TESTIMONY OF SHARLA B. ARTZ
SECURITY AND RESILIENCE POLICY, AREA VICE PRESIDENT
XCEL ENERGY

BEFORE THE HOUSE ENERGY AND COMMERCE COMMITTEE
SUBCOMMITTEE ON ENERGY

HEARING TITLED "SECURING AMERICA'S ENERGY INFRASTRUCTURE: ADDRESSING CYBER AND PHYSICAL THREATS TO THE GRID"

DECEMBER 2, 2025

Introduction

Chairman Latta, Ranking Member Castor, and members of the Subcommittee, thank you for the invitation to testify on this important topic. My name is Sharla Artz, and I am the Security and Resilience Policy Area Vice President for Xcel Energy. Xcel Energy is a large investor-owned utility operating in eight western and midwestern states, serving 3.9 million electric customers and 2.2 million natural gas customers. Xcel Energy is a member of certain national trade associations, including the Edison Electric Institute (EEI), which represents all U.S. investor-owned electric companies. EEI's members provide electricity for nearly 250 million Americans and operate in all 50 states and the District of Columbia. My testimony today is on behalf of both Xcel Energy and EEI more broadly. For Xcel Energy and EEI's member companies, securing the energy grid from all hazards, including cyber threats, is a top priority.

The energy grid is critical to America's national security and economic competitiveness. With electricity demand growing dramatically to support critical technologies like artificial intelligence and the proliferation of data centers that fuel our digital lives, electricity is more essential than ever to our nation's energy dominance. Ensuring a secure, reliable, and resilient energy grid is a responsibility Xcel Energy and the electric power sector take extremely seriously.

As the grid continues to modernize, so too do the threat actors who seek to undermine U.S. critical infrastructure. For years, the U.S. intelligence community[1] has warned of the potential for malicious nation-state exploitation of U.S. critical infrastructure. Today, we know from our federal partners that Chinese state-sponsored cyber actors known as Volt Typhoon have compromised multiple U.S. critical infrastructure providers with the intent of disrupting

[1] 2025 Annual Threat Assessment of the U.S. Intelligence Community

operational controls. With the increasingly complex geopolitical threat landscape, sophistication of ransomware operations by transnational organized criminals, and the use of artificial intelligence (AI) to conduct cyber attacks[2], we have seen an uptick in threats to critical infrastructure organizations across all sectors. The threat is real, it is advanced and it is persistent. Thus, Xcel Energy and our industry partners work constantly to mitigate these threats and provide resilient power to our communities and those we serve.

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. Because of this shared responsibility, investor-owned utilities work collaboratively with our federal, state and local partners, with each other, with rural cooperatives, public power and with other critical infrastructure sectors to achieve this vital national security mission.

Our 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 regulations;
2. Partnerships among industry and government for proactive defense; and
3. Preparing for and exercising recovery plans against all hazards.

Resilience for National Security

Private sector critical infrastructure asset owners and operators are on the front lines of defending our nation's essential services from rapidly evolving threat actors on a daily basis. The attacks by Russia against Ukraine's power system solidified the importance of creatively, constructively and collaboratively addressing threats to critical infrastructure. For this reason, the energy sector has

[2] AI firm claims Chinese spies used its tech to automate cyber attacks

been actively implementing security risk mitigation programs and engaged with our government partners to develop tools, technologies and processes that enhance visibility into critical control systems, improve situational awareness and information sharing for emerging threats, and make sure we have comprehensive plans in place to respond and recover quickly when incidents occur.

Security 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. The standards cover key components of effective risk management including supply chain risk management and physical security. For over 15 years, 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. That process ensures utility owner and operator expertise from across the stakeholder community informs the security controls that most effectively reduce prioritized risks.

In addition to NERC CIP, companies like Xcel Energy are subject to the TSA Security Directives. First issued in 2021, industry and TSA have worked together to enhance the existing security controls implemented to secure natural gas infrastructure systems. Since their issuance, the collaboration between TSA and industry has resulted in requirements that allow asset owners and operators to tackle priority risks with controls that achieve the desired outcomes.

The industry also uses voluntary standards and maturity frameworks to improve the security of their systems. Examples include the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Department of Energy's (DOE's) Cybersecurity Capability Maturity Model (C2M2) and the 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). The frameworks and guidance provided in these efforts allow utilities of all shapes and sizes to assess their current maturity, identify areas for improvement, and benchmark against existing known best practices.

