STATEMENT OF SCOTT I. AARONSON
SENIOR VICE PRESIDENT, ENERGY SECURITY & INDUSTRY OPERATIONS
EDISON ELECTRIC INSTITUTE

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

"Protecting America's Energy Infrastructure in Today's Cyber and Physical Threat Landscape"

JANUARY 13, 2026

Introduction

Chairman Latta, Ranking Member Castor, and members of the Subcommittee, thank you for the opportunity to testify. My name is Scott Aaronson, and I am Senior Vice President for Energy Security & Industry Operations at the Edison Electric Institute (EEI). EEI is the association that represents all U.S. investor-owned electric companies. EEI's member companies provide electricity for nearly 250 million Americans and operate in all 50 states and the District of Columbia. The electric power industry supports more than seven million jobs in communities across the United States. EEI's member companies invested more than $200 billion in 2025 to make the energy grid stronger, smarter, more dynamic, more flexible, and more secure against all hazards, including cyber threats. I appreciate your invitation to discuss this important topic on their behalf.

We rely on safe, reliable, affordable, and resilient energy to power our daily lives, run our nation's economy, and support national security. Today, demand for electricity is growing at the fastest pace in decades, creating challenges for our nation, as well as opportunities to ensure America is home to the industries, technologies, and jobs of tomorrow. America's investor-owned electric companies are uniquely positioned to meet growing demand and to address evolving risks, while working to keep customer bills as low as possible.

Energy Security is National Security

The electric grid is the cornerstone of modern society, enabling virtually every aspect of daily life. Electric companies invest in the electric grid, supporting resilience and the ability to deliver power in the face of both manmade and natural threats while also keeping costs as low as possible for customers through economies of scale and more than a century of operational experience. The grid is constantly evolving and adding new large loads, including data centers, advanced manufacturing, and other demands that support both U.S. national and economic security; extraordinary growth and scale is something that it can accommodate effectively. These electric companies serve residential and commercial customers, as well as critical infrastructure including military installations, hospitals, water treatment facilities, and first responders. As an

industry that works at the intersection of energy and security, it's never been clearer that energy security is national security.

The electricity subsector is a part of the energy sector that is designated by National Security Memorandum/NSM-22 as one of the 16 critical infrastructure sectors whose assets, systems, and networks are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, economic security, or public health and safety. The reliance of virtually all industries on electric power means that every critical infrastructure sector depends on the energy sector.

The electricity subsector employs a risk-based, defense-in-depth approach to security, including employing a variety of tools and strategies that support existing voluntary and mandatory standards and regulations, both of which are valuable tools in ensuring the security and resilience of critical infrastructure operators.

Throughout the country investor-owned electric companies are meeting and exceeding existing regulatory standards, as the federal government, states, and private sector work together to reduce risk holistically and continue to enhance our security posture.

Threats Facing U.S. Electric Companies

EEI member companies are mindful of the full range of threat actors that have targeted U.S. critical infrastructure, from cyber groups backed by nation-states to homegrown perpetrators of physical attacks.

On the cybersecurity front, U.S. electric companies face the threat of sophisticated cyber-attacks from the governments and militaries of foreign adversaries, as well as a barrage of attacks from less-sophisticated actors—who are increasingly enhancing their capabilities with the use of new and emerging technology to enable attacks, including artificial intelligence (AI). In addition to evolving threats, we also must contend with third party vulnerabilities in our software and in our critical supply chains.

On the physical security front, the U.S. has seen an uptick in physical attacks against energy infrastructure in recent years—as reported by law enforcement agencies. And emerging technology like low-cost, long-range drones poses new forms of scalable threats to energy infrastructure—as demonstrated by the recent attacks on Ukraine's power grid. These threats represent risks not only to the grid, but to the customers and communities that EEI member companies serve.

Defending Critical Infrastructure

Our industry's collaborative national security lines of effort are rooted in 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. Adherence to mandatory and enforceable reliability, physical, and cybersecurity regulatory standards;
2. Partnerships among industry and government that support proactive defense and sharing of evolving threat information; and,
3. Resilience to incidents, including preparations and exercises, as well as spare equipment sharing and mutual assistance programs to support recovery from all hazards.

Collaboration Between Government and Private Sector

EEI members have a fundamental responsibility to operate the U.S. electric grid to ensure the reliable flow of electricity that powers the nation. As owners of this responsibility, our members know that their infrastructure is a target for sophisticated adversaries – including nation-state actors. As a result, our members maintain a collaborative partnership with the federal government. This partnership helps maintain awareness of threats and vulnerabilities and appropriate sharing of technical expertise to identify and address active threats.

Information sharing between government and private sector is essential to this partnership. Much of this partnership is enabled by protections afforded to private sector in the Cybersecurity and Information Sharing Act of 2015, which we strongly urge Congress to reauthorize before it expires at the end of this month.

