STATEMENT OF SCOTT I. AARONSON

VICE PRESIDENT, SECURITY AND PREPAREDNESS

EDISON ELECTRIC INSTITUTE

BEFORE THE U.S. SENATE HOMELAND SECURITY AND

GOVERNMENTAL AFFAIRS COMMITTEE

"PERSPECTIVES ON PROTECTING THE ELECTRIC GRID FROM AN ELECTROMAGNETIC PULSE OR GEOMAGNETIC DISTURBANCE"

February 27, 2019

Summary

America's electric companies work every day to produce and deliver energy that is reliable, affordable, safe, and increasingly clean for their customers and the communities they serve. The energy grid powers our economy and our way of life, and 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. The Edison Electric Institute's (EEI's) member companies prepare for all hazards—that includes man-made threats, such as physical and cyber attacks or impacts from intentional electromagnetic interference, and naturally occurring events, including severe weather of every kind, earthquakes, and geomagnetic disturbances. 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, which are 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 impacts 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 ability to respond and recover following 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 Subsector 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, exercises, and facilitating cross-sector coordination.

Addressing dynamic threats to the energy grid requires vigilance and a coordinated approach that leverages government and industry resources. We appreciate both Congress and the Administration's support of the electric power sector, and we look forward to continuing our close collaboration to meet the evolving threats.

Introduction

Chairman Johnson, Ranking Member Peters, and members of the Committee, 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 $865 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 power 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. While I am not representing the ESCC officially, I serve as a member of the Secretariat that supports the Council, so my perspectives are shaped by that role and are aligned with the broader industry.

We appreciate the continued interest the Committee has on grid security and, specific to this hearing, the impacts of electromagnetic pulse (EMP) and natural geomagnetic disturbances (GMDs) on the energy grid.

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 and the communities they serve. The energy grid powers our economy and our way of life, and 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, which are 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 impacts 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) Reliability Standards that include cyber and physical security requirements. Entities found in violation of NERC 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.

Through these standards, the entire bulk power system enjoys a baseline level of security and reliability. 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.

Response and Recovery. The electric power sector is proud of its record on reliability, which includes the resilience of the system. When outages do occur, many key investments help electric companies restore power safely and as quickly as possible. Our industry invests more than $100 billion each year to make the energy grid stronger, smarter, cleaner, more dynamic, and more secure. Further, 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. These exercises 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.

How GMDs Differ from EMPs

The threats we are here to discuss today are EMPs and GMDs. First, I want to highlight that there are important differences between man-made EMPs, such as those from directed energy weapons or nuclear detonations, and naturally occurring GMDs, such as solar flares. Though both create magnetic disturbances, their characteristics are very different. Therefore, each threat must be addressed independently, and appropriate mitigation and protection strategies must be implemented for each.

GMDs are naturally occurring events that the electric power industry has managed for decades. The industry is subject to mandatory and enforceable standards, developed by NERC under

FERC oversight, to protect the energy grid from the impacts of GMDs, and electric companies have operating processes and procedures to manage GMD risks.

To mitigate the threat of GMDs on the energy grid, there are two standards in place regarding GMDs. NERC's standard TPL-007-1 requires transmission-owning electric companies to assess and analyze their transmission systems under a severe 1-in-100-year GMD benchmark planning event. Last year, NERC developed TPL-007-2, a modification to TPL-007-1. In November, FERC approved TPL-007-2, which broadens the definition of GMDs, requires grid operators to collect certain data, and imposes deadlines for corrective actions. The other standard, EOP-010-1, requires operating plans, processes, and procedures to mitigate the effects of a GMD event.

There are two categories of intentional, man-made EMPs. The first, a high-altitude EMP caused by the detonation of a nuclear weapon in the atmosphere, is a high-consequence, low-likelihood threat that would have a potentially catastrophic impact on society. Since a nuclear attack on U.S. critical infrastructure would be an act of war or terrorism, the federal government has primary responsibility for preventing high-level EMPs as a matter of national security. The industry also is taking steps to better understand the impact of this threat to its systems to engineer greater resilience against such a catastrophic incident.

