U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

March 12, 2018

TO: Members, Subcommittee on Energy

FROM: Committee Majority Staff

RE: Hearing entitled "DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response"

I. INTRODUCTION

The Subcommittee on Energy will hold a hearing on Wednesday, March 14, 2018, at 10:00 a.m. in 2123 Rayburn House Office Building. The hearing is entitled, "DOE Modernization: Legislation Addressing Cybersecurity and Emergency Response."

II. WITNESSES

PANEL I

- **Mark Menezes**, Under Secretary of Energy, U.S. Department of Energy, *accompanied by* **Patricia Hoffman**, Principal Deputy Assistant Secretary, Office of Electricity Delivery & Energy Reliability.

PANEL II

- **Scott Aaronson**, Vice President, Security and Preparedness, Edison Electric Institute;
- **Mark Engels**, Senior Enterprise Security Advisor, Dominion Energy;
- **Tristan Vance**, Director, Office of Energy Development, State of Indiana;
- **Zachary Tudor**, Associate Laboratory Director for National and Homeland Security, Idaho National Laboratory; and,
- **Kyle Pitsor**, Vice President of Government Relations, National Electrical Manufacturers Association.

III. BACKGROUND

A. DOE Energy Security and Emergency Response Authorities

When the Department of Energy (DOE) was organized in 1977, energy security concerns revolved around oil supply shortages. As a result, energy security emergency functions in the Department of Energy Organization Act focused on distributing and allocating fuels in an

emergency.[1] Over time, while DOE's organic statute remained largely unchanged, its responsibilities and authorities have evolved substantially beyond what was envisioned forty years ago. Energy delivery systems have become increasingly interconnected and digitized, while society has become more dependent on energy in all its forms—expanding the opportunities for cybersecurity threats and other hazards that may require emergency response.[2]

Today, DOE's mission to advance the national, economic, and energy security of the United States requires it to act as the lead agency for the protection of electric power, oil, and natural gas infrastructure. DOE has authority and responsibilities for the physical and cybersecurity of energy delivery systems from laws that Congress has passed and Presidential directives. Congress has provided DOE with a wide range of emergency response and cybersecurity authorities affecting multiple segments of the energy sector, beginning with the Department of Energy Organization Act, and most recently with the Fixing America's Transportation Act (FAST Act).[3] The FAST Act, which was signed into law in 2015, designated DOE as the Sector-Specific Agency (SSA) for the energy sector and provided the Department with several new energy security authorities to respond to physical and cyberattacks to energy systems.

DOE's cybersecurity roles and responsibilities are also guided by the Federal Government's operational framework, as provided by the Presidential Policy Directive 41 (PPD-41) issued in 2016 addressing "United States Cyber Incident Coordination." A primary purpose of PPD-41 is to improve coordination across the Federal Government by clarifying roles and responsibilities. Under the PPD-41 framework, DOE serves as the lead agency for the energy sector, coordinating closely with other agencies and the private sector to facilitate the response, recovery, and restoration of damaged energy infrastructure.[4]

B. Physical Security and Cybersecurity for Pipeline and LNG Facilities

As the Energy SSA, DOE is required to coordinate with multiple Federal and State agencies and collaborate with energy infrastructure owners and operators on activities associated with identifying vulnerabilities and mitigating incidents that may impact the energy sector. To perform these duties effectively, DOE must account for each interrelated segment of the nation's energy infrastructure, including pipelines, which are subject to an array of other Federal authorities. In a January 24, 2018 letter, the Committee wrote to Secretary Perry to better understand the level of coordination among governmental agencies.[5]

Along with DOE, the Transportation Security Administration (TSA) has responsibility related to security for pipelines. According to the Congressional Research Service (CRS), the Aviation and Transportation Security Act of 2001, which established the Transportation Security

---

[1] P.L. 95-91
[2] For a discussion of the DOE's statute and the changing energy security landscape, see "Report to Congress: Valuation of Energy Security for the United States," Department of Energy, January 2017, pages 2-3.
[3] P.L. 114-94
[4] *See* Annex for Presidential Policy Directive – United States Cyber Incident Coordination. Released July 26, 2016.
[5] *See* Letter from Chairman Greg Walden to Secretary Rick Perry dated January 24, 2018, available at: https://energycommerce.house.gov/wp-content/uploads/2018/01/20180124DOE.pdf

Administration within the Department of Transportation, authorized the agency "to issue, rescind, and revise such regulations as are necessary" to carry out its functions.[6] TSA was transferred to the Department of Homeland Security, created under the Homeland Security Act of 2002.[7] The Implementing Recommendations of the 9/11 Commission Act of 2007 directs TSA to promulgate pipeline security regulations and carry out necessary inspection and enforcement if the agency determines that regulations are appropriate.[8]

Although TSA has regulatory authority for pipeline security, its activities to date have relied upon voluntary industry compliance with the agency's security guidance and best practice recommendations. A 2017 report by CRS highlighted several recent attacks on domestic pipeline systems and identified issues for Congress to consider, including a 2016 report by the DHS Inspector General concluding that "TSA lacks an intelligence driven, risk-based security strategy that informs security and resource decision across all transportation modes."[9,10] The CRS report also revealed that TSA only has six dedicated full-time equivalent staff administering its pipeline security work.

