COMMITTEE ON ENERGY AND COMMERCE
Questions for the Record Responses from Under Secretary for Energy Mark Menezes
DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response."
March 14, 2014

QUESTIONS FROM CHAIRMAN UPTON

Q1. During your appearance before us in January, you mentioned that expectations for DOE's emergency response exceeded its authorities.

Q1a. From your experience to date, are there some additional tools or authorities for DOE that would help improve the ability of the agency's deployment of resources in an emergency?

A1a. The U.S. energy security and emergency response posture has changed since the formation of the Department. New energy security threats have emerged and it is necessary to ensure that we have updated authorities to reflect our new reality. A key area that could enhance DOE capabilities to support security and resilience within the energy sector includes a Federal energy infrastructure prioritization and risk management framework through state and local governments, territories, and tribes to utilize during a multi-state catastrophic incident and to enable strategic investment and programs with energy assurance plans.

Q1b. Was DOE fully prepared to respond effectively to FEMA task orders during the response to the three hurricanes this past year? What can be done to enhance that response?

A1b. Regarding the hurricanes in the contiguous United States, the answer is yes. DOE worked with industry and Federal, state, and local partners to facilitate response and recovery activities. As part of the whole-of-government response to these disasters, DOE deployed response personnel to support state emergency operations centers, FEMA Incident Management Assistance Teams, and regional and national response coordination centers, including several weeks of 24-hour coverage at FEMA's National Response Coordination Center in Washington, DC. DOE responders worked with interagency partners as well as with state government and industry representatives to identify information and resource gaps and inform DOE's engagements to support the restoration efforts.

Regarding Puerto Rico, Hurricane Maria presented an unprecedented challenge to the existing response and funding structures and, as such, departments and agencies are assessing continued improvements to adequately prepare for and recover from disasters. After the storm, DOE coordinated and executed recovery efforts with FEMA, the U.S.

Army Corps of Engineers (USACE), and other agencies to restore power. As with the other hurricanes on the mainland, DOE worked with industry, state, territorial and local partners and deployed its own personnel.

As part of the Department's After-Action Review process, DOE is working to better utilize its capabilities and expertise, to include how these capabilities support each phase from pre-incident preparedness, response, damage assessment, and restoration to long-term recovery.

In addition, DOE, FEMA, USACE, and other partners are establishing a standing Interagency Power Task Force that will serve as a standing coordinating element and, during incidents, transition to a crisis planning component of Emergency Support Function #12.

Q2. DOE works with the Department of Homeland Security, TSA and others to ensure protection of pipelines, but these agencies have other priorities as well. Given its responsibilities in the energy sector broadly, Mr. Menezes, should DOE help make sure there is comprehensive and effective coordination over pipeline security?

A2. Under Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, the Department of Homeland Security (DHS) coordinates the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure, including the integration and coordination of Federal cross-sector security and resilience activities. DOE is designated as the sector-specific agency (SSA) for the energy sector. DHS and the Department of Transportation are the Co-SSAs for the transportation sector, which includes pipelines. DOE supports the established model that places responsibility on DHS to lead comprehensive and effective cross-sector coordination related to the safety and security of the Nation's pipelines. DOE works closely with DHS and other interagency partners to support the private sector in its protection efforts. As the SSA for the energy sector, DOE also co-chairs the Oil and Natural Gas Sector Coordinating Council (ONG SCC) and the Energy Sector Government Coordinating Council (EGCC), which provide a forum for information sharing between all responsible public and private officials. The ONG SCC also includes a Standing Pipeline Working Group.

Q3. The department's role in energy supply emergencies involves working with state emergency offices. Last year, the House passed legislation, HR 3,050, to enhance DOE's support of state energy assurance planning, including cybersecurity support.

Q3a. I understand you are proposing to elevate and consolidate emergency response functions in a new office-an Office of Cybersecurity, Energy Security, and Emergency Response (CESER). Will the functions in this new office include state energy assurance planning?

