STATEMENT OF SCOTT I. AARONSON
EXECUTIVE DIRECTOR, SECURITY AND BUSINESS CONTINUITY
EDISON ELECTRIC INSTITUTE
AND
SECRETARIAT MEMBER
ELECTRICITY SUBSECTOR COORDINATING COUNCIL

BEFORE THE U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON ENERGY

"THE ELECTRICITY SECTOR'S EFFORTS TO RESPOND TO CYBERSECURITY THREATS"

FEBRUARY 1, 2017

Summary

We depend upon reliable and secure electricity to power our economy and our way of life. Providing this energy and protecting the energy grid against threats are responsibilities that our nation's electric companies take very seriously. Importantly, electric companies understand that they cannot protect all assets from all threats and, instead, must manage risk. Rather than trying to achieve the impossible task of protecting every asset from every conceivable threat, companies follow a multi-layered risk management approach to grid protection known as defense-in-depth.

Under FERC oversight, NERC establishes security standards and regulations that are important to the industry's security posture. In addition to regulations and standards, close coordination and the sharing of threat information between the government and industry help to protect the grid.

The Electricity Subsector Coordinating Council (ESCC), the principal liaison between the federal government and the electric power sector, coordinates efforts to prepare for, and respond to, national-level incidents or threats to electric-sector critical infrastructure. The ESCC focuses on four main areas to improve grid security: Tools and Technology; Information Flow; Incident Response and Recovery; and Cross-Sector Coordination.

Protecting and defending the energy grid against threats are not enough; we also must plan to respond and recover should an incident impact operations.

We also are working to deal with new and emerging cyber threats, such as those potentially associated with distributed energy resources and the Internet of Things.

Security cannot be static; threats evolve and so must we. The electric sector embraces this fact, as demonstrated by the ongoing development of regulatory standards; the high-level partnerships developed under the ESCC that are enabling us to accomplish more in less time; and the focus on constantly evolving preparedness by applying lessons learned from exercises and real-world events.

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 Executive Director for Security and Business Continuity 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, operate in all 50 states and the District of Columbia, and directly and indirectly support more than 1 million American jobs. EEI has more than 60 international electric company members, and 270 industry suppliers and related organizations as associate members. 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.

In addition to my role at EEI, I also serve as a member of the Secretariat for 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. 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.

The ESCC has been held up by the National Infrastructure Advisory Council as a model for how critical infrastructure sectors can more effectively partner with government. In fact, the ESCC

has been a catalyst for major initiatives that are improving the security posture of the industry and, by extension, the nation.

My testimony focuses on the initiatives the electric power industry is taking to respond to grid security threats, the value of our government-industry partnership in the face of threats to the electric sector, and the public policy considerations and strategic initiatives that can enhance the cybersecurity of one of the nation's most critical infrastructure sectors.

Managing Risk: An Overview of Threats to Critical Electric Infrastructure

Electric companies understand that reliable and secure electricity is essential to the nation's economy and our way of life. Providing reliable service is a responsibility electric companies take very seriously. Importantly, companies also understand that they cannot protect all assets from all threats and, instead, must manage risk. Rather than trying to achieve the impossible task of protecting every asset from every conceivable threat, the electric sector follows a multi-layered risk management approach to grid protection known as "defense-in-depth."

The key to this strategy involves setting priorities to protect the most critical energy grid components against the most likely threats. If we frame risk as a function of likelihood and consequence, then we can allocate resources more effectively to meet those threats.

The ESCC is an important partnership that has developed between government and industry to ensure the sector and our nation are secure. Man-made events (such as coordinated cyber and physical attacks) and natural phenomena (like solar flares, major earthquakes, or weather events

on the scale of Superstorm Sandy) require coordination between government and industry, as well as across the critical infrastructure sectors. Every critical infrastructure industry is dependent upon each other to provide services to customers.

Grid operators prioritize risk in order to enhance protection around critical assets, engineer redundancy to avoid single points of failure, stockpile spare equipment for hard-to-replace components, and develop other contingencies to minimize impact regardless of the nature of the incident.

By exercising and applying lessons from actual events, electric companies are able to enhance grid protection, resiliency, and restoration efforts. Invaluable insights have been gained from events such as Hurricane Katrina, Superstorm Sandy, the April 2013 Metcalf Substation attack in California, and events in Ukraine, where industry experts accompanied a Department of Energy (DOE) after-action assessment team.