The second type of EMP is related to the use of smaller directed energy weapons against a single facility or piece of equipment. Mitigation strategies for this type of EMP threat include physical protection measures, including limiting line-of-sight and controlling access, while also relying on system redundancy. To cause significant damage to the energy grid, dozens of directed energy weapons would need to be built, deployed, and detonated in a coordinated attack without being detected or stopped by law enforcement. To address the physical protection of critical equipment, NERC developed the CIP-014-1 standard, which requires transmission-owning electric companies to identify and protect critical transmission stations and substations, along with their associated control centers.

Industry Initiatives and Collaboration

Policymakers and the electric power industry share the goal of developing capable, cost-effective mitigation to threats. Because the effects of an EMP attack on the energy grid are not understood sufficiently or remain classified, crafting appropriate mitigations and making business-risk decisions to address EMP threats require more research to better understand how EMPs could impact the grid; inform the development of EMP-resistant grid components; and develop best practices to help limit the impact of these threats.

To address these challenges, the Electric Power Research Institute (EPRI), an independent research organization funded by industry, launched a research project in 2016 to provide a scientific basis for investments to mitigate EMP threats on the transmission system, inform response and recovery efforts, and develop other partnerships that will help the nation's critical infrastructure be better prepared for existential threats to the energy grid. As the primary liaison between senior leadership in the federal government and the industry, the ESCC is working with government partners to better understand the threat posed to energy infrastructure from a man-made EMP. The ESCC also supports EPRI's efforts.

As referenced above, regardless of the cause of damage to the energy grid, preparations to ensure mitigation, response, and restoration are the same: grid operators prioritize risk 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 impacts. The ESCC is involved in all aspects of these preparations.

- **Exercises:** Electric companies plan and regularly exercise for a variety of emergency situations that could impact our ability to provide electricity. The industry participates in numerous local, state, and national exercises every year. One such exercise, GridEx IV, involved more than 450 organizations and 6,500 participants from industry, government agencies, and partners in Canada and Mexico. Managed by NERC and the Electricity Information and Analysis Center (E-ISAC), GridEX IV also included an executive tabletop exercise where 40 electric power sector executives and senior U.S. government officials worked through incident response protocols to address widespread outages. GridEx events are conducted every two years; GridEx V is planned for November 2019.

- **Mutual Assistance Programs:** The three segments of the electric power industry—public power, investor-owned, and electric cooperatives—have long had in place mutual assistance response networks to share employees and resources to restore power after emergencies. The years of experience industry has had in deploying these resources is a

valuable tool. In fact, the ESCC has led efforts to create a Cyber Mutual Assistance (CMA) program that allows electric and natural gas companies to share critical personnel and equipment in the event of cyber-related emergencies. To date, more than 150 electric and natural gas companies are participants, covering about 80 percent of the country's electricity customers and 75 percent of U.S. domestic natural gas customers.

- **Spare Equipment Programs:** Electric companies regularly share transformers and other equipment through long existing bi- and multi-lateral sharing arrangements and agreements. The industry is expanding equipment sharing programs—like the Spare Transformer Equipment Program (STEP) and SpareConnect program—to improve grid resiliency.

- **Transformer Transportation Emergency Support Guide:** The ESCC, in coordination with other critical infrastructure sectors and the government, has developed a Transformer Transportation Emergency Support Guide to expedite the deployment of large spare equipment, such as transformers, over rail, roadways, and waterways quickly in an emergency.

- **Supplemental Operating Strategies:** Following GridEx III and the cyber incident affecting Ukrainian distribution electric companies, the industry focused on energy grid operations under sub-optimal circumstances. The ESCC asked grid experts at the North American Transmission Forum (NATF) to explore "extraordinary measures" that can be anticipated, planned for, and practiced so they are not contemplated for the first time during an incident that disables significant technology used to operate the grid. These "extraordinary measures" include, but are not limited to, operating systems in "manual" configuration where systems are not allowed to automatically re-energize, engaging in planned separations of portions of the grid to avoid cascading outages, leveraging secondary and tertiary back-up systems, or operating in other degraded states.

- **Grid Security Emergency (GSE) Authorities:** To support the Department of Energy's (DOE's) GSE Authorities planning, the ESCC requested that the NATF develop a report to identify potential actions that would inform the government on how emergency orders effectively could bolster electric companies' protection, response, and recovery efforts. NATF, in coordination with DOE, determined that, since there are existing industry procedures that address operations and risk mitigation associated with GMD, the report would focus on before, during, and following a GMD event.

