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

September 25, 2018

TO: Members, Subcommittee on Energy

FROM: Committee Majority Staff

RE: Hearing entitled "DOE Modernization: The Office of Cybersecurity, Energy Security, and Emergency Response."

I. INTRODUCTION

The Subcommittee on Energy will hold a hearing on Thursday, September 27, 2018, at 10:15 a.m. in 2322 Rayburn House Office Building. The hearing is entitled, "DOE Modernization: The Office of Cybersecurity, Energy Security, and Emergency Response."

II. WITNESSES

- **Karen Evans**, Assistant Secretary for Cybersecurity, Energy Security, and Emergency Response, Department of Energy.

III. BACKGROUND

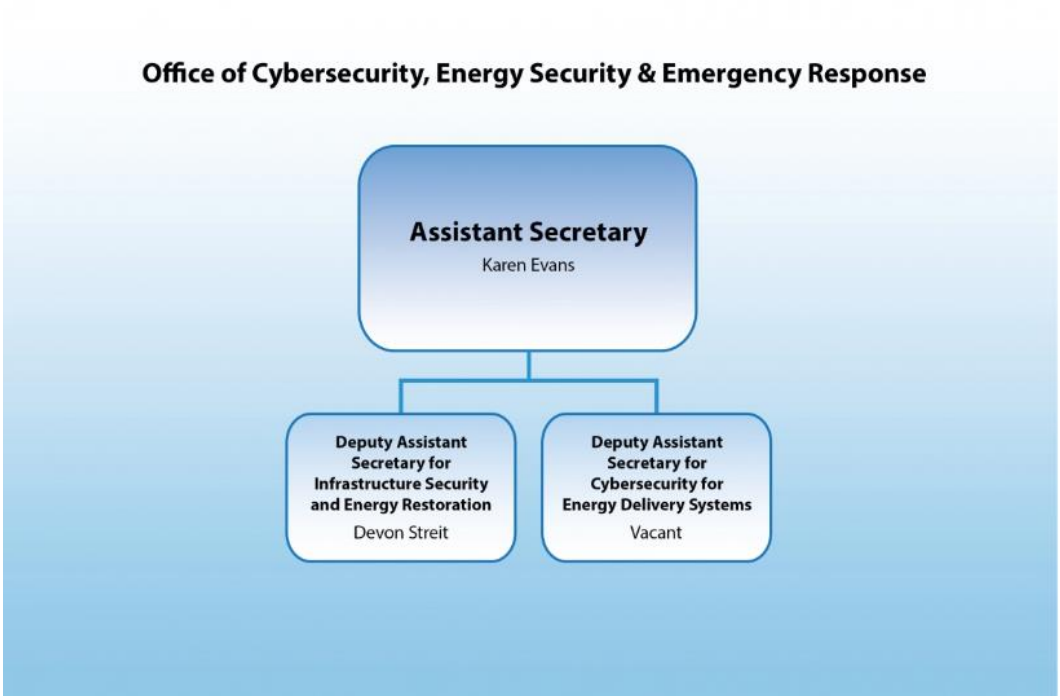
When the Department of Energy was organized in 1977, energy security concerns revolved around oil supply shortages. As a result, energy security emergency functions in the Department of Energy Organization Act focused on distributing and allocating fuels in an emergency. Over time, while DOE's organic statute remained largely unchanged, its responsibilities and authorities have evolved substantially beyond what was envisioned 40 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.

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, including in the Department of Energy Organization Act, the Energy Policy Conservation Act, the Natural Gas Act, the Federal Power Act, the Defense Production Act, and most recently the Fixing America's Surface Transportation Act (FAST Act).

Office of Cybersecurity, Energy Security, and Emergency Response

On February 14, 2018, the Energy Secretary established a new Office of Cybersecurity, Energy Security, and Emergency Response (CESER) at DOE.[1] The CESER office is led by an Assistant Secretary who is responsible for DOE's emergency preparedness and coordinated response to disruptions to the energy sector, including physical and cyber-attacks, natural disasters, and man-made events. On August 28, 2018, Karen Evans was confirmed as Assistant Secretary for CESER by the U.S. Senate.