It is this flexibility and adaptability in the face of an always-evolving threat environment that are positioning the industry to be prepared to manage risk and to respond to all hazards.

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

The electric power sector's defense-in-depth approach to protecting grid assets includes several tools that, when taken together, provide a more comprehensive approach to the industry's security posture. Specifically, the industry is subject to rigorous, mandatory, and enforceable reliability regulations; closely coordinates with industry and government partners at all levels;

and has efforts in place to prepare, respond, and recover should energy grid operations be impacted.

Security standards and regulations are important to the industry's security posture. 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 with input from subject matter experts across the industry and government. Currently, the electric power sector must comply with Version 6 of the cybersecurity standards, and additional modifications are underway to add new requirements mirroring best practices in cybersecurity.

In addition to implementing Version 6 of the cybersecurity requirements, NERC and the industry are developing new requirements to address supply chain cybersecurity. The industry also is implementing new mandatory requirements for physical security as part of the broader suite of NERC regulatory standards.

The industry also uses voluntary standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, as well as DOE's Cybersecurity Capability Maturity Model (C2M2). Electric companies throughout the industry are assessing their

cybersecurity capabilities against this framework and maturity model and, based on results, prioritizing their investments to strengthen cybersecurity.

While regulations and standards provide a solid foundation for strengthening the industry's security posture, they alone are insufficient. As the threat environment evolves, so must the industry's security efforts.

In addition to regulations and standards, close coordination and the sharing of threat information between government and industry help to protect the energy grid.

As noted throughout this testimony, protection of critical infrastructure is a shared responsibility between the government and industry. The ESCC was formed to help coordinate these efforts and to ensure we are appropriately deploying each other's expertise, capabilities, and assets. The ESCC consists of electric company CEOs and trade association leaders who represent all segments of the electric sector and who actively partner with government executives to prepare for, and respond to, national-level incidents or threats to critical infrastructure.

A key characteristic of the ESCC is executive engagement. In addition to providing resources and accountability that have pushed both the government and industry to work very closely and very quickly, senior executives on both sides also help to ensure unity of effort and unity of message among their organizations. During an incident, the ESCC's role—while not operational—is to provide situational awareness, ensure coordination with government on response and recovery efforts, and align messaging.

The industry and government leaders are focusing on four main areas that improve the security posture of the industry and the nation:

1. Tools & Technology: Deploying government technologies that improve situational awareness and enable machine-to-machine information sharing;

2. Information Flow: Making sure actionable intelligence and threat indicators are communicated to the right people at the right time in the right way;

3. Incident Response and Recovery: Planning and exercising to coordinate responses to an incident;

4. Cross-Sector Coordination: Working closely with other interdependent infrastructure sectors (*e.g.*, communications, downstream natural gas, financial services, water) to ensure all are prepared for, and can respond to, national-level incidents.

Some specific examples of ESCC initiatives within these areas of focus:

Cybersecurity Risk Information Sharing Program (CRISP)

The electric power sector is deploying the Cybersecurity Risk Information Sharing Program (CRISP) to bolster its situational awareness and information sharing. CRISP is 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. CRISP seeks to facilitate timely bi-directional sharing of actionable unclassified and classified threat information, using advanced collection, analysis, and dissemination tools to identify threat patterns and trends across the electric power industry. CRISP enables near real-time sharing of cyber threat data among government and industry stakeholders.

Cyber threat information shared through CRISP is helping to inform important security decisions, not just among participating companies but also to all E-ISAC members throughout the electric sector, as information gleaned by the technology is then shared anonymously through the E-ISAC portal. More than 75 percent of all electricity customers are served by electric companies that have deployed CRISP.

Sharing Actionable Intelligence

The electric power industry values its security partnership with the U.S. government. One recent event provides a real-world illustration of how the industry-government partnership works to enhance cybersecurity. In late December 2016, senior DOE and Department of Homeland Security (DHS) officials briefed the ESCC and other energy sector representatives regarding Russian cyber incidents against U.S. private-sector interests. Critical infrastructure sectors—including the electric sector—took immediate steps to review and to secure their systems based on this intelligence. As it turned out, one U.S. electric company discovered a suspected Russian presence on its enterprise network. The company shared this information with DOE, DHS, and all appropriate authorities. Fortunately, no systems responsible for grid operations were impacted.

