COMMITTEE ON
ENERGY & COMMERCE
CHAIRMAN FRANK PALLONE, JR.

MEMORANDUM

July 9, 2019

To: Subcommittee on Energy Members and Staff

Fr: Committee on Energy and Commerce Staff

Re: Hearing on "Keeping The Lights On: Addressing Cyber Threats To The Grid"

On **Friday, July 12, 2019, at 9:30 a.m. in the John D. Dingell Room, 2123 of the Rayburn House Office Building**, the Subcommittee on Energy will hold a hearing entitled, "Keeping The Lights On: Addressing Cyber Threats To The Grid."

I. BACKGROUND

A. Department of Energy – Office of Cybersecurity, Energy Security, and Emergency Response

Last year, the Department of Energy (DOE) announced the establishment of a new office of Cybersecurity, Energy Security, and Emergency Response (CESER) as part of its fiscal year (FY) 2019 budget request. DOE tasked the Office of Cybersecurity with protecting the Nation's energy infrastructure "from cyber threats, physical attack and natural disaster."[1] The Senate confirmed Karen S. Evans as the Assistant Secretary for CESER on August 28, 2018.[2] The FY 2020 budget request includes $157 million for the CESER office, which is a $37 million increase from the FY 2019 enacted level.[3]

The CESER office administers two major programs: the Cybersecurity for Energy Delivery Systems (CEDS) and the Infrastructure Security and Energy Restoration (ISER) programs. CEDS's mission is to mitigate the risk of energy disruptions caused by cyber events through both near- and long-term initiatives. CEDS focuses on accelerating the speed and effectiveness of cyber risk and vulnerability sharing by partnering with industry to create a

---

[1] Department of Energy, FY2019 Congressional Budget Request – Volume 3 Part 1 (Mar. 2018) (www.energy.gov/sites/prod/files/2018/03/f49/DOE-FY2019-Budget-Volume-3-Part-1_0.pdf).

[2] Department of Energy, *CESER Leadership (https://www.energy.gov/ceser/ceser-leadership)* (accessed Apr. 29, 2019).

[3] Congressional Research Service, *FY2020 Budget Request for the Department of Energy* (Mar. 22, 2019) (IN11082).

nationwide cyber supply chain capability analysis, and by expediting research and development advances.[4] The ISER program coordinates a nationwide initiative to safeguard energy infrastructure from disruptions by supporting a regional voluntary delivery model. ISER aims to increase outreach to state, local, tribal, and territorial partners to make sure their energy assurance plans include integrated information sharing initiatives and align with activities undertaken by the energy industry sector.[5]

B. Cybersecurity Provisions of Public Law 114-94, Fixing America's Surface Transportation (FAST) Act

On December 4, 2015, President Obama signed the Fixing America's Surface Transportation (FAST) Act into law, which included the Upton-Pallone amendment that provides DOE with new authority to address cybersecurity threats. The law designates DOE as the sector-specific agency to carry out all cybersecurity responsibilities for the energy sector. It further requires the Secretary of Energy to coordinate with the Department of Homeland Security and other related agencies to report directives, conduct incident management and provide technical assistance to critical energy infrastructure owners and operators. Under the law, DOE is also the lead agency responsible for coordinating with state and local governments, tribes, and U.S. territories. The law also facilitates the protection and voluntary sharing of critical electric infrastructure information between private sector asset owners and the Federal government. Additionally, it exempts designated "Critical Electric Infrastructure Information" from certain Federal and State disclosure laws for a period up to five years and requires the Federal Energy Regulatory Commission (FERC) to facilitate voluntary information sharing between Federal, State, local and tribal authorities, the Electric Reliability Organization (ERO), regional entities, and owners, operators and users of the bulk-power system in the United States. [6]

C. Cybersecurity Authority of the Federal Energy Regulatory Commission

The Energy Policy Act of 2005 granted FERC the authority to approve mandatory cybersecurity standards proposed by the entity designated to serve as the ERO.[7] The North American Electric Reliability Corporation (NERC) serves as the ERO, and it is capable of proposing reliability standards for the protection of critical infrastructure.[8] In addition, FERC

[4] *See* note 1.

[5] *Id*.

[6] Fixing America's Surface Transportation Act, Pub. L. No. 114-94.

[7] Energy Policy Act of 2005, Pub. L. 109-58.

[8] Congressional Research Service, *The Federal Power Act (FPA) and Electricity Markets* (Mar. 10, 2017) (R44783).

has established the Office of Energy Infrastructure Security (OEIS) to address physical and cyber threats.[9]

II. WITNESSES

The following witnesses have been invited to testify:

The Honorable Karen S. Evans
Assistant Secretary
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
U.S. Department of Energy

J. Andrew (Andy) Dodge, Sr.
Director
Office of Electric Reliability
Federal Energy Regulatory Commission

Mr. Jim Robb
President and Chief Executive Officer
North American Electric Reliability Corporation

[9] Federal Energy Regulatory Commission, *Office of Energy Infrastructure Security (OEIS)* (https://www.ferc.gov/about/offices/oeis.asp) (accessed Jul. 3, 2019).