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

January 30, 2017

TO: Members, Subcommittee on Energy

FROM: Committee Majority Staff

RE: Hearing entitled "The Electricity Sector's Efforts to Respond to Cybersecurity Threats"

I. INTRODUCTION

On Wednesday, February 1, 2017, at 10:15 a.m. in 2322 Rayburn House Office Building, the Subcommittee on Energy will hold a hearing entitled "The Electricity Sector's Efforts to Respond to Cybersecurity Threats." The hearing will examine the various practices that have been deployed across the electric power sector to confront cybersecurity risks and examine what is necessary to ensure the reliability and resilience of the nation's electricity transmission systems in light of these risks.

II. WITNESSES

- **Gerry W. Cauley**, President and CEO, North American Electric Reliability Corporation (NERC);
- **Scott L. Aaronson**, Executive Director, Security and Business Continuity, Edison Electric Institute (EEI), on behalf of the Electricity Subsector Coordinating Council;
- **Barbara Sugg**, Vice President for IT and Chief Security Officer, Southwest Power Pool (SPP), on behalf of ISO/RTO Council (IRC), and;
- **Chris Beck,** Chief Scientist and Vice President for Policy, The Electric Infrastructure Security Council (EIS Council).

III. BACKGROUND

Energy reliability and security is of the utmost importance to U.S. national security, national economic interests, and basic health and welfare. Electricity in particular is an essential part of modern life,[1] the disruption of which would impact not only households, but virtually every sector of the economy, including the critical infrastructure related to transportation, drinking water, communications and information, finance, and oil and gas production.

[1] In 2000, the National Academy of Engineering cited electrification, and the vast networks of electricity that power the developed world, as the greatest achievement affecting quality of life in the 20th Century.

The U.S. electricity system connects electricity producers and consumers by transmission and distribution lines and related transmission facilities. This system is part of the North American electric system, which is composed of four separate power grids or interconnections: the Eastern Interconnection (generally for states east of the Rocky Mountains and including Canada from Saskatchewan to the Maritime provinces), the Western Interconnection (from the Pacific Ocean to the Rocky Mountain states and the Canadian provinces of Alberta and British Columbia), the Texas Interconnected System (ERCOT), and the Québec Interconnection.

As the Federal Energy Regulatory Commission (FERC) explains, each interconnection is essentially one large machine and comprises three main functions: generation, transmission, and distribution.[2] Electric generation (supply) creates electricity using various generating technologies with specific operating characteristics. The transmission system connects and transfers large amounts of power from generators to the distribution system, delivering electricity to population centers. The distribution system then routes electricity to individual customers (referred to as load). Together, these systems are connected and operate in an electric balance, where load and supply are matched. Keeping this balance and maintaining reliability is a very complex enterprise involving skilled operators, sophisticated computers and design, rigorous maintenance, and a network of defensive strategies—involving real-time monitoring and control, short and long term planning, coordination, communications, and security of critical assets—based on the assumption that equipment can and will fail unexpectedly.

All told, the bulk-power system in the United States and Canada has more than 200,000 miles of transmission lines, is valued at over $1 trillion, and is capable of annually delivering over 3,800 terawatt hours of electricity to more than 334 million people.[3]

Recent cyber-related events have raised concerns about the security and resiliency of the nation's electricity system. For example, in December 2015, cyberattacks on the Ukrainian Power Grid represented the first publically acknowledged cyber incidents to result in power outages, bringing increased attention to the potential risks posed to the U.S. electricity system by cyber threats.[4] These concerns are increased by the recognition that as technology advances and integrates into the electricity system, new threats and vulnerabilities can arise, creating significant and new challenges for thousands of system operators to confront.

Congress, government agencies, and the private sector have taken significant steps to address current and future cyber risks. These steps include establishing mandatory nationwide reliability standards, promoting public-private partnerships, and providing new authorities to address grid security emergencies.