A3a. Establishing CESER will enable the Department to strengthen its role as the sector-specific agency for the energy sector under PPD 21, support national security responsibilities, and better address natural disasters and emerging threats. By combining Departmental elements that support response and recovery, DOE will enhance the efficiency and effectiveness of the preparedness cycle for the energy sector for all hazards. Forming one office to support energy stakeholder engagement through planning for and responding to incidents while developing supporting capabilities, training, exercising, and evaluating lessons learned will more directly inform research and development efforts in resilience based on lessons learned from operational activities. Additionally, the important subject matter expertise collected supports the critical role energy plays in national security, and the office will work with all energy sector stakeholders, including states for state energy assurance planning.

Q3b. What are your priorities for continuing to assist state level emergency planning?

A3b. DOE supports local and state resilience planning and emergency preparedness. The Department recognizes that the response to energy sector incidents begins at the state, local, tribal, and territorial (SLTT) levels. As such, DOE routinely engages with state and local emergency management offices and energy assurance officials on a myriad of resilience and energy security initiatives that support their resilience planning efforts.

In February 2016, DOE signed an updated Agreement for Enhanced Federal and State Energy Emergency Coordination, Communications, and Information Sharing with the

National Association of State Energy Officials (NASEO), the National Association of Regulatory Utility Commissioners (NARUC), the National Governors Association (NGA), and the National Emergency Management Association (NEMA). The updated agreement lays the groundwork for information sharing amongst SLTT governments around the country to promote energy resilience and accelerated response. As part of this agreement, DOE and state associations provide training and seminars for Energy Assurance Coordinators, and DOE and the states have developed information sharing protocols and processes to streamline response operations, which are tested through drills and exercises.

DOE also hosted the Liberty Eclipse Energy Assurance Exercise in December 2016 in Newport, RI, with nearly 100 exercise participants from 11 states, private industry, the Department of Homeland Security, the Federal Emergency Management Agency, the Department of Defense, and other interagency partners. During the exercise, participants confronted a fictitious cyber incident that cascaded into the physical sector and discussed the challenges of restoring electrical and fuel systems. The exercise resulted in greater awareness of challenges for cyber incident coordination with states and the need for updating state energy assurance plans. DOE plans to do additional exercises like Liberty Eclipse moving forward.

In 2017, OE worked with NASEO to provide technical assistance to twelve states to update their state energy assurance plans. Later this year DOE will be able to test our plans and information sharing at this year's Clear Path exercise, to be held either in or near Washington, DC, in May. Clear Path VI will build on the successful implementation of the second regionally-focused Clear Path exercise, which occurred during May 2017 and 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. Clear Path VI will also address 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.

Q4. You mention in your testimony that, among the activities that are a priority, will be “early stage activities that improve cybersecurity and resilience to harden and evolve critical energy infrastructure.”

Q4a. Would you elaborate some examples of research to create next generation systems, components and devices with “cybersecurity built in”?

A4a. DOE’s Cybersecurity for Energy Delivery Systems (CEDS) program works to redesign system architectures to enable energy delivery systems (EDS) to adapt and survive a cyber-attack, while decreasing the cyber-attack surface. CEDS research partnerships are advancing tools and technologies that make EDS resilient against malicious manipulation, integrate cybersecurity as part of the design of power system components, and develop red-teaming techniques specifically tailored to EDS cybersecurity technologies. Here are a few examples of CEDS-supported research partnerships:

- The Los Alamos “Quantum Security Modules for the Power Grid” project leverages the groundbreaking capabilities of quantum communications to generate and manage the encryption keys that guarantee data integrity. This research uses quantum physics principles to reveal in real-time an adversarial attempt to intercept the key exchange. Unlike traditional cryptography solutions, quantum keys pair the benefits of higher security with lower computational complexity.

- Schweitzer Engineering Laboratories Inc. partnered with Sandia National Laboratories and Tennessee Valley Authority to develop the Padlock Project security gateway, which detects tampering with field devices, such as those attached to utility poles, and guards against unexpected cyber-activity. The Padlock Project also integrates the results from the exe-Guard project, which provides for deny-by-default cybersecurity.

- Likewise, CEDS supported a research partnership led by ABB called “Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF),” which enables power grid protective devices to automatically identify and reject any malicious command that would jeopardize grid stability. CODEF runs a quick physics-based simulation to evaluate how a command would affect grid operations, and then ignores all faulty commands, thereby protecting the system against malware, spoofing, and insider attacks. The prototype was demonstrated in transmission-level operations at the Bonneville Power Administration, and the team is now beginning the process to integrate it into the ABB product lines.