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.[3]

Self-assessments are now conducted by companies annually. In addition to demonstrating that security is a priority for our executives, this yearly exercise provides 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, the Culture of Security initiative now includes peer reviews. The peer reviews cover topics ranging from physical security processes, training of personnel, and cybersecurity architectures. Participating electric companies invite security professionals from other electric companies to review their peers, identify opportunities for improvement, and socialize best practices. The process is extensive, builds strong relationships across industries, and identifies security-enhancing opportunities that can be shared more broadly across the industry.

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.

[3]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.

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, given the dynamic threat environment regulations alone are insufficient and 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. We appreciate the continued partnership of our Sector Risk Management Agency, the Department of Energy, as they have the sector-specific expertise and relationships to understand our risks and mitigation strategies.

The electric power sector has worked with DOE and other 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. Understanding the adversaries' tactics, techniques, procedures and motivations also helps asset owners plan their infrastructure with security and resilience to these threats in mind. While the sector values current coordination efforts through partnerships like the Energy Threat Analysis Center, the Cybersecurity Risk Information Sharing Program (CRISP), and the Electricity Subsector Coordinating Council (ESCC), there is opportunity to continue to enhance these partnerships.

Industry and government have long understood the importance of actionable intelligence tailored to address sector specific threats and impacts. The Energy Threat Analysis Center, or "ETAC," was created to address this need. First piloted in 2023 and now consisting of 17 private sector entities including Xcel Energy, ETAC is an operational collaborative that convenes experts from the DOE and the U.S. energy sector to identify, analyze, and mitigate cyber threats to America's critical energy infrastructure. The ETAC integrates industry data and context with government

intelligence to reduce risk to the energy sector writ large. Housed at the National Renewable Energy Laboratory (NREL) in Colorado and including representatives from multiple national labs, ETAC analysts from public power utilities, rural cooperatives, investor owned utilities, and oil and natural gas entities are able to review threat intelligence in real time, assess impact to the energy sector and develop risk mitigations that are shared via the Electricity Information Sharing and Analysis Center (E-ISAC) and the Downstream Natural Gas Information Sharing and Analysis Center (DNG ISAC) to energy providers across the country. In addition to DOE, ETAC facilitates industry collaboration with other federal partners, including DHS, the military and federal security and law enforcement agencies expanding cross agency information sharing with the private sector.

As an example of the positive impact ETAC has made, after the public disclosure of PRC-linked Salt Typhoon's compromise of major U.S. telecommunications providers in late 2024, ETAC issued four threat memos (March-August 2025) that took government information, injected private sector data and provided specific, actionable best practices to mitigate the identified threat. These products garnered 1000+ views on the E-ISAC portal demonstrating strong industry interest and utilization.

In addition to ETAC, Xcel Energy and our industry utilize other government partnerships to enhance system security. For example, private sector owners and operators participate in the DHS's Joint Cyber Defense Collaborative (JCDC), TSA's Surface Information Sharing Cell (SISC's) industry briefings, the NSA's Cybersecurity Collaboration Center and the FBI's Cybersecurity Action Team. Xcel Energy actively engages our state partners as well, participating in the Minnesota Fusion Center, the Texas Fusion Center and holding a permanent seat at the Colorado Information Analysis Center. Our Threat Intelligence team uses these partnerships to further our understanding and our partners' understanding of the threat and corresponding operational risk.

Identifying threats encompasses more than people to people interaction but also involves the deployment of technology that rapidly detects threats. A prime example of an effort that brings the expertise of national labs, the voluntary efforts of industry, the reach of the E-ISAC, and the intelligence apparatus of government is the Cyber Risk Intelligence Sharing Program, or "CRISP." The CRISP program includes DOE, the Pacific Northwest National Laboratories, and the E-ISAC, which manages the program. Participants in the program deploy unique sensors on their networks and share that data with intelligence analysts. The sensors monitor network traffic, send the data to the national lab for analysis for potential adversarial activity. Participants are then alerted to potential threats so that they can take action to protect their systems. More than 90 percent of U.S. electric customers are served by a company that has deployed CRISP sensors. The information gleaned from the sensors and the associated analysis has proven extremely valuable to identifying and addressing cybersecurity risks.

