STATEMENT OF SCOTT I. AARONSON

VICE PRESIDENT, SECURITY AND PREPAREDNESS

EDISON ELECTRIC INSTITUTE

BEFORE THE U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON ENERGY

"DOE MODERNIZATION: LEGISLATION ADDRESSING CYBERSECURITY AND EMERGENCY RESPONSE"

MARCH 14, 2018

Summary

America's electric companies work every day to produce and deliver energy that is reliable, affordable, safe, and increasingly clean for their customers. The energy grid powers our economy and our way of life, so providing reliable service is a responsibility electric companies take very seriously.

Threats to that reliability have changed over time and continue to evolve. So, too, has our approach to security. EEI's member companies prepare for all hazards—that means physical and cyber events, naturally occurring or manmade threats, and severe weather of every kind. Our security strategies are not put in place with one threat in mind. Our companies take a "defense-in-depth" approach with several layers of security strategies, designed to eliminate single points of failure. Finally, since our companies cannot protect every asset from every threat all the time, we must prioritize based on the likelihood and severity of a threat, as well as work to manage consequences by restoring power quickly and safely regardless of why an outage occurred.

There are three main components to the electric power sector's defense-in-depth approach: mandatory and enforceable reliability regulations; industry/government partnerships; and efforts to enhance our response and recovery to incidents.

Security is a shared responsibility. While most critical infrastructure is owned largely by the private sector, government at all levels can and must play a role in protecting it. Through partnerships like the Electricity Sector Coordinating Council (ESCC), government and industry leverage one another's strengths. This partnership manifests itself in many ways, including deployment of government technologies, multi-directional information sharing, drills and exercises, and facilitating cross-sector coordination.

We appreciate both Congress and the Trump Administration's support of the electric power sector. Just as EEI's member companies evolve to meet new threats, our government partners continuously improve their posture through new initiatives, most recently the establishment of the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) at the Department of Energy.

Introduction

Chairman Upton, Ranking Member Rush, and members of the Subcommittee, thank you for the opportunity to testify. My name is Scott Aaronson, and I am Vice President for Security and Preparedness at the Edison Electric Institute (EEI). EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for 220 million Americans and operate in all 50 states and the District of Columbia. For EEI's member companies, securing the energy grid is a top priority. I appreciate your invitation to discuss this important topic on their behalf.

The electric power industry—which includes investor-owned electric companies, public power utilities, and electric cooperatives—supports more than 7 million American jobs and contributes $880 billion annually to U.S. gross domestic product, about 5 percent of the total.

While I am here today in my EEI capacity and am testifying on behalf of our membership, I would like to highlight another thread that ties the electric sector together: the Electricity Subsector Coordinating Council (ESCC). The ESCC is comprised of the chief executive officers of 22 electric companies and 9 major industry trade associations, including EEI, the American Public Power Association (APPA), and the National Rural Electric Cooperative Association (NRECA). This group—which includes all segments of the industry, representing the full scope of electric generation, transmission, and distribution in the United States and Canada—serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level incidents or threats to critical infrastructure.

We appreciate the continued interest the Committee has on grid security. I was pleased to testify before this Subcommittee in February 2017. In addition to addressing the legislation before the Subcommittee, I would like to update the Committee on several items and reiterate a few key themes.

All Hazards: The Electric Power Industry's Approach to Security

America's electric companies work every day to produce and deliver energy that is reliable, affordable, safe, and increasingly clean for their customers. The energy grid powers our economy and our way of life, so providing reliable service is a responsibility electric companies take very seriously.

Threats to that reliability have changed over time and continue to evolve. So, too, has our approach to security. EEI's member companies prepare for all hazards—that means physical and cyber events, naturally occurring or manmade threats, and severe weather of every kind. Our security strategies are not put in place with one threat in mind. Our companies take a "defense-in-depth" approach with several layers of security strategies, designed to eliminate single points of failure. Finally, since our companies cannot protect every asset from every threat all the time, we must prioritize based on the likelihood and severity of a threat, as well as work to manage consequences by restoring power quickly and safely regardless of why an outage occurred.

Defense-in-Depth: Standards, Partnerships, and Response

I would like to highlight three main components to the electric power sector's defense-in-depth approach: mandatory and enforceable reliability regulations; industry/government partnerships; and efforts to enhance our response and recovery to incidents.

Standards. Under the Federal Power Act and Federal Energy Regulatory Commission (FERC) oversight, the electric power sector is subject to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards that include cyber and physical security requirements. Entities found in violation of CIP standards face penalties that can exceed $1 million per violation per day. These mandatory standards continue to evolve using the process created by Congress to allow for input from subject matter experts across the industry and government.

The industry also uses voluntary standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Department of Energy's (DOE's) Cybersecurity Capability Maturity Model (C2M2).

Through these standards, the entire bulk power system enjoys a baseline level of security. Standards are important, but with intelligent adversaries operating in a dynamic threat environment, regulations alone are insufficient and must be supplemented.

Partnerships. Security is a shared responsibility. While most critical infrastructure is owned largely by the private sector, government at all levels can and must play a role in protecting it.

Through partnerships like the ESCC, government and industry leverage one another's strengths. This partnership manifests itself in many ways, including deployment of government technologies, multi-directional information sharing, drills and exercises, and facilitating cross-sector coordination.

