Testimony of Adrienne Lotto

Senior Vice President of Grid Security, Technical & Operations Services

American Public Power Association

Before the House Energy & Commerce Committee

Subcommittee on Energy

Hearing on

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

January 13, 2026

Chairman Guthrie, Ranking Member Pallone, Subcommittee Chairman Latta, and Subcommittee Ranking Member Castor, and members of the committee, thank you for inviting me to share my perspectives on the legislation being considered today. Public power utilities know that a reliable energy grid is the lifeblood of the nation's economic and national security, as well as vital to the health and safety of all Americans and take very seriously their responsibility to maintain a secure and reliable electric grid.

My name is Adrienne Lotto. I am the senior vice president of grid security, technical and operations services at the American Public Power Association (APPA). APPA is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. APPA represents public power before the federal government to protect the interests of the more than 55 million people that public power utilities serve in 49 states and five territories, and the 100,000 people they employ. Public power utilities account for 15 percent of all sales of electric energy (kilowatt-hours) to end-use consumers and are load-serving entities with the primary goal of providing the communities they serve with safe and reliable electric service at the lowest reasonable cost.

By way of personal background, my career has focused on addressing cross-sectional issues associated with cybersecurity, public policy, risk management, law, and the environment. I have a Juris Doctor from Pace University School of Law and a Bachelor of Science from the State University of New York at Albany. Prior to joining APPA in 2022, I was vice president, chief risk, and resilience officer at the New York Power Authority, and before that I served as acting principal deputy assistant secretary for the Department of Energy's (DOE) Office of Cybersecurity, Energy Security and Emergency Response (CESER). I am also currently the chair of the external advisory board for the Advanced Research for Integrated Energy Systems (ARIES) program at the National Laboratory of the Rockies.

The key pillars of cyber and physical security (collectively known as "grid security") are:

1) mandatory and enforceable standards;

2) information sharing and public-private partnerships; and

3) "defense-in-depth" and sector-wide preparation exercises.

To effectuate this, APPA strongly supports:

1) Reauthorization of the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program (RMUC);

2) The release of the Critical Infrastructure Partnership Advisory Council (CIPAC) replacement, by Department Homeland Security (DHS) known as Alliance of National Councils for Homeland Operational Resilience (ANCHOR); and

3) Regulatory harmonization.

Mandatory and Enforceable Standards

Congress approved the mandatory and enforceable standards regulatory regime for the bulk power system in the Energy Policy Act of 2005 (EPAct05) (section 215 of the Federal Power Act (FPA)). Under section

215, the North American Electric Reliability Corporation (NERC), working with electric industry experts, regional entities, and government representatives, regularly drafts reliability, physical security, and cybersecurity standards that apply across the North American grid, including Canada. Participation by industry experts and compliance personnel in the NERC critical infrastructure protection (CIP) standards development process ensures that the standards are technically sound, fair, and balanced. The Federal Energy Regulatory Commission (FERC) has the power to approve or remand those standards as they apply in the United States. To ensure compliance, under FERC's oversight, NERC and its regional entities conduct rigorous audits and can levy substantial fines for non-compliance. Additionally, FERC can instruct NERC to develop new or revised reliability standards with a short turnaround time. CIP standards establish an important baseline of security—but they are a floor, not a ceiling—and grid security is and should be much more than a compliance exercise.

The electric sector is unique in that it is cyber incident reporting mandates to DOE via an Electric Emergency Incident and Disturbance Report (DOE-417) and NERC/FERC. This broad mandate requires an electric utility to report any cyber event that causes or could potentially cause interruptions of grid operations as well as any attempt to compromise a critical system.

Another layer of mandatory cyber incident sharing requirements will be added through Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). Signed into law in March 2022, CIRCIA will require covered critical infrastructure entities to report cyber incidents within 72 hours and ransomware payments within 24 hours to DHS Cybersecurity and Infrastructure Security Agency (CISA). In March 2024, CISA released a notice of proposed rulemaking (NOPR) to begin implementing CIRCIA and is poised to promulgate finalized regulations this year. APPA is concerned that the NOPR is overbroad with respect to reporting requirements for small, distribution-only electric utilities. While reporting obligations are appropriate for large utilities that serve millions of customers, it is unnecessary and burdensome to impose the same obligation on hundreds of community-owned electric utilities that serve fewer than

2,000 customers each and pose a negligible risk to the reliability of the broader grid. APPA is also concerned that CISA has not finalized plans and agreements to avoid duplicative reporting requirements. Prior to issuing a final rule, APPA believes that CISA should complete its consultations with DOE and FERC and enter an information sharing agreement with them. Finally, the Cyber Incident Sharing Act of 2015 (CISA 2015) set up policies and procedures for voluntary sharing of cybersecurity threat information between and among the federal government and private entities (the definition of which includes public power utilities) and provides limited liability protection for these activities. CISA 2015 expired on September 30, 2025; it was temporarily reauthorized as part of a larger appropriations bill through January 30, 2026. APPA urges Congress to approve a long-term reauthorization of CISA 2015 to ensure that the legal structure for information sharing remains in place.

Information Sharing and Public Private Partnerships

The electric power industry works closely with the federal government, including NERC, FERC, DOE, and DHS, on matters of critical infrastructure protection. One important venue for this collaboration is the Electricity Subsector Coordinating Council (ESCC). The ESCC 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. APPA and public power utilities play a leadership role in the ESCC, which includes utility CEOs and trade association leaders.. Their counterparts include senior administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations. It must be noted that the absence of CIPAC protections without any replacement hinders the ability of industry to engage fully with federal government partners. Industry was apprised by DHS that the administration's proposed CIPAC replacement, known as ANCHOR, is ready for publication in the *Federal Register*; public power encourages the administration to finalize it quickly.