In this case, thanks to close and ongoing coordination through the ESCC, actionable government intelligence was shared with private-sector operators throughout the sector to better inform their defenses. Electric companies, in turn, continue to share information about compromises with the government to raise awareness of cybersecurity incidents across the private sector and to inform best practices for protection and mitigation.

Cyber Mutual Assistance

The electric power industry has a culture of mutual assistance; when a weather event or natural disaster impacts a region, crews and lineworkers from all over North America descend on the affected region to restore power. Through storm preparation and mutual assistance networks, electric companies have decades of experience working together in response to major incidents.

For example, the sector's response to Superstorm Sandy had companies from as far away as California, Texas, and Canada sending equipment and crews into the affected regions to restore power. More than 80 companies and tens of thousands of mutual assistance crews responded. Similar responses were seen following Hurricanes Katrina and Rita, and, most recently, following Hurricane Matthew last October. In short, mutual assistance is not just a program, it is in our industry's DNA.

As cyber risks proliferate, the industry, with the ESCC's leadership, moved to develop a cyber mutual assistance program to aid electric companies in restoring necessary computer systems following a regional or national cyber incident. This program builds on the industry's culture of

mutual assistance to develop resource-sharing relationships that can provide surge capacity should a cyber incident exceed the capacity for an individual company to respond.

In addition, electric companies work to maintain and strengthen their ties to state agencies, state and local law enforcement, as well as state Fusion Centers that receive, gather, analyze, and share threat information.

Protecting and defending the energy grid are not enough; we also must plan to respond and recover should an incident impact operations.

Owners and operators of critical infrastructure strive for a 100-percent success rate in their protection efforts, but the adversary only needs to be right once. Given these odds, a comprehensive approach to security must include contingency plans to respond and recover as quickly as possible in the event something occurs.

DOE FAST Act Emergency Authority

Congress took steps to ensure a single government entity would have emergency authority and ultimate responsibility in the event of a true grid security emergency resulting from a cyber attack or other types of intentional or existential threats to the grid. The 2015 transportation bill ("Fixing America's Surface Transportation Act" or FAST Act) provides that, upon a Presidential determination of a grid security emergency, DOE has authority to issue an order for emergency measures to be taken by NERC, a regional entity, or electric sector owners and operators. We commend you for your foresight in addressing this issue, and we are working with DOE to determine the scope and process for such emergency orders. We also appreciate language in the

bill providing liability protections for actions taken in compliance with an order, as well as important protections against public disclosure of sensitive critical energy infrastructure information shared with DOE and FERC.

Spare Equipment Sharing and Transportation

Just as electric companies share crews as part of the industry's voluntary mutual assistance programs to restore power, they also regularly share transformers and other equipment. The electric power sector is expanding equipment-sharing programs—like the Spare Transformer Equipment Program (STEP), *SpareConnect*, and two newer industry-led programs, Grid Assurance and RESTORE (Regional Equipment Sharing for Transmission Outage Restoration)—to improve grid resilience no matter the threat.

The electric power sector's success regarding these transformer-sharing programs depends upon the industry's ability to move large spare equipment, such as transformers, quickly over our rails, roadways, and waterways. That is why the industry is working with other critical infrastructure sectors and the government to improve the coordination and preparation involved in moving large transformers during an emergency. For example, electric companies, Class I railroads, and the heavy hauler and rigging industries have developed a Transformer Transportation Emergency Support Guide to help move these critical assets rapidly in an emergency.

Exercises

Electric companies plan and regularly exercise for a variety of emergency situations—including cyber attacks—that could impact their ability to provide electricity. The largest so far, in

November 2015, was the third biennial industry-wide grid security and incident response exercise known as GridEx III, which brought together more than 364 organizations and 4,400 participants from industry, government agencies, and partners in Canada and Mexico to participate in a rigorous and comprehensive two-day drill that simulated coordinated cyber and physical attacks on the energy grid.

GridEx III also included an executive tabletop exercise that brought together 32 electric power sector executives and senior U.S. government officials to work through incident response protocols to address widespread outages. GridEx III was a continuation of industry-government efforts to participate in exercises that strengthen the security and resiliency of the energy grid.