C. Physical Security and Cybersecurity for the Electric Grid

With respect to its responsibilities for security of the electric power system, DOE works closely with electric sector owners and operators to detect and mitigate risks to critical electric infrastructure. DOE collaborates with the electric sector to develop technologies, tools, exercises, and other resources to assist the energy sector in evaluating and improving their security preparedness.[11]

Along with DOE, the Federal Energy Regulatory Commission (FERC) has authority over the reliability of the electric grid. Congress, through the Energy Policy Act of 2005,[12] provided FERC with the authority to approve mandatory cybersecurity standards proposed by the Electric Reliability Organization (ERO). The North American Electric Reliability Corporation (NERC) currently serves as the ERO. NERC proposes reliability standards for planning and operating the North American bulk power system. These critical infrastructure protection (CIP) reliability standards[13] address physical security and cybersecurity of critical electric infrastructure.

Cooperation between the Federal government and electricity sector extends beyond mandatory and enforceable standards. The Electricity Subsector Coordinating Council (ESCC)[14] serves as the principal liaison between the Federal government and the electric power sector in coordinating efforts to prepare for national-level incidents or threats to critical infrastructure. The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership, funded

---

[6] P.L. 107-71
[7] P.L. 107-296
[8] P.L. 110-53
[9] Congressional Research Service. Pipeline Security: Recent Attack. April 11, 2017.
[10] Department of Homeland Security. Office of Inspector General. Transportation Security Administration Needs a Crosscutting Risk-Based Security Strategy. September 9, 2016.
[11] Department of Energy. Energy Sector Cybersecurity Preparedness.
[12] P.L. 109-58
[13] *See* North American Electric Reliability Corporation for further information.
[14] *See* Electric Subsector Coordinating Council for further information.

by DOE and industry. CRISP is managed by the Electricity Information Sharing and Analysis Center (E-ISAC)[15] and facilitates the timely bi-directional sharing of unclassified and classified threat information with energy sector partners.[16]

IV. SUMMARY OF LEGISLATION

A. H.R. 5174, Energy Emergency Leadership Act

H.R. 5174 amends the Department of Energy Organization Act to include energy emergency and energy security among the functions that the Secretary shall assign to an Assistant Secretary; provides that these functions include responsibilities with respect to infrastructure, cybersecurity, emerging threats, supply and emergency planning, coordination, response, and restoration; and provides that these functions also include the provision of technical assistance, support, and response capabilities with respect to energy security threats, risks, and incidents to State, local, and tribal governments and the energy sector.

B. H.R. 5175, Pipeline and LNG Facility Cybersecurity Preparedness Act

H.R. 5175 requires the Secretary of Energy to carry out a program to coordinate Federal agencies, States, and the energy sector to ensure the security, resiliency, and survivability of natural gas pipelines, hazardous liquid pipelines, and liquefied natural gas facilities. The bill also requires the Secretary to coordinate response and recovery to physical and cyber incidents impacting the energy sector, develop advanced cybersecurity applications and technologies, perform pilot demonstration projects, develop workforce development curricula relating to physical and cybersecurity, and provide mechanisms to help the energy sector evaluate, prioritize, and improve physical and cybersecurity capabilities.

C. H.R. 5239, Cyber Sense Act

H.R 5239 directs the Secretary of Energy to establish a voluntary DOE program that identifies and promotes cyber-secure products intended for use in the bulk-power system. The Secretary of Energy would be required to establish a testing process to identify products and technologies, including industrial control systems intended for use in the bulk-power system. In addition, the Secretary would be required to establish cybersecurity vulnerability reporting processes and maintain a related database. The Secretary also would be required to provide technical assistance to electric utilities, product manufacturers, and other electricity sector stakeholders to mitigate identified cybersecurity vulnerabilities.

H.R. 5239 instructs the Secretary to develop guidance for electric utilities for products tested and identified as cybersecure under the Cyber Sense program and to provide reasonable notice and solicit comments from the public, prior to establishing or revising the Cyber Sense testing process. Any cybersecurity vulnerability reported pursuant to this program, the disclosure of which the Secretary of Energy reasonably foresees would cause harm to critical

[15] *See* Electricity Information Sharing and Analysis Center for further information.
[16] Department of Energy. Cybersecurity for Critical Energy Infrastructure.

electric infrastructure, shall be deemed "critical electric infrastructure information" as defined by section 215A(d) of the Federal Power Act.

D. H.R. 5240, Enhancing Grid Security through Public-Private Partnerships Act

H.R. 5240 requires the Secretary of Energy to establish a program to facilitate and encourage public-private partnerships to promote and advance physical and cybersecurity of electric utilities. The Secretary of Energy is directed to carry out a program to (1) develop, and provide for voluntary implementation of, maturity models, self-assessments, and auditing methods for assessing the physical security and cybersecurity of electric utilities; (2) provide training and technical assistance to electric utilities to address and mitigate cybersecurity supply chain management risks; and (3) increase opportunities for sharing best practices and data collection within the electric sector.

The Secretary is also required to take into consideration different sizes of electric utilities and the regions they serve and to prioritize electric utilities with fewer available resources due to size or region. Any information an electric utility provides to the Federal government through this program will be exempt from public disclosure under Federal, State, or tribal law.

The bill also provides for a report to Congress addressing cybersecurity as it relates to the electric distribution system directs the Secretary to assesses priorities, policies, procedures, and actions for enhancing the physical and cybersecurity of electric distribution system, including the costs and benefits of implementing these priorities, policies, procedures, and actions.

Finally, H.R. 5240 directs the Department of Energy to update the Interruption Cost Estimate Calculator, a tool designed for and utilized by electric reliability planners at electric utilities, government organizations or other entities that are interested in estimating interruption costs and benefits associated with infrastructure improvements.

V. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Peter Spencer, Annelise Rickert, Brandon Mooney, or Mary Martin of the Majority Committee staff at (202) 225-2927.