STATEMENT OF SCOTT I. AARONSON
SENIOR VICE PRESIDENT, SECURITY AND PREPAREDNESS
EDISON ELECTRIC INSTITUTE

BEFORE THE U.S. SENATE
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SUBCOMMITTEE ON WATER AND POWER

HEARING TO "EXAMINE THE FEDERAL AND NON-FEDERAL ROLE OF ASSESSING CYBER THREATS TO AND VULNERABILITIES OF CRITICAL WATER INFRASTRUCTURE IN OUR ENERGY SECTOR"

APRIL 10, 2024

Introduction

Chairman Wyden, Ranking Member Risch, and members of the Subcommittee, thank you for the opportunity to testify. My name is Scott Aaronson, and I am Senior 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 nearly 250 million Americans and operate in all 50 states and the District of Columbia. For EEI's member companies, securing the energy grid from all hazards, including cyber threats, is a top priority. I appreciate your invitation to discuss this important topic on their behalf.

The energy grid powers our way of life and is critical to America's security and economic competitiveness. Today, demand for electricity is growing dramatically across the economy to support evolving customer needs, as well as critical technologies like artificial intelligence and the proliferation of data centers that fuel our digital lives. Ensuring a secure, reliable, resilient energy grid is a responsibility that EEI's member companies and the electric power sector take extremely seriously.

Threat Landscape

As the grid continues to evolve, so, too, do the threat actors who seek to undermine U.S. critical infrastructure. For years, the U.S. intelligence community has warned of the potential for malicious nation-state exploitation of U.S. critical infrastructure. Today, we know from our federal partners that People's Republic of China state-sponsored cyber actors known as Volt Typhoon have compromised multiple U.S. critical infrastructure providers with the intent of disrupting operational controls.

With the increasingly complex geopolitical threat landscape and the sophistication of ransomware operations by transnational organized criminals, we have seen an uptick in threats to critical infrastructure organizations across all sectors. The infiltration of the controls of a New York dam in 2013, and the exploitation of programmable logic controllers in Pennsylvania and across the Water and Wastewater Systems Sector by Iranian government-affiliated cyber actors in late 2023, are clear examples of the opportunistic approach that nation-state adversaries like Iran will continue to leverage and are a stark reminder of the need to continue to monitor and to harden U.S. critical infrastructure.

Critical infrastructure security is a shared responsibility and a national imperative. While most critical infrastructure is owned by the private sector, government at all levels can and must play a role in protecting it, especially when it comes to defending against nation-state actors.

To address this, EEI's member companies and the electric power sector take a "defense-in-depth" approach with several layers of security strategies designed to eliminate single points of failure. There are three main components to our defense-in-depth approach:

1. Mandatory and enforceable reliability, physical security, and cybersecurity regulations;
2. Partnerships among industry and government; and
3. Efforts to enhance our resilience to all hazards.

All Hazards Security: Defense-in-Depth

Cyber and physical security threats will continue to evolve, which is why the electric power sector focuses on enhancing visibility into critical control systems, improving situational awareness and information sharing for emerging threats, and ensuring we have comprehensive plans in place to respond and recover quickly when incidents occur.

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, the Department of Energy's (DOE's) Cybersecurity Capability Maturity Model (C2M2), and, most recently, DOE's Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources (DER) that are being developed in partnership with state regulatory bodies through the National Association of Regulatory Utility Commissioners (NARUC).

In addition to complying with standards, the sector strongly believes in advancing a culture of security. Thanks to leadership from the chief executives of all U.S. investor-owned electric companies, EEI developed a "Culture of Security" initiative that has provided tools to improve security culture for individual electric companies and a venue for sharing practices across the industry.[1]

Self-assessments are now conducted by companies annually. In addition to demonstrating that security is a priority for the "C-suite," these yearly exercises provide a venue for security teams and leaders across business units to address corporate security culture and to better align efforts.

When it comes to securing specific systems like operational technology for power delivery, much of the expertise is in the sector. To leverage this expertise, electric companies are now piloting a peer review program to have security professionals from electric companies review their peers, identify opportunities for improvement, and socialize best practices.

The commitment from industry operators to participate in these programs highlights both the shared responsibility felt across the sector and the desire to learn from each other. While culture alone does not improve security posture, it is the foundation on which new efforts are built and ensures that today's imperatives remain tomorrow's priorities.

Through these standards and voluntary regimes, the bulk power system and other critical grid components benefit from a baseline level of security. While these standards are important,

[1]Scott Aaronson, Edison Electric Institute, Protecting the energy grid is a team sport (October 2021), https://www.securitymagazine.com/articles/96231-protecting-the-energy-grid-is-a-team-sport.

regulations alone are insufficient given the dynamic threat environment, and they must be supplemented by industry-government partnerships and coordinated response and recovery efforts.