In addition to the information sharing initiatives described above, industry and government are strategically assessing threats to energy infrastructure at the executive level. The Electricity Subsector Coordinating Council or "ESCC," consists of electric company CEOs and trade association leaders who represent all segments of the electric sector, and serves as the primary interface between government leaders and the private sector to address national security priorities, leveraging the strengths government and industry each provide. Together, the ESCC executives and government partners proactively prepare for, and respond to, national-level incidents or threats to critical infrastructure.

A key characteristic of the ESCC is executive engagement. Our CEOs and Senior Officials from the federal government sit at the same table and work through the key risks that impact our sector. 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 participating organizations. The concerted collaboration creates efficiencies needed for effective and rapid threat remediation efforts. 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.

Preparedness, Response and Recovery

Preparing for incidents is a regular component of our security and resilience practices and exercises help us improve the effectiveness of our individual and collective response to various incidents. 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. The first GridEx was conducted in 2011 at the direction of NERC and industry and has grown every time it has occurred. Most recently, GridEx VIII saw increased participation and included thousands of participants from across the U.S. and Canada. At Xcel Energy, our two days of distributed play included over 316 participants, including 64 participants from external partnering organizations, such as state emergency managers and homeland security advisors.

At the end of distributed play, the E-ISAC brings together ESCC CEOs, Canadian Cybersecurity officials, cross sector participants and leaders from the U.S. government to review the coordination and communication processes between industry and government in responding to a hypothetical coordinated attack by a nation state. These discussions help us identify needed improvements to facilitate resilience during a time of crisis.

While GridEx is one of the largest exercises, industry participates in many additional exercises across the state and federal level to enhance our shared understanding of processes, priorities and opportunities for improvement. In Wisconsin, for example, the Wisconsin National Guard, the state emergency operations center and utilities exercise regularly. Similarly, in Colorado, utilities in the state exercised with NORAD and Northern Command to enhance response capability mutual understanding. In Virginia, the 91st Cyber Brigade recently hosted Cyber Fortress 2025, a joint, interagency, intergovernmental, multinational exercise focused on electric utilities. The 2-week exercise allowed federal, state, and local entities to coordinate directly with electric industry leaders and plan for future collective response and resiliency activities. The Department of Energy also hosts regionally-based exercises focused on response to natural and man-made

threats, such as Liberty Eclipse and Clear Path. Next year, the American Gas Association will host the biennial Natural Gas Exercise, an exercise in which operators test and validate response/recovery plans for cybersecurity and physical security threats that stress gas control and corporate business continuity. These drills sharpen not just the unity of effort between energy industry 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.

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 members are forecast to spend more than $200 billion this year — and more than $1.1 trillion over the next five years — to make the energy grid stronger, smarter, 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.

More recently, we have 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 natural gas and power companies, cooperatives, municipalities, Canadian power 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.

How Government Can Help

Government should continue to fund information sharing collaboration initiatives, like ETAC, so they can build upon the strong foundation established in this unique environment. Expanding programs like CRISP enhances industry and government understanding of the threat landscape and thus needs additional government funding to accomplish that expansion.

Congress should authorize ETAC so that this unique public private partnership can adapt and grow to address evolving threats. Explicit recognition of this program allows industry partners and DOE to shape the joint effort to address the evolving risk landscape and to incorporate needed partners in the work effort.

Continued support and recognition of the importance of Sector Risk Management Agencies for sector risk reduction efforts is essential to critical infrastructure protection. The energy system expertise contained within DOE and the national lab complex assures that risk assessment is informed by system operational understanding. Supporting DOE leading government engagement with industry is most efficient and effective while minimizing duplication or conflicting initiatives.

It is equally critical to recognize that certain information about the energy grid—such as detailed operational data and security protocols—must be protected from public disclosure. The release of such sensitive information could inadvertently aid malicious actors and undermine the security of our infrastructure. Although some state-level initiatives seek to increase public access to grid information, we continue to urge policymakers and regulators to carefully balance transparency with the imperative to safeguard details that, if disclosed, could pose risks to national security and public safety. Protecting this information is essential to maintaining the resilience and reliability of the grid in the face of evolving threats.

Conclusion

Thank you again for holding this hearing. As evidenced in my testimony, the industry's commitment to security and our willingness to work with both public and private partners across all sectors to address all hazards is a constant effort. 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.