Additionally, we urge for a timely release of the Department of Homeland Security's Alliance of National Council for Homeland Operational Resilience (ANCHOR) effort, which helps facilitate candid national security discussions.

We'd also encourage congressional action to enable more effective collaboration between the federal government and the energy sector, in response to cyberattacks.

For example, there may be instances where the federal government asks or orders a private sector entity to take, or refrain from taking, certain actions, as part of efforts to address threats to the nation's power grid. For example, the government may order utilities to ensure certain areas have power during an emergency for national security purposes. Or, conversely, an agency may ask that a utility allow a threat to persist to support an investigation.

While utilities stand ready to collaborate with the federal government to address threats and emergency situations, existing law does not provide sufficient legal liability protection for utilities that accommodate such an order. Addressing barriers like these will enable even more effective public-private coordination to defend the grid at critical moments.

Legislation Before the Subcommittee

Strengthening the Energy Threat and Analysis Center (ETAC)

Given the value the Energy Threat and Analysis Center (ETAC) has provided to the energy sector, and the nation, EEI, on behalf of its members, strongly supports Congressional action to provide additional authorization and authorities to the ETAC. We appreciate the focus on explicitly codifying the ETAC's mission to bring government and the energy sector together; and on providing the ETAC with the legal tools needed to facilitate candid discussion of extremely sensitive security and operational topics. The ETAC has repeatedly proven its value for the energy sector, the government, and the nation's critical infrastructure community.

A founding principle of the ETAC is that, while its work is conducted by a volunteer coalition of the willing drawn from across the energy sector, the insights, warnings, and mitigations it

develops are made available to the entire sector to help raise awareness of potential threats, and make concrete defensive measures more accessible, for even the least-resourced entities. In the face of two of the most significant cyber threats the U.S. has faced this decade, the ETAC was able to provide actionable guidance that benefitted not just the entities that participate in its activities—but the entire energy sector. The ETAC conducted analysis through its unique collaborative model that provided actions for critical infrastructure owners and operators to take to ensure the continued security and resilience of their real-time systems.

Over the last five years, the ETAC has grown from just four utility partners to seventeen. The ETAC expanded its membership to encompass investor-owned utilities, public power utilities, electric cooperatives, and oil and gas entities. Our companies have dedicated ETAC analysts who sit alongside government experts at the National Laboratory of the Rockies (NLR), and work with them in both classified and unclassified settings, to produce the ETAC's unique products.

Given the value the ETAC has provided to the energy sector, and the nation—and its continued growth and maturation— EEI, on behalf of its members, strongly supports Congressional action to provide additional authorization and authorities to the ETAC. We appreciate the focus on explicitly codifying the ETAC's mission to bring government and the energy sector together; and on providing the ETAC with the legal tools needed to facilitate candid discussion of extremely sensitive security and operational topics.

Strengthening the Leadership of Federal Energy Security Partners

EEI and its members benefit daily from our close relationship with our government partners at DOE's Office of Cybersecurity, Energy Security and Emergency Response (CESER), which, as our Sector Risk Management Agency (SRMA), serves as our primary government partner on energy security issues. CESER supports critical infrastructure on the threats of today and leads innovation on cybersecurity at the National Labs to prepare for tomorrow. We appreciate Congress's efforts to strengthen the leadership, capabilities and resources of CESER.

We particularly appreciate the strong bipartisan support for CESER in the energy funding bill that the House passed last week, which we see as a sign of Congressional commitment to ensure that we have empowered partners in government who can help us identify, mitigate, and defend against cyber and physical threats, as well as natural hazards.

Strengthening the State-Level Focus on Energy Security

We appreciate Congress's continued support of the states' role in energy security. It is more important than ever that our state government partners are empowered to understand the implications of the real and significant threats that our members face and encouraged to proactively engage with the critical infrastructure owners and operators defending against them on a daily basis.

Strengthening the Cybersecurity of our Energy Partners: Rural/Municipal Utilities, & Pipelines

While a number of bills before the Subcommittee today do not directly address EEI member companies, cybersecurity- like energy security - is a team sport. We are supportive of Congressional action to support rural electric cooperatives and municipal utilities and pipeline operators. Many of the programs and exercises in the energy sector include our partners outside of the IOU community, as we all are working toward the same goal – the reliability, security, and affordability of the U.S. energy grid. Advancing the capabilities and defenses of any grid operator raises the collective capabilities and defenses of the entire grid.

Conclusion

The threats to our energy system will only continue to grow and evolve. But, as I hope I have conveyed, EEI members are working tirelessly to defend the grid against cyber and physical attacks of all forms.

This effort has benefitted significantly from the numerous close partnerships we've been able to develop across the U.S. federal government—and I urge this Subcommittee and the Congress to continue your robust support to strengthen our defenses and keep the power flowing to all Americans.