In its GridEx III After-Action Report, NERC found that, since GridEx II in 2013, industry and government responses to a significant cyber/physical attack continued to improve. The report identified a number of recommendations for industry and government to continue to strengthen their coordination, preparation, and response capabilities. As was the case with GridEx I and II, these recommendations provide a road map for how the ESCC, with input from NERC, and the government should address security issues. GridEx IV is scheduled for November 2017.

Other recent national-level exercises in which the industry has participated include: Clear Path IV, conducted by DOE in April 2016; Cascadia Rising, sponsored by FEMA in 2016; Cyber Guard, a two-week DOD-NSA cyber exercise involving experts from government and the energy, IT, and transportation sectors; and a Treasury Department Joint Financial Services-

Electric Sector Cyber Exercise in August 2016 that examined incident response capabilities and interdependencies between the two sectors.

Supplemental Operating Strategies

One example of "lessons learned" from these exercises and the December 2015 cyber incident affecting Ukraine is a renewed focus on supplemental strategies for operating the energy grid under sub-optimal circumstances. Whether resorting to manual operations, engaging in planned separations, leveraging secondary and tertiary back-up systems, or operating in other degraded states, the industry is working with grid experts to explore "extraordinary measures" that can be anticipated, planned for, and practiced so these are not being contemplated for the first time during an incident.

We continue to plan and move forward to deal with emerging cyber threats.

In addition to the many ongoing industry cybersecurity and resiliency programs, some of which are highlighted in my testimony, the electric sector also is looking ahead to deal with new and emerging cyber issues.

For example, as new distributed energy resources (DER) and behind-the-meter assets have a growing impact on grid operations, new vulnerabilities are created because these technologies are not subject to the same reliability mandates and security requirements that electric companies must meet. Electric companies do not have organizational control over most DER systems, and the customers controlling DER systems do not have a thorough understanding of cyber vulnerabilities or the knowledge and capability to combat cyber threats.

DER may provide an increasing number of potential entry points for access to electric companies' control systems and can affect the operation of the transmission system. DER systems are more reliant on communication and information sharing between grid components, some of which may be open to physical and internet access, making them more vulnerable.

While the promise of DER can increase grid resilience, the integration of these resources at all points in the electric system must be coordinated thoughtfully. The promise of DER and its contributions to resilience require coordinated planning and investments in controls to ensure energy grid operators have visibility into these new resources.

Similarly, the installation of billions of internet-connected consumer devices is another area of potential concern. While devices comprising the "Internet of Things" (IoT) typically are not directly connected to energy grid infrastructure in the same way as DER, electric companies still recognize the risks related to cyber attacks that may seek to leverage the IoT in a way that would impact the energy grid and electric reliability.

The industry already has faced instances of distributed denial of service attacks similar to IoT-leveraged incidents in other business sectors last year. However, these attacks have focused on business systems (such as customer service), and electric reliability has not been impacted. Nevertheless, the E-ISAC and the government share actionable intelligence with the industry and electric companies routinely examine their internet-facing systems for vulnerabilities to ensure that all systems have adequate protections in place.

Conclusion

With exercises and real-world events serving as catalysts for new initiatives—from developing a cyber mutual assistance regime to looking at extraordinary measures the sector can take to mitigate damage from incidents—the electric sector is constantly improving its security posture and approach to preparedness.

Security cannot be static; threats evolve and so must we. The electric sector embraces this fact as demonstrated by the ongoing development of regulatory standards, the high-level partnerships developed under the ESCC that are enabling us to accomplish more in less time, and the focus on constantly improving preparedness by applying lessons learned from exercises and real-world events. As industry and government leadership improves our ability to protect critical infrastructure from all types of threats, we look forward to working with Congress on this important mission.

I appreciate the Subcommittee holding this hearing to learn more about cyber and other threats facing the industry. It is my hope that this testimony provides insight into what the electric sector is doing to address these threats, while also making clear that there is no such thing as risk elimination, only risk management.

As we work to manage risks facing the sector and the nation, I am proud to say our nation's electric companies and the government share a sense of urgency, and are working closely in innovative ways to protect critical energy infrastructure from attacks and to limit the consequences of an attack should one occur.