The CESER office has two divisions each led by a Deputy Assistant Secretary. The Infrastructure Security and Energy Restoration Division leads efforts to secure the U.S. energy infrastructure against all hazards, reduce the impact of disruptive events, and respond to and facilitate recovery from energy disruptions, in collaboration with industry and State and local governments. The Cybersecurity for Energy Delivery Systems Division mitigates the risk of energy disruption from cyber incidents and other emerging threats within the energy environment. For FY2019, DOE requested $96 million to fund the CESER office. The conference report of FY2019 included an appropriated amount of $120 million.



[1] *See* Press Release, U.S. Department of Energy, "Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response." (Feb. 14, 2018),https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency

Sector-Specific Agency for Energy

Pursuant to the FAST Act and Presidential Policy Directive 21 (PPD-21), DOE is the Sector Specific Agency (or SSA) for the energy sector. 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.[2] In response, Secretary Perry noted that "a coordinated government approach to the cyber and physical security of pipelines, led by the Department of Energy, is essential to ensuring the safe and reliable flow of energy across the U.S."[3]

DOE's cybersecurity roles and responsibilities are also guided by the FAST Act and 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.

Physical Security and Cybersecurity of Energy Infrastructure

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.[4]

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,[5] 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[6] address physical security and cybersecurity of critical electric infrastructure.

---

[2] *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
[3] *See* Letter from Secretary Rick Perry to Chairman Greg Walden dated March 13, 2018, available at: https://docs.house.gov/meetings/IF/IF03/20180314/107999/HHRG-115-IF03-20180314-SD053.pdf
[4] Department of Energy. Energy Sector Cybersecurity Preparedness.
[5] P.L. 109-58
[6] *See* North American Electric Reliability Corporation for further information.

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 Administration within the Department of Transportation, authorized the agency "to issue, rescind, and revise such regulations as are necessary" to carry out its functions.[7] TSA was transferred to the Department of Homeland Security, created under the Homeland Security Act of 2002.[8] 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.[9]

Public/Private Partnerships and Information Sharing

CESER works closely with energy sector owners and operators to better detect risks and mitigate them more rapidly by fostering industry assessment capabilities, developing operational threat analysis tools, and working with the intelligence community to better share actionable threat and intelligence information.

The Electricity Subsector Coordinating Council (ESCC)[10] 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 by DOE and industry. CRISP is managed by the Electricity Information Sharing and Analysis Center (E-ISAC)[11] and facilitates the timely bi-directional sharing of unclassified and classified threat information with energy sector partners.[12]

Energy Sector Emergency Response and Restoration

The Infrastructure Security and Energy Restoration (ISER) office, within CESER, leads DOE's emergency preparedness and coordinated response to disruptions to the energy sector. ISER plans, trains, and coordinates year-round with all relevant stakeholders so that it can meet our nation's energy needs by deploying energy emergency responders to coordinate and facilitate system restoration activities with local, state, territorial, Federal, public and private sector stakeholders, in some cases, coordinating the utilization of certain legal authorities and waivers on behalf of the energy sector.

ISER provides situational awareness of affected energy infrastructure and systems to the White House and the rest of the Federal government during an event, in coordination with state, local and industry stakeholders. For the current hurricane season and for hurricanes Maria, Irma,

---

[7] P.L. 107-71
[8] P.L. 107-296
[9] P.L. 110-53
[10] *See* Electric Subsector Coordinating Council for further information.
[11] *See* Electricity Information Sharing and Analysis Center for further information.
[12] Department of Energy. Cybersecurity for Critical Energy Infrastructure.

Nate, and Harvey in fall 2017, DOE provided situational reports with details on the storms' impacts, and the energy industry's recovery and restoration activities.

IV. ISSUES

The following issues may be examined at the hearing:

- What will the CESER office's role be in the execution of DOE's responsibilities as a Sector Specific Agency for energy related emergencies?
- How will the CESER office work with other agencies within the larger federal emergency and cybersecurity response framework?
- What are lessons learned from recent natural disasters that can inform DOE's preparedness and response work in energy emergencies?
- What is necessary to assure critical energy infrastructure protection, from all hazards, and to respond effectively to energy supply disruptions following an event?

V. STAFF CONTACTS

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