GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

MEMORANDUM

January 30, 2017

To: Subcommittee on Energy Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

Re: Hearing on "The Electricity Sector's Efforts to Respond to Cybersecurity Threats"

On **Wednesday, February 1, 2017, at 10:15 a.m. in room 2322 of the Rayburn House Office Building**, the Subcommitee on Energy will hold a hearing entitled, "The Electricity Sector's Efforts to Respond to Cybersecurity Threats."

I. BACKGROUND

The U.S. electric grid consists of interconnected transmission lines, local distribution systems, generation facilities, and related communications systems. The grid's increasing reliance on automation and two-way communications increases its vulnerability to cyber-attacks and remote strikes. Operations controls over the transmission grid and generators are increasingly managed by computer systems linked to the Internet or other communications systems and to each other. These trends, in addition to the rise of advanced metering and other smart grid capabilities, amplify reliability, cybersecurity and other security-related concerns.

So far, the U.S. power grid has not suffered any major successful attacks, but network security professionals warn that such attacks are not unheard of.[1] This past December, 225,000 people in Kiev lost power as a result of suspected Russian hacking. Some cybersecurity experts believe that this kind of attack is achieveable against the U.S. grid. Although the U.S. grid is different and better protected against cyberattacks, it is presumed our systems could take longer

[1] *Why a power grid attack is a nightmare scenario,* The Hill (Dec. 30, 2016) (online at http://thehill.com/policy/cybersecurity/281494-why-a-power-grid-attack-is-a-nightmare-scenario).

to recover from an attack.[2]

II. QUADRENNIAL ENERGY REVIEW

On January 19, 2014, President Obama issued a Presidential Memorandum directing the federal government to conduct a Quadrennial Energy Review (QER) and establishing a task force to conduct that review and "submit a Quadrennial Energy Review Report to the President every 4 years…."[3]

Recently, the Department of Energy (DOE) released the second installment of the QER titled "Transforming the Nation's Electricity System." Included in this second installment is a review of evolving cyber threats to the grid. In its report, DOE issued the following findings on electricity grid cybersecurity:

> The current cybersecurity landscape is characterized by rapidly evolving threats and vulnerabilities, juxtaposed against the slower-moving deployment of defense measures. Mitigation and response to cyber threats are hampered by inadequate information-sharing processes between government and industry, the lack of security-specific technological and workforce resources, and challenges associated with multi-jurisdictional threats and consequences. System planning must evolve to meet the need for rapid response to system disturbances.[4]

Reports of cybersecurity incursions in the U.S. and Canadian energy sector have decreased from 111 reported incidents in 2013 to 46 in 2015. While none of these incidents have succeeded in inhibiting or disrupting power system operations, risks may change as distributed energy, smart grid technologies and other advanced technologies become more widespread.[5]

III. THE FAST ACT - GRID SECURITY EMERGENCY AUTHORITY

On December 4, 2015, President Obama signed into law the Fixing America's Surface Transportation (FAST) Act which, among other things, contained a bipartisan provision sponsored by Rep. Upton creating a new section 215A of the Federal Power Act to provide the Secretary of Energy with authority to address grid security emergencies. Under the law, if the

---

[2] *Everything We Know About Ukraine's Power Plant Hack,* Wired (Jan. 20, 2017) (online at https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/).

[3] The White House, *Presidential Memorandum – Establishing a Quadrennial Energy Review* (Jan. 19, 2014) (online at www.whitehouse.gov/the-press-office/2014/01/09/presidential-memorandum-establishing-quadrennial-energy-review).

[4] U.S. Department of Energy, *Quadrennial Energy Review, Transforming the Nation's Electricity System,* at 4-2 (Jan. 2017).

[5] *Id.* at 4-35.

President provides a written directive or determination identifying a grid security emergency, the Secretary is authorized to take emergency measures to protect the bulk power system or defense critical electric infrastructure, with such measures to expire no later than 15 days from the directive's issuance. The law also facilitates the protection and voluntary sharing of critical electric infrastructure information between private sector asset owners and the Federal government. The FAST Act 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 to facilitate voluntary information sharing between Federal, State, local and tribal authorities, the Electric Reliability Organization, regional entities, and owners, operators and users of the bulk-power system in the U.S.

IV. WITNESSES

The following witnesses have been invited to testify:

Mr. Scott Aaronson
Executive Director, Security and Business Continuity
Edison Electric Institute

Dr. Chris Beck
Chief Scientist and Vice President for Policy
The Electric Infrastructure Security Council

Mr. Gerry Cauley
President and CEO
North American Electric Reliability Corporation

Ms. Barbara Sugg
Vice President and Chief Security Officer
Southwest Power Pool