- **Research & Development:** The ESCC R&D strategic committee is overseeing the industry's collaboration efforts with the government, including the national labs, on resilience and infrastructure investments for grid security R&D. The Committee serves as the coordination point for EPRI's EMP and GMD work.

Government's Role in EMP and GMD

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

Most notably, thanks to Secretaries Perry and Nielsen and their respective teams' efforts, as well as legislation passed by Congress last year, we believe government is well-positioned to continue its support of industry in securing the nation's most critical infrastructure. Specifically, the establishment of DOE's new Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and the Department of Homeland Security's (DHS's) Cybersecurity and Infrastructure Security Agency (CISA) elevated and deepened the relationship between our industry, DOE, and DHS on issues of cybersecurity, EMP, GMD, and energy grid response and resilience initiatives.

With input from the industry, DOE released the Electromagnetic Pulse Resilience Action Plan[1] in 2017 that identified five goals: (1) improve and share understanding of EMP threats, effects, and impacts; (2) identify priority infrastructure; (3) test and promote mitigation and protection approaches; (4) enhance response and recovery capabilities to an EMP attack; and(5) share best practices across government and industry, nationally and internationally. The EPRI project is complementing and helping achieve these goals.

Last October, DHS released the Strategy for Protecting and Preparing the Homeland against Threats from Electromagnetic Pulse (EMP) and Geomagnetic Disturbance (GMD).[2] The Strategy lays out an approach for DHS to take to protect critical infrastructure and prepare to respond and recover from potentially catastrophic electromagnetic incidents. As noted by DHS, the Strategy primarily is focused on Departmental activities; however, it does recognize continued close collaboration with private sector critical infrastructure owner-operators. This partnership is essential to help critical infrastructure owners and operators manage EMP and GMD risk.

Conclusion

[1] https://www.energy.gov/sites/prod/files/2017/01/f34/DOE%20EMP%20Resilience%20Action%20Plan%20January%202017.pdf

[2] https://www.dhs.gov/sites/default/files/publications/18_1009_EMP_GMD_Strategy-Non-Embargoed.pdf

Thank you again for holding this hearing. I am hopeful that my testimony underscores the industry's commitment to security and our willingness to address threats from EMP and GMD to the nation's critical energy infrastructure. Addressing dynamic threats to the energy grid requires vigilance and coordination that leverages government and industry resources. Through the NERC-FERC standards process, the industry will continue to address bulk power system issues associated with GMDs. In the next few months, EPRI will share its EMP findings with the industry, providing the necessary information for companies to better understand the potential impact of EMP incidents to the transmission system and recommendations for mitigation approaches and investments.

Through the ESCC, the electric power industry will continue to strengthen its government partnerships, coordinate with other critical infrastructure sectors, engage and educate external stakeholders and the public, and make necessary investments in the energy grid to help ensure it is stronger, more reliable, and more resilient in the face of any threat.

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. As policymakers, there are several ways in which you can support our efforts. First, we recommend that the newly reconstituted EMP Commission include owners and operators of critical infrastructure and EPRI. Having the knowledge of experts in grid engineering and operations would enable the Commission to produce a more meaningful and informed product. I encourage all Members of the Committee to receive a classified briefing on the EMP threat. I believe our government partners along with industry representatives, would be more than happy to continue this discussion in classified space.

I want to reiterate that this is an extremely complex issue that cannot be solved with a "one-size-fits-all" solution. Prescriptive legislative directives, especially before EPRI completes its work, could have unintended consequences on operations of the energy grid and increase costs to our customers. Similarly, as recommendations and solutions are identified, the industry will take action, engage Congress, and, if necessary, leverage the NERC/FERC standards-setting process

that produces standards based upon expert input—a necessity when it comes to the vast and complex bulk electric system.

Finally, the industry will continue to work with Congress on response and recovery initiatives that support its all-hazard approach to threats. At the end of the day, it doesn't matter why the lights are out, as we must work together collectively to restore power safely and as quickly as possible.

We look forward to working with your respective committees and other relevant committees to meet this most-important mission. Thank you, and I look forward to answering any questions you may have.