This unity of effort driven by industry working with government has produced significant, tangible results. The sector continues to deploy the Cybersecurity Risk Information Sharing Program (CRISP), a public-private partnership that includes industry, DOE, Pacific Northwest and Argonne National Laboratories, and the Electricity Information Sharing & Analysis Center (E-ISAC), which manages the program. More than 75 percent of U.S. electric customers are served by a company that has deployed CRISP, and this program will continue to grow as the information gleaned from its sensors and the associated analysis has proven extremely valuable to identifying and addressing cybersecurity risks.

Response and Recovery. The electric power sector is proud of its record on reliability, but outages do occur. When outages happen, many key investments help companies restore power safely and as quickly as possible. Our industry invests more than $120 billion each year to make the energy grid stronger, smarter, cleaner, more dynamic, and more secure. The deployment of more than 75 million smart meters, covering more than 60 percent of American households, improves resiliency and service for our customers. The industry's culture of mutual assistance unleashes a world-class workforce amidst the toughest conditions to restore power safely; neighbors helping neighbors during the worst of the worst.

Industry-government exercises, such as the biennial GridEx, sharpen the industry's skill set, ensuring that when incidents happen our playbook has been tested before it is put into action. GridEx IV, held in November 2017, brought together more than 6,000 participants representing more than 400 organizations from across the electric power industry and federal and state governments. These drills sharpen not just the unity of effort between electric companies and government agencies, but also practice unity of message to ensure that we speak with one voice to our customers and your constituents during incidents.

Today, we have supplemented that traditional response and recovery with a 21st-century addition: cyber mutual assistance. The same surge capacity that rushes to companies in need during hurricanes, winter storms, and wildfires stands ready to assist and share resources in the face of a potential cyber incident. So far, more than 140 entities including investor-owned natural gas and power companies, cooperatives, municipalities, Canadian power companies, and Regional Transmission Organizations/Independent System Operators (RTOs/ISOs), are participating in the program. These entities cover more than 80 percent of U.S. electricity customers, roughly 75 percent of U.S. domestic natural gas customers, and 74 percent of natural gas distribution pipelines.

Government's Role in Grid Security

As stated above, grid security is a shared responsibility. We appreciate both Congress and the Trump Administration's support of the electric power sector. Just as EEI's member companies evolve to meet new threats, our government partners continuously improve their posture through new initiatives.

For example, we applaud DOE Secretary Perry and his team for establishing DOE's new Office of Cybersecurity, Energy Security, and Emergency Response (CESER). Legislation passed by this Committee codified DOE's role as the sector-specific agency, and we believe the elevation of CESER will deepen the relationship between our industry and DOE on issues of cybersecurity and energy grid response initiatives. H.R. 5174, the Energy Emergency Leadership Act, amends DOE's enabling statute by adding the new function "energy emergency and energy security" for the to-be-appointed CESER Assistant Secretary. We appreciate the clarification that technical assistance and response capabilities are provided "upon request of a…energy sector entity," but encourage the Committee to consider defining energy emergency and energy security.

The Cyber Sense discussion draft is nearly identical to Section 1106 of H.R. 8, the House-passed comprehensive energy bill from last Congress. The bill establishes "a voluntary Cyber Sense program to identify and promote cyber-secure products intended for use in the bulk-power system." As mentioned above, the electric power industry—and specifically our bulk power system assets—are subject to mandatory and enforceable cyber and physical security standards developed by NERC and approved by FERC. Notably, since House passage of the energy bill in December 2015, a supply chain risk management standard was developed by NERC and proposed to be adopted by FERC. While that standard may obviate the need for a program like Cyber Sense, the Committee may consider supporting ongoing efforts at DOE to establish testing facilities that have similar goals and outcomes to the discussion draft.

The discussion draft "Enhancing Grid Security through Public-Private Partnerships Act" contains several notable provisions. Section 2 establishes a DOE program to advance industry cyber and physical security. The section is aimed at smaller companies—and follows work DOE already is doing through initiatives such as the Rural Cooperative Cybersecurity Capabilities Program between DOE and NRECA and APPA's Cybersecurity Cooperative Agreement with DOE. EEI is supportive of the report ordered by Section 3 of the bill. This DOE-led report on distribution cyber and physical security should address several emerging questions that many in the industry also are asking: What considerations should be made to protect a distribution system that is outside of mandatory NERC CIP standards? How can we secure newer technology that is largely consumer-grade, and may increase the energy grid's attack surface?

The number of distribution assets—including distributed energy resources and customer devices "behind the meter"—is growing and can impact the broader electricity system. As deployment increases throughout the electric delivery system, the security of these interconnected devices must be considered to prevent cybersecurity incidents from impacting reliability.

To be clear, the distribution system has been—and should continue to be—regulated locally by state regulatory commissions. As such, it is welcome that state commissions are one of the consulted entities for the report, alongside industry stakeholders. At the same time, there is benefit to uniform standards since these vendors and their devices are sold across state lines. However, mandates should be avoided, as they could be prohibitively expensive for electric companies and their customers. Taken together, it is clear that a collaborative, risk-based

approach to security at the distribution level is essential. This report should drive that approach and consider the many different entities in the distribution grid—electric companies and others.

Conclusion

Thank you again for holding this hearing. I am hopeful that my testimony underscores the industry's commitment to security and our willingness to work with many partners to address all hazards. We look forward to continuing close collaboration with our government partners to meet the evolving threat. We appreciate the bipartisan support that grid security legislation historically has enjoyed in Congress and the work you have done to enhance our security posture. We look forward to working on these legislative proposals and others to meet this most-important mission.