Partnerships. As threats evolve, the value of industry-government partnership and the need to remain vigilant cannot be overstated. The electric power sector has worked with government partners to develop and deploy sophisticated threat monitoring tools and to create an environment where threat intelligence is shared in near real-time and where operational collaboration among asset owners and government operators is the norm. This gets information into the hands of system operators quickly to better protect and defend their critical systems against rapidly evolving threats. While the sector values current coordination efforts, there is opportunity to continue to enhance timely and actionable information sharing through partnerships like the Electricity Subsector Coordinating Council (ESCC), the Cybersecurity Risk Information Sharing Program (CRISP), and the Energy Threat Analysis Center (ETAC).

Through partnerships like the ESCC, government and industry leverage one another's strengths. 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, unity of guidance, and unity of message among participating organizations.

This partnership manifests itself in many ways, including deployment of government technologies, multi-directional information sharing, drills and exercises, and facilitating cross-sector coordination. The ESCC has been seen as a model across critical infrastructure sectors due to its CEO-level engagement and prioritization of security and preparedness for all hazards. This unity of effort driven by industry working with government has produced significant, tangible results. The sector continues to deploy CRISP, an industry-government 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 have proven extremely valuable to identifying and addressing cybersecurity risks.[2]

The sector also leverages DOE's ETAC, another public-private partnership that benefits from the tools and insights energy infrastructure owners and operators have deployed on their systems, coupled with DOE's National Laboratories and the intelligence community that come together to exchange data, identify risks, and develop mitigation strategies to protect energy systems from adversaries like Volt Typhoon, among others. I would like to thank Chairman Manchin and Ranking Member Risch for their leadership on the *ETAC Establishment Act* and encourage the

[2] Sonal Patel, POWER, DOE Lays Out How Power Sector Could Win the Cybersecurity Battle (May 2018), https://www.powermag.com/doe-lays-out-how-power-sector-could-win-the-cybersecurity-battle/.

Committee to consider this legislation as a way to build on the progress of the ETAC pilot program.

Response and Recovery. The electric power sector is proud of its record on reliability, but outages and incidents do occur. When these happen, many key investments help companies restore power safely and as quickly as possible. EEI's member companies invest more than $150 billion each year to make the energy grid stronger, smarter, cleaner, more dynamic, and more secure. The industry's culture of mutual assistance deploys a world-class workforce amidst the toughest conditions to restore power for customers safely and efficiently.

More recently, we have also 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 190 entities, including investor-owned electric and natural gas companies, electric cooperatives, public power utilities, Canadian electric companies, and Regional Transmission Organizations/Independent System Operators (RTOs/ISOs), are participating in the program. EEI manages these efforts and has determined that 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.

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. Most recently, GridEx VII included more than 15,000 participants from approximately 250 North American organizations, including the electric industry, cross-sector partners from natural gas and telecommunications, and U.S. and Canadian government partners.[3] The two-day exercise tested operational and policy measures that would be needed to restore the energy grid following a severe cyber and physical security attack. 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.

Critical Infrastructure Interdependencies

The electric power sector is proud of the work we do to build "defense-in-depth" across our industry, but we understand that alone is not enough. We also must work with government and cross-sector industry partners to build that same "defense-in-depth" across the nation to reduce systemic risk and to ensure all are prepared for, and can respond to, national-level incidents. The federal government can support industry in reducing systemic risk associated with critical infrastructure interdependencies by:

1. Coordinating with industry on the revision of Presidential Policy Directive 21 (PPD-21);
2. Considering interdependencies in the revision of the National Cyber Incident Response Plan (NCIRP);
3. Evaluating critical infrastructure supply chain interdependencies; and

[3] North American Electric Reliability Corporation, GridEx VII Report Highlights Further Action to Enhance Grid Resilience (April 2024), https://www.nerc.com/news/Headlines%20DL/GridEx%20VII%20Lessons%20Learned%20Report.pdf.

4. Prioritizing and resourcing the most critical of U.S. critical infrastructure, including such regimes as Defense Critical Electric Infrastructure (DCEI) and Systemically Important Entities (SIE) as established by the Cyberspace Solarium Commission.

PPD-21 on Critical Infrastructure Security and Resilience. This policy directive identifies the energy sector as uniquely critical due to the enabling functions it provides across all critical infrastructure sectors. PPD-21 also delineates roles and responsibilities to specific federal agencies known as Sector Risk Management Agencies (SRMAs). SRMAs are meant to serve as a day-to-day federal interface for prioritizing, collaborating, and coordinating sector-specific activities including cyber incident response.

The productive relationship between the power sector and DOE as its SRMA often serves as an example for other sectors, especially through its ESCC leadership model. As the Administration pursues plans to revise this decade-old policy document, we welcome the opportunity for industry engagement to elaborate on the best practices learned through collaboration with our SRMA.

