STATEMENT OF SCOTT I. AARONSON
MANAGING DIRECTOR, CYBER AND INFRASTRUCTURE SECURITY
EDISON ELECTRIC INSTITUTE

BEFORE THE U.S. SENATE HOMELAND SECURITY
AND GOVERNMENT AFFAIRS COMMITTEE

"ASSESSING THE SECURITY OF CRITICAL INFRASTRUCTURE:
THREATS, VULNERABILITIES, AND SOLUTIONS"

MAY 18, 2016

Introduction

Chairman Johnson, Ranking Member Carper, and members of the Committee, thank you for the opportunity to testify. My name is Scott Aaronson, and I am Managing Director for Cyber and Infrastructure Security 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 70 international electric companies as Affiliate Members, and 270 industry suppliers and related organizations as Associate Members. For EEI's member companies, securing the power 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 Secretary for the Electricity Subsector Coordinating Council (ESCC). The ESCC is comprised of the chief executive officers of 21 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 disasters 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 value of the government-industry partnership in the face of threats to the electric sector, as well as the public policy considerations and strategic initiatives that can enhance the security of the nation's most critical infrastructure.

Managing Risk: An Overview of Threats to Critical Electric Infrastructure

Electric companies understand that reliable electricity is essential to the nation's security and our way of life. Providing reliable service is a responsibility the industry takes extremely seriously. Importantly, the industry also understands that it 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.

The key to this strategy involves setting priorities to protect the most critical power 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.

With threats that are less likely to occur, but could have potentially severe impacts to grid reliability, an important partnership has developed between government and industry to ensure the sector and our nation are secure. It is the man-made events—such as coordinated cyber and physical attacks or an electromagnetic pulse (EMP)—or the natural phenomena, like solar flares, major earthquakes, or weather events on the scale of Superstorm Sandy, that require coordination between government and industry, as well as across the critical infrastructure sectors.

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 recent events in Ukraine where industry experts accompanied a 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 truly prepared to manage risk and respond to all hazards.

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

The electric power sector takes what is known as a “defense-in-depth” approach to protecting grid assets. This 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 power 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 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 of up to $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 3 of the cybersecurity standards, while Versions 5 and 6 become enforceable on July 1, 2016. These new versions are more rigorous than the past versions. Not only do they increase the scope of the standards, they also add several new cybersecurity requirements that mirror best practices in cybersecurity.

In addition to implementing Versions 5 and 6 of the cybersecurity requirements, prompted in part by lessons learned from the aforementioned Metcalf attack, the industry is implementing new mandatory requirements for physical security as part of the broader suite of NERC regulatory standards.

The industry also is using voluntary standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, as well as the Department of Energy's Cybersecurity Capability Maturity Model (C2M2). Electric companies throughout the industry are assessing their cybersecurity capabilities against this framework and capability 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 protect the power grid.

As has been 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 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, align messaging, and coordinate with government on response and recovery efforts.

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

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;

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

4. Cross-Sector Coordination: Working closely with other interdependent infrastructure sectors to ensure all are prepared for, and can respond to, national-level incidents.

Within these areas of focus there are three specific ESCC initiatives I would like to highlight:

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, the electric power sector has 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. In short, mutual assistance is not just a program, it is in our DNA.

As cyber risks proliferate, the industry is organizing itself to pool resources in the face of incidents that exceed the capacity of individual companies to respond. In its early stages now, a framework is being developed to identify and share resources during incidents. Over the long-term, this project—with the backing and leadership of senior industry executives—will evolve based on the cyber incident response needs of the industry. In addition, electric companies work to maintain and strengthen their ties to state agencies, state and local law enforcement, and state Fusion Centers that receive, analyze, gather, and share threat information.

Cybersecurity Risk Information Sharing Program (CRISP)

The electric power sector has deployed CRISP to bolster its situational awareness and information sharing. CRISP developed as a partnership among five pilot electric companies, the Department of Energy (DOE), the Electricity Information Sharing & Analysis Center (E-ISAC), and the Pacific Northwest and Argonne National Laboratories. CRISP enables near real-time sharing of cyber threat data among government and industry stakeholders, while supporting machine-to-machine threat mitigation.

Cyber threat information shared through CRISP is helping to inform important security decisions not just among participating companies, but to all E-ISAC members throughout the electric sector, as information gleaned by the technology is then shared anonymously through the E-ISAC portal. By the end of this year, more than 75 percent of all electricity customers will be covered by an electric company that will have deployed CRISP, but the entire industry continues to benefit.

Electromagnetic Pulse (EMP) Mitigation

The ESCC works closely with the government to better understand the threat posed to electric infrastructure from a man-made EMP, either from a high-altitude nuclear blast or a so-called “directed energy” weapon. Based on these discussions, and building on research done by the

National Labs and Department of Defense, the Electric Power Research Institute (EPRI) is undertaking a major collaborative research effort with DOE. This project is designed to enhance our understanding of system impact should such an attack occur and to explore the effectiveness of mitigation strategies (including hardening and recovery). The project will allow grid-specific research to inform the application of technologies that will increase grid resilience and accelerate recovery.

A recent Government Accountability Office (GAO) report recommended enhanced federal agency coordination with industry to identify and prioritize risk-management activities, such as research and development efforts, to address EMP risks to the grid. The recently initiated EPRI project is just such an effort.

Protecting and defending electric infrastructure 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.

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 the newly announced Grid Assurance program—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 developed a new Transformer Transportation Emergency

Support Guide to expedite the deployment of equipment and services that would be needed to move these critical assets rapidly in an emergency.

With respect to exercises, this past November, NERC conducted the third biennial industry-wide grid security and incident response exercise, known as GridEx III. GridEx III 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 power 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 power grid.

On March 31, NERC released its GridEx III After-Action Report to the public. Overall, NERC found that since GridEx II, industry and government responses to a significant cyber / physical attack continue to improve. The After-Action 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 will provide a road map for how the ESCC, with input from NERC, and the government will address security issues over the next two years.

With exercises and real-world events serving as catalyst 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.

Conclusion

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.

On behalf of owners and operators of critical electric infrastructure, I appreciate the Committee holding this hearing to learn more about 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 the electric sector and the government are working closely in innovative ways to protect critical infrastructure from attacks and to limit the consequences of an attack should one occur.