Written Testimony of Under Secretary Mark Menezes

U.S. Department of Energy

Before the

Subcommittee on Energy

Committee on Energy and Commerce

U.S. House of Representatives

March 14, 2018

Introduction

Chairman Upton, Ranking Member Rush, and distinguished Members of the Subcommittee, thank you for the opportunity to participate in this legislative hearing to discuss strategic priorities for addressing the cybersecurity threats facing our national energy infrastructure and the Department of Energy's (DOE's) role in protecting these critical assets. Maintaining and improving a resilient energy infrastructure is a top priority of the Secretary and a major focus of the Department; hence, our focus on cybersecurity is paramount.

Our national security and economy depend on the availability of a reliable and resilient energy infrastructure. The mission of the Office of Electricity Delivery and Energy Reliability (DOE-OE) is to strengthen, transform, and improve the resilience of energy infrastructure to ensure access to reliable and secure sources of energy. The Secretary and DOE are committed to working with our public and private sector partners to protect the Nation's critical energy infrastructure from physical security events, natural and man-made disasters, and cybersecurity threats.

Office of Cybersecurity, Energy Security, and Emergency Response

To demonstrate our focus on the aforementioned mission, the Secretary announced last month that he is establishing an Office of Cybersecurity, Energy Security, and Emergency Response (CESER). This organizational change will strengthen the Department's role as the Sector-Specific Agency (SSA) for Energy Sector Cybersecurity, supporting our national security responsibilities.

The CESER office will play an essential role in coordinating government and industry efforts to address these energy sector threats. Initially, the office will be comprised of work we currently do in DOE-OE's Infrastructure Security and Energy Restoration (ISER) division and Cybersecurity and Emerging Threats Research and Development (CET R&D) division.

The President has requested slightly more than $95 million in FY 2019 for CESER with a focus on early-stage activities that improve cybersecurity and resilience to harden and evolve critical energy infrastructure. These activities include early-stage R&D at National Laboratories to develop the next generation of control systems, components, and devices with cybersecurity built in. This includes a greater ability to share time-critical data with industry to detect, prevent, and recover from cyber events.

The creation of the CESER office will build on all that we do today and elevate the Department's focus on energy infrastructure protection and will enable more coordinated preparedness and response to cyber and physical threats and natural disasters. This must include electricity delivery, oil and natural gas infrastructure, and all forms of generation. The Secretary's desire to create dedicated and focused attention on these responsibilities will provide greater visibility, accountability, and flexibility to better protect our Nation's energy infrastructure and support asset owners.

DOE's Roles and Responsibilities for Energy Sector Cybersecurity

In preparation for, and 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: Department of Homeland Security (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's role in energy sector cybersecurity was codified by Congress through the Fixing America's Surface Transportation (FAST) Act. That legislation designated DOE as the Sector-Specific Agency for Energy Sector Cybersecurity. In extreme cases, the Department can use its legal authorities such as those in the Federal Power Act, as amended by the FAST Act, to assist in response and recovery operations. Congress enacted several important new energy security measures in the FAST Act as it relates to cybersecurity. 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 the reliability of 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. The Grid Security Emergency authority is unique to DOE and an important element in partnering with DHS and DOJ to fully address the cybersecurity risks to the energy sector.

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 co-chaired with 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.

As defined in the National Infrastructure Protection Plan, the industry coordinating councils or "SCCs" are created by owners and operators and are self-organized, self-run, and self-governed, with leadership designated by the SCC membership. The SCCs serve as the principal collaboration points between the government and private sector owners and operators for critical infrastructure security and resilience coordination and planning, as well as a range of sector-specific activities and issues.

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.

Legislative Technical Assistance

Although the Administration does not have a position on any of the legislation under discussion today, I would like to provide the Subcommittee with some high level priorities for the Department in context of the FY 2019 budget request and some specific comments on each of the cyber bills. Overall, investing in energy security and resilience from an all hazards approach is vital, given the natural and man-made threats facing the Nation's energy infrastructure, the energy industry, and supply chain. The FY 2019 request would provide the Department an opportunity to invest in early stage research, network threat detection, cyber incident response teams, and testing of supply chain components and systems.

Amending the Department of Energy Organization Act

The DOE Organization Act, enacted in 1977, emphasizes energy supply shortages as a threat to national security and does not explicitly address threats posed by malicious actors targeting the Nation's critical energy infrastructure. DOE currently has broad authority to act in the event of a Grid Security emergency. Continuing to conduct preparedness and response activities will help DOE fulfill its responsibilities and expectations of our role as the lead SSA for the Energy Sector.

Cybersecurity and Physical Threats to the Electric Grid

The cyber attacks on the Ukrainian grid underscored the urgency of the cyber threat to everyone involved in the protection and operation of the Nation's power grid. Continuing to build off current work is critical in mitigating the risks that the electric grid faces. Sharing and promoting best practices, including maturity model assessments, physical and cyber risk assessments, and training are all important components of this risk mitigation.