In the context of today's hearing, there are three SRMAs to consider—DOE as the SRMA for the Energy Sector, the Environmental Protection Agency (EPA) as the SRMA for the Water Sector, and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) as the SRMA for the Dams Sector. Clarifying federal roles and responsibilities through the PPD-21 revision will help coordination across sectors like the energy, water, and dams sectors.

NCIRP. Both water and dams are integral to the operation of the electric system, and government and industry across each sector should be in lock step to ensure timely and effective cyber incident response. Hydropower provides about 40 percent of the "black start" resources necessary to restore power in the event of grid failure.[4] In addition, dams are a key piece of the operations and deployment of renewables across the U.S. grid, particularly in the West.[5] Accordingly, we also encourage CISA to consider these interdependencies as it revises the NCIRP this year.

Supply Chain Interdependencies. The integrity of the information and communications technology (ICT) supply chain is important to the operation and reliability of critical infrastructure. A compromise of this integrity can result in the delivery of a product with malicious functionality. Similar to other risks, the ICT supply chain risk cannot be fully mitigated, but it can be managed.

This risk cuts across all sectors, but also across functional and organizational boundaries within a given entity, touching multiple activities throughout the procurement cycle. While much of the responsibility for ICT supply chain integrity falls on the cyber asset manufacturers, the end-users bear much of the risk.

---

[4] Jose R. Garcia, et al., Oak Ridge National Laboratory, Hydropower Plants as Blackstart Resources (May 2019), https://www.energy.gov/eere/water/articles/hydropower-plants-black-start-resources.

[5] Abhishek Somani, et al., Pacific Northwest National Laboratory, Hydropower's Contributions to Grid Resilience (Oct. 2021), https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-30554.pdf.

Support from government to help protect the supply chain, testing of components, and better collaboration across the critical sectors in concert with manufacturers are all important opportunities for managing the ICT supply chain risk.

CISA's National Risk Management Center conducts critical infrastructure risk interdependence analyses, including dam failure simulation modeling and cross-sector risks for the electric power sector. Through this effort, CISA may consider analyzing supply chain interdependencies that could lead to cascading risk across multiple sectors. As critical infrastructure owners and operators work to root out potential risk associated with reliance on foreign components, we look to SRMAs like CISA, DOE, EPA, and other federal partners to help address this shared national security responsibility. We must prioritize investments in key supply chains *now* to build out the infrastructure necessary to support the increased demand for electricity needed to leverage technologies key to U.S. competitiveness and national security.

Risk Management. Finally, we encourage our federal partners to continue to work with cross-sector owners and operators to prioritize critical infrastructure risk mitigation—because if everything is critical then nothing is. Instead of trying to achieve the impossible task of protecting every asset from every threat, the electric sector sets priorities to protect the most critical energy grid components against likely threats; to build redundancy into the system to make it more resilient; to coordinate preparation and response efforts with the government; and to develop contingency plans for response and recovery if grid operations are impacted.

DOE has included $2.5 million for DCEI in its Fiscal Year 2025 Congressional Justification, and CISA has similarly prioritized efforts to designate and support SIEs. As each of these efforts, and others, may progress, we urge our federal partners to harmonize efforts and to streamline initiatives to ensure practical application across interdependent critical infrastructure sectors.

Opportunities and Challenges with Artificial Intelligence (AI)

The energy grid is becoming increasingly dynamic and complex. As EEI's member companies work to build and secure the grid of the future, technological applications like AI offer great potential for American economic competitiveness and innovation, while also creating new challenges.

AI systems have the potential to bring many benefits to society, including enabling electric companies to better analyze and use vast amounts of data and to operate an increasingly complex grid that includes more distributed resources. In the years ahead, the need to significantly expand the capacity of the transmission system will necessitate greater coordination across a wide range of stakeholders.[6] The increased usage of AI will rely on an expanded network of data centers and data centers rely on large amounts of electricity. As mentioned, we must prioritize investments in

[6] *See* DOE, National Transmission Needs Study (Oct. 2023) (finding that significant intra-regional and interregional transmission capacity expansion will be needed to address a range of issues, including increased electricity demand, the need to interconnection new clean resources, alleviate system congestion, and improving reliability and resilience), https://www.energy.gov/sites/default/files/2023-12/National%20Transmission%20Needs%20Study%20-%20Final_2023.12.1.pdf.

critical electric infrastructure supply chains *now* to build out the infrastructure needed to support the increased use of AI across the U.S.

In addition, for the opportunities of AI to be fully realized, it must be developed, deployed, and operated in a secure and responsible way. Security must be a core requirement, not just in the development phase, but throughout the life cycle of the AI systems in the energy sector and across all infrastructure sectors that will support these technological advancements.

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 both public and private partners across all sectors to address all hazards. We appreciate the bipartisan support that grid security legislation historically has enjoyed in Congress and the work you have done to enhance the energy sector's security posture. We look forward to working together to continue to build critical infrastructure security and resilience for the safety, security, and well-being of all Americans.