Q4b. What are some of the technologies that will improve the ability to share time-critical data with industry?

A4b. To address the need for timely sharing of threat information as well as the rapid recognition of cyber-attacks against critical energy infrastructure and development of mitigations and to reduce the risk of consequences, DOE supports the Cybersecurity Risk Information Sharing Program (CRISP) and Cybersecurity for the Operational Technology Environment (CYOTE) pilot projects to help improve capabilities. The Energy Sector currently doesn’t have a comprehensive capability to share time-critical data with industry; CRISP (focused on information technology [IT]) and CYOTE (focused on operational technology [OT]) are working to address this gap. CRISP and CYOTE are advancing data sharing and analysis capabilities within the energy sector’s IT environments, as well as in the complex OT environments where threat monitoring and detection is less widespread.

Q4c. To what extent will the new Office of Cybersecurity, Energy Security, and Emergency Response manage this research?

A4c. Protecting America’s energy systems from cyber-attacks and other risks is a top national priority for the Department. The establishment of the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) prioritizes robust cybersecurity programs across the energy sector, with a focus on early-stage activities that improve cybersecurity and resilience to harden and evolve critical grid infrastructure.

CESER programs will continue the Office of Electricity Delivery and Energy Reliability's activities to enhance the resilience (the ability to withstand and quickly recover from disruptions and maintain critical function) and security (the ability to protect system assets and critical functions from unauthorized and undesirable actors) of the U.S. energy infrastructure.

Q5. You reference the budget proposals for the Department to invest in cyber incident response teams.

Q5a. What do you mean when you say "cyber incident response teams?"

A5a. The Department is seeking to continue developing our expertise to establish operational technology cyber incident response teams for our Power Marketing Administrations. These teams could augment the Federal leads for cyber incident response at DHS and FBI by providing subject matter expertise when appropriate and requested.

Q5b. How does this fit with Department of Homeland Security incident response teams?

A5b. Under PPD-41: United States Cyber Incident Coordination, DHS, acting through the National Cybersecurity and Communications Integration Center, is the lead agency for asset response. The SSAs will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure. Under this policy, agencies would coordinate to provide unity of effort. DOE cyber incident response teams are an internal resource for Federally owned energy infrastructure and could contribute specialized knowledge, skills, and abilities to account for the unique combination of energy systems and cybersecurity.

Q5c. What role does coordination play to enhance situational awareness so that efforts can be prioritized?

A5c. Coordination is the foundation of all emergency response efforts and also extends to situational awareness as the data about what is occurring comes from a wide set of stakeholders. This coordination highlights issues occurring and the combination of those events leads to prioritization of addressing the issues.

Q6. You make reference to CRJSP-the cybersecurity risk information sharing program—would you explain what this does and how much of the industry it covers?

A6. CRISP analyzes near-real-time IT data from utilities using U.S. intelligence to detect cyber-attacks and threats, and delivers alerts and mitigations back to owners and operators. Participating utilities voluntarily share their IT system traffic, which undergoes classified and unclassified analysis to identify threat patterns and attack indicators across the energy industry. Current CRISP participants provide electricity to about 75 percent of the Nation's electric customers.

Q6a. Are there examples where the program has helped address emerging cyber threats?

A6a. Intelligence analysis of CRISP data alerted operators to threat indicators and identified sophisticated intrusions of electric utilities. CRISP reports supported responses to key attacks in 2017 including WannaCry, CrashOverride/Industroyer, and Petya.

Q6b. What is necessary to expand coverage of the program to cover the full electric sector?

A6b. The FY 2019 Budget Request for Cybersecurity for Energy Delivery Systems (CEDS) supports starting development of a significantly improved information sharing model. The effort will capitalize on the existing CRISP experience and concepts, using the latest available technology, architecture, and innovative partnerships with the energy sector to provide the enhanced cyber protection for the energy sector. The resulting next-generation CRISP will address both IT and OT infrastructure as compared to the existing CRISP, which is IT-centric, and CYOTE, which is OT-centric. The vision is to dramatically increase the footprint across the energy sector infrastructure and to gain a higher level of threat detection capability.