---

[2] For additional background see the Federal Energy Regulatory Commission's "Reliability Primer" beginning at page 9, from which this description is adapted, at www.ferc.gov/legal/staff-reports/2016/reliability-primer.pdf

[3] North American Energy Reliability Corporation at www.nerc.com/news/documents/understanding%20the%20grid%20dec12.pdf

[4] The Ukraine incidents affected 225,000 customers and lasted for several hours in three service territories, which was considered comparatively low impact in terms of overall power system impacts, according to *Analysis of the Cyber Attack on the Ukrainian Power Grid*, by SANS ICS, March 18, 2016. See www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

Mandatory and Enforceable Standards.

In 2005, Congress acted to establish reliability standards for the electricity sector by passing the Energy Policy Act of 2005, which amended the Federal Power Act authorized FERC to commission an Electric Reliability Organization (ERO) with the authority to establish and enforce reliability standards. Under this authority, FERC designated the North American Electric Reliability Corporation (NERC) as the ERO. NERC is a non-profit international regulatory authority whose mission is to assure the reliability and security of the North American bulk power system. Through an extensive stakeholder process, FERC, NERC, and industry stakeholders have developed and implemented infrastructure protection standards for cybersecurity.

Public-Private Partnerships.

Complementing the mandatory reliability standards are a number of voluntary efforts including improved public-private partnerships. The Electricity Subsector Coordinating Council (ESCC) serves as the principal liaison between the electric power sector and the Federal Government.[5] The CEO-led council represents all segments of electricity industry. According to the ESCC, the goal of the council is to "foster and facilitate the coordination of sector-wide, policy related activities and initiatives designed to improve the reliability and resilience of the electricity sector, including physical and cyber security infrastructure."[6] The Electricity Information Sharing and Analysis Center (E-ISAC) serves as the primary security communications channel for the electricity industry, gathering and analyzing security data and threat information from the Department of Homeland Security and other entities, and sharing as appropriate with stakeholders. The E-ISAC operates in collaboration with the Department of Energy (DOE) and the ESCC, and is operated as an independent organization by NERC.[7]

Independent System Operators and Regional Transmission Organizations.

Following FERC Orders to open access to transmission power grids,[8] the first independent grid operators came into existence in the late 1990's. Shortly after, Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs) joined in an industry-wide collaboration called the ISO/RTO council (IRC), which today represents nine ISO/RTO members. ISOs/RTOs administer wholesale energy markets and are responsible for implementing industry and government cybersecurity standards to safeguard the electricity system from cybersecurity threats.

Cybersecurity Provisions under the FAST Act of 2015.

The Fixing America's Surface Transportation (FAST) Act of 2015 updated and expanded the Department of Energy's (DOE) authorities to counter cybersecurity threats. Specifically, section 61003 amends the Federal Power Act (FPA) and designates the DOE as the lead sector-

[5] *See* Electricity Subsector Coordinating Council Brochure (2016)
[6] *Id.*
[7] *See* E-ISAC at https://www.esisac.com/
[8] Order No. 888, Docket No. RM95-8-000, RM94-7-001 and Order No. 889, Docket No. RM95-9-000

specific agency for energy sector cybersecurity.[9] These provisions provide the Secretary of Energy the authority to address grid security emergencies if the 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 defend critical infrastructure, including ordering critical electric infrastructure owners and operators to take appropriate actions. The Act defines "Grid Security emergency" as an "occurrence or imminent danger of—a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communication networks, including hardware, software, and data, that are essential to the reliability of critical electric infrastructure or of defense critical electric infrastructure."[10]

The FAST Act also facilitates the protection and voluntary sharing of critical infrastructure information between private sector asset owners and the Federal Government. Additionally, the FAST Act exempts designated Critical Electric Infrastructure Information from certain federal and state disclosure laws; requires FERC to facilitate voluntary information sharing among federal, state, local and tribal authorities, the electric reliability organization (ERO), regional entities, owners, operators, and users of the bulk-power system in the United States; and establishes sanctions for the unauthorized disclosure of shared information.

IV. ISSUES

The following issues may be examined at the hearing:

- The role of security standards, and oversight of standards implementation.
- Risk assessment, planning, and defense strategies to protect against emerging threats.
- Information sharing practices and related collaboration to identify and respond to emerging threats.
- What are the response planning and practices in the event of a large scale system failure?

V. STAFF CONTACTS

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

[9] Fixing America's Surface Transportation Act, Pub. L. No. 114-94, 129 Stat. 1312 (2015)
[10] *Id.*