, we are taking the first steps in the transformational change necessary to meet the priority of the Secretary of ensuring the security of our Nation's critical energy infrastructure.

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.