Q6c. Does CRISP apply to the oil and gas sector? If so, what is the coverage?

A6c. The CRISP concept, technology and approach is applicable to the oil and gas sector as a voluntary program, but current CRISP members are primarily from the electric sector. Some of these CRISP members do have gas operations and dialogue is underway to enroll oil and natural gas entities as CRISP participants.

Q7. Would you also explain in more detail the Cybersecurity for the Operational Technology Environment (CYOTE) pilot project?

A7. The CYOTE pilot will enable OT data sharing and analysis capability with four pilot utilities for the complex OT environment. This complements the existing CRISP program, which focuses on the security of IT networks. As part of this pilot, DOE is examining how we can work with the electricity sector to leverage U.S. intelligence capabilities to prevent, detect, or delay a cyber-attack on utility OT networks that could disrupt power. A primary objective of this pilot will be to assess whether U.S. intelligence analysis can provide actionable information to utilities to take preventive or corrective measures to reduce OT cyber risks.

Q7a. What would the sectors be where this is and can be deployed?

A7a. CYOTE would be deployed across the Nation's energy sector, including their critical energy infrastructure. The energy sector includes the electricity and oil and natural gas subsectors.

Q8. You mention in your testimony that liability protections for the department, labs, and participating energy sector entities would enable the Department to develop its testing capabilities to understand cybersecurity vulnerabilities. Please elaborate why lack of liability protections might impede your ability to perform this mission?

A8. Effective public-private partnerships are vital to the resilience and security of the energy sector. This collaboration will enable the entities involved to research and test key components of the energy sector, locate vulnerabilities, and recommend mitigations. Currently, this collaboration exists due to trust built through longstanding relationships between DOE, the national laboratories, and energy sector entities.

COMMITTEE ON ENERGY AND COMMERCE
Questions for the Record Responses from Under Secretary for Energy Mark Menezes
DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response."
March 14, 2014

QUESTIONS FROM REPRESENTATIVE GRIFFITH

We have a new pipeline that is already being built in my district and a lot of my constituents are concerned about all kinds of issues.

Q1. Are new pipelines with more technology more vulnerable than the older ones already in the ground?

A1. The cybersecurity of the Nation's pipeline infrastructure is of critical importance. The Department of Homeland Security's (DHS's) National Cybersecurity and Communications Integration Center (NCCIC) provides cybersecurity assistance across all critical infrastructure sectors, including pipelines. DHS's Transportation Security Administration (TSA) Pipeline Security Program is designed to enhance the security preparedness of the Nation's hazardous liquid and natural gas pipeline systems and provides recommended cybersecurity guidelines for pipeline operators. The Department of Transportation's (DOT's) Pipeline and Hazardous Materials Safety Administration (PHMSA) regulates pipeline safety pursuant to 49 C.F.R. §§ 100–199, which includes automated and manual safety requirements for regulated pipelines.

For newer pipelines, operational technologies such as supervisory control and data acquisition (SCADA) and Process Control Systems provide robust communication and computing power to operate physical components such as pumps and compressors along the pipelines. The pipeline systems can be vulnerable to cyber threats if security best practices are not followed or properly deployed. Pipeline security guidelines developed by TSA, the Interstate Natural Gas Association of America, and the American Petroleum Institute are being used by pipeline operators to protect both legacy pipelines and those with newer operation control and monitoring technologies.

Q1a. I would also ask that you look at what we can do as far as making sure that the new pipelines have technology in them that let us know if there's an earthquake in the area or a collapse somewhere. The faster people know about it, the faster we can respond.

A1a. Pipeline operators continuously monitor the status of their pipeline networks. SCADA systems provide real-time information and alert operators to any unexpected changes to the status of the system, including information that can indicate a ground shift. In seismically active areas and areas subject to ground shift, many operators install ground monitors to provide additional real-time data. PHMSA regulates pipeline safety pursuant to 49 C.F.R. §§ 100–199, which includes automated and manual safety requirements for regulated pipelines.