Presidential Policy Directive-21 (PPD-21) clearly defines resilience as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

The energy industry's challenge in addressing resilience is defining cost-effectiveness as it builds in cybersecurity and invests in mitigation solutions that provide a strong return on investment. The Interruption Cost Estimate (ICE) Calculator tool, which was developed by Lawrence Berkeley National Laboratory and Nexant, Inc. and funded by DOE-OE, is designed for electric reliability planners at utilities, government organizations, or other entities that are interested in estimating interruption costs and/or the benefits associated with reliability improvements in the United States. For any hazard, including cyber events, the ICE Calculator provides analytical foundations for reliability investments. In 2015, the Department updated the 2009 meta-analysis that provides estimates of the value of service reliability for U.S. electricity customers. The meta-dataset now includes 34 different datasets from surveys fielded by 10 different utility companies between 1989 and 2012.[1]

The Department, in partnership with the ESCC, has identified several priorities moving forward, including resilient communications systems (which are heavily interdependent with energy systems), control system monitoring, proactive cyber threat detection and threat analysis, and supply chain assessments and mitigation to supply chain threats. Additionally, DOE is prioritizing providing preparedness and response support to the energy sector through the facilitation of requests for technical assistance. DOE serves as the a central hub for the energy sector and, in coordination with the Department of Homeland Security (DHS) and other interagency partners as described above, is able to help integrate DOE and DHS response teams with industry response and planning activities. The Department has been asked to provide financial and technical assistance to state, local, tribal, and territorial governments to revise and implement energy security and resilience plans as well.

Cyber Sense

Securing the electric sector supply chain is critical to the security and resilience of the electric grid. Products must be tested for known vulnerabilities in order to assess risk and develop mitigations. Universities, third parties and the National Laboratories have all conducted vulnerability testing.

[1] https://eaei.lbl.gov/tool/interruption-cost-estimate-calculator;
https://eaei.lbl.gov/publications/updated-value-service-reliability

Ultimately, success in any product development program includes a strong quality control process through which a business seeks to ensure that product quality is maintained or improved and manufacturing errors are reduced or eliminated, even as products are updated. Quality control requires the business to create an environment in which both management and employees strive for perfection. This process is applicable to the integration of cybersecurity in the energy sector's supply chain design and manufacturing process. It is also important to note that in terms of supply, this bill references components and devices in the electric system.

In FY 2019, the Department is proposing a supply chain testing program to test and mitigate vulnerabilities in partnership with industry. Liability protections for any action or asserted failure to act by the United States, participating energy sector entity, or National Laboratory during such activities would enable the Department to develop integrated testing capabilities to understand supply chain, component, and network vulnerabilities and inform the design of resilient products.

Cybersecurity for Pipelines and Liquefied Natural Gas Facilities

As part of the Transportation Sector, DHS and the Department of Transportation (DOT) are the co-lead sector-specific agencies for pipeline cybersecurity. As the sector-specific agency for the energy sector, DOE works closely with relevant government agencies and oil and natural gas subsector partners on security and resilience, including cybersecurity through the ONG SCC and EGCC. DOE works with the DHS National Protection and Programs Directorate, the Transportation Security Administration, the U.S. Coast Guard, the DOT Transportation Pipeline and Hazardous Materials Safety Administration, and the Federal Energy Regulatory Commission regarding pipeline security and safety initiatives as they relate to resilience and reliability. Similar to the electric sector, physical and cybersecurity of crude and petroleum pipelines and liquefied natural gas facilities are critical.

<u>DOE's Cybersecurity Strategy for the Energy Sector</u>

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.

As part of a comprehensive energy cybersecurity resilience strategy, the Department is focusing cyber support efforts to enhance visibility and situational awareness of operational networks; increase alignment of cyber preparedness and planning across local, state, and Federal levels; and leverage the expertise of DOE's National Labs to drive cybersecurity innovation.

Enhance Visibility and Situational Awareness of Operational Networks

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 cyber attacks 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.

The purpose of CRISP is to share information among electricity subsector partners, DOE, 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 network 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 over 75 percent of continental United States electricity customers. If CRISP has demonstrated one finding to DOE, it is 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 for threat detection 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.

Increase Alignment of Cyber Preparedness and Planning Across Local, State, and Federal Levels

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-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.

DOE-OE engages directly with our public and 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 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.

Communication capabilities that are survivable, reliable, and accessible, by both industry and government, will be key to coordinate 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 state partners now to further shape the types of orders that may be executed under the Secretary’s authority, while also clarifying how we communicate and coordinate the operational implementation of these orders.

Continued coordination with Federal 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.

Leverage the Expertise of DOE's National Laboratories to Drive Cybersecurity Innovation

Beyond providing guidance and technical support to the energy sector, DOE-OE also supports a R&D portfolio designed to develop advanced tools and techniques to provide enhanced cyber protection for key energy systems. Intentional, malicious cyber threat challenges to our energy systems are on the rise in both number and sophistication. This evolution has profound impacts on the energy sector.

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.

DOE-OE'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 research and development effort. DOE-OE co-funds industry-led, National Laboratory-led, and university-led 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.

DOE is also working in conjunction with the National Rural Electric Cooperative Association (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 they have the tools and resources needed to address security challenges. 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

Cyber threats continue to evolve and DOE is working diligently to eliminate and mitigate the potential consequences of these threats. Establishing the CESER office is a result of our laser focused attention to cyber and physical security. Our long-term vision is significant and will positively impact our national security. The establishment of this office will be the first step in the transformational change necessary to meet the ever changing cyber landscape highlighted by our National Intelligence Agencies.

Finally, I would like to highlight that the risk of physical and cyber threats is continuously being exacerbated by a set of circumstances that are increasing the interdependence of the various energy systems throughout the Nation. This significantly increases our overall risk due to the increased number of penetration points that can significantly impact national security and the economy.

As always, I appreciate the opportunity to appear before this Subcommittee 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.