Q2. I think we also need to look, and would like your help, in figuring out if we need to draft legislation to get DOE on the frontend, because I'm not sure FERC is looking into how to make this pipeline less vulnerable.

A2. DOE has established a public-private collaboration with government partners and the pipeline industry to secure the transport of oil and natural gas. DOE, through the Office of Electricity Delivery and Energy Reliability (OE), works with the DHS National Protection and Programs Directorate (NPPD), TSA, U.S. Coast Guard, and Infrastructure Security Compliance Division, as well as the DOT PHMSA and the Federal Energy Regulatory Commission (FERC) to streamline pipeline security and safety initiatives as they relate to resilience and reliability.

Under Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, DHS coordinates the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure, including the integration and coordination of Federal cross-sector security and resilience activities. DOE is designated as the sector-specific agency (SSA) for the energy sector. DHS and DOT are the co-SSAs for the transportation sector, which includes pipelines. DOE supports the established model that places responsibility on DHS to lead comprehensive and effective cross-sector coordination related to the safety and security of the Nation's pipelines. DOE works closely with DHS and other interagency partners to support the private sector in its protection efforts. As the SSA for the energy sector, DOE also co-chairs the Oil and Natural Gas Sector Coordinating Council (ONG SCC) and the Energy Sector Government Coordinating Council (EGCC), which provide a forum for information sharing between all responsible public and private officials. The ONG SCC also includes a Standing Pipeline Working Group.

Q2a. Should we move it away from the more occupied area to one that is less likely to be attacked by bad actors or to create a problem, should there be an issue?

A2a. DOE is not part of the regulatory or permitting process to determine the routes of new pipeline systems. The construction of new interstate natural gas pipelines is regulated by FERC. New pipelines may also be subject to regulatory and permitting requirements from the Department of Transportation, Environmental Protection Agency, Department of Interior, and Department of State, as well as state and local requirements.

Q3. Likewise, it would also seem to me that DOE would want to know who had extra capacity in a new pipeline. With the right kind of technology, it could tell instantly whether or not they had the ability to take on more natural gas at a particular moment should there be a failure in some other area, so that we can get that natural gas to where it needs to go by rerouting it possibly. While we're laying this pipe is the time to put in new innovations and thoughts and I'm hoping DOE has some thoughts.

A3. Pipeline owners and operators are generally aware of any unused capacity on their pipelines as well as where additional product may be needed. As the sector specific agency for the energy sector, DOE works with private and public sector partners to ensure that relevant information about regional fuel supplies is shared so that the private sector can make informed decisions.

COMMITTEE ON ENERGY AND COMMERCE
Questions for the Record Responses from Under Secretary for Energy Mark Menezes
DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response."
March 14, 2014

QUESTIONS FROM REPRESENTATIVE LOEBSACK

Q1. We have a lot of existing pipelines now that may not be as subject to a cybersecurity threat. Can you distinguish those that are already in the ground versus the newer ones which might be more vulnerable, given the technology?

A1. The cybersecurity of the Nation's pipeline infrastructure is of critical importance. The Department of Homeland Security's (DHS's) National Cybersecurity and Communications Integration Center (NCCIC) provides cybersecurity assistance across all critical infrastructure sectors, including pipelines. DHS's Transportation Security Administration (TSA) Pipeline Security Program is designed to enhance the security preparedness of the Nation's hazardous liquid and natural gas pipeline systems and provides recommended cybersecurity guidelines for pipeline operators. The Department of Transportation's (DOT's) Pipeline and Hazardous Materials Safety Administration (PHMSA) regulates pipeline safety pursuant to 49 C.F.R. §§ 100–199, which includes automated and manual safety requirements for regulated pipelines.

For newer pipelines, operational technologies such as supervisory control and data acquisition (SCADA) and Process Control Systems provide robust communication and computing power to operate physical components such as pumps and compressors along the pipelines. The pipeline systems are vulnerable to cyber threats if security best practices are not followed or properly deployed. Pipeline security guidelines developed by TSA in collaboration with private sector partners including the American Gas Association (AGA), the Interstate Natural Gas Association of America (INGAA), and the American Petroleum Institute (API) are being used by pipeline operators to protect both legacy pipelines and those with newer operation control and monitoring technologies.