Moreover, industry not only works with the ESCC but there is also robust electric utility industry

participation in information sharing organizations known as the Electricity Information Sharing and Analysis Center (E-ISAC) and the Multi-State Information Sharing and Analysis Center. 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 Laboratory, 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 and send the data to the national lab for analysis of potential adversarial activity. Participants are then alerted to potential threats so they can act to protect their systems. The information gleaned from the sensors and the associated analysis has proven extremely valuable to identifying and addressing cybersecurity risks.

Defense In Depth and Sector Wide Preparedness

The goal of every utility and the entire industry is to manage risks prudently. Still, there are tens of thousands of diverse facilities throughout the U.S. and Canada that cannot be protected 100 percent of the time from all threats, requiring utilities to prioritize facilities and assets that, if damaged, would have the most severe impacts on their ability to keep the power on. As such, the electric power industry employes threat mitigation known as "defense-in-depth" that focuses on preparation, prevention, response, and recovery to "all hazard" threats to electric grid operations. Electric utilities plan and regularly exercise for a variety of emergency situations that could impact their ability to provide electricity. One of the biggest exercises, GridEx, takes place every two years. Managed by NERC and the E-ISAC, the most recent one, GridEx VIII, took place in November and involved hundreds of organizations and thousands of participants from industry, government agencies, and partners in Canada.

Building off the success of GridEx, APPA hosted its first ever cyber mutual aid exercise, Safe Haven,

in fall 2025, funded by DOE CESER. The Safe Haven exercise was held in Washington state and Kansas, locations that were selected in coordination with DOE based on several criteria. The scenario featured a cyber event that had a physical impact on the grid.

The electric utility industry has long had in place mutual aid response networks to share employees and resources to restore power after natural disasters and other emergencies. The ESCC uses the concept of traditional mutual assistance networks to develop the Cyber Mutual Assistance Program that can help electric and natural gas companies, public power utilities, and rural electric cooperatives restore critical computer systems following significant cyber incidents. The program now includes 200 entities across all segments of the industry, serving more than 85 percent of all U.S. electric customers.

Rural and Municipal Utility Cybersecurity Act

Enacted in 2021, the Rural and Municipal Advanced Cybersecurity Grant and Technical Assistance (RMUC) Program was authorized and appropriated $250 million in grants and technical assistance over five years to rural, municipal, and small investor-owned electric utilities to enhance their security posture. APPA believes the program is a once in a generation opportunity to improve the cybersecurity of under-resourced, not-for-profit utilities that should be extended and expanded.

Through RMUC, APPA received a four-year, $4 million cooperative agreement to establish the Cyber Pathways Program. This program is designed to support public power utilities with cybersecurity assessments, training, and a new cybersecurity designation program to recognize utilities implementing cybersecurity best practices. Cyber Pathways focuses on resource-limited public power utilities, connecting them with cybersecurity resources, and improving their cyber maturity and incident response capabilities.

The program has realized several successes, such as the completion of a legal framework for utility cybersecurity assessment data, which outlines the specific rights and protections for assessment data to ensure utilities are aware of who has what right to their data; a report on cybersecurity frameworks in use by public power utilities, which was based on a survey of public power utilities to identify experiences in using existing cybersecurity frameworks and assessments to identify the unique needs of smaller, resource-limited utilities who are often poorly served by more complex cybersecurity frameworks; cybersecurity training for dozens of public power utility employees at the Safe Haven exercises; and steady progress developing the Cybersecurity Accelerator Program (CAP) designation program to improve the cybersecurity maturity of public power entities. Going forward, APPA will develop publications and resources for utilities to improve and test their cyber incident response plans; provide additional cybersecurity trainings; and work with members through CAP to improve their cyber posture.

APPA has also been selected for negotiation of a financial assistance award under the DE-FOA-0002986 Advanced Cybersecurity Technology (ACT) Funding Opportunity Announcement. APPA's proposal for Topic Area 3 – Enhancing the Cybersecurity Incident Response Capabilities of the Municipal Utility Workforce, would award $2 million over four years to improve cybersecurity incident response capabilities at 19 utilities that agreed to participate. With this funding, APPA would be able to assess utilities' cybersecurity incident response policies, procedures, and plans and then work with participants to improve and then test these protocols through exercises; develop customized cybersecurity incident response training; and development of a cybersecurity incident response toolkit.

APPA believes there is much more to do to build on the successes achieved thus far in the RMUC program. As such, APPA strongly supports the RMUC Act, which would reauthorize the program through 2030 and authorize $250 million in appropriations.

Energy Threat Analysis Center Act of 2026

Section 40125(c) of the Infrastructure Investment and Jobs Act authorized DOE to develop a program to enhance and periodically test DOE emergency response and coordination capabilities, expand cooperation of DOE with the intelligence community for energy sector-related threat collection and analysis, and extend and enhance industry participation in E-ISAC information sharing. Pursuant to this provision, the Energy Threat Analysis Center (ETAC) was piloted in 2023. Housed at the National Laboratory of the Rockies, ETAC is working to integrate industry data with government intelligence to identify potential threats and develop actionable risk mitigation strategies. As detailed above, information sharing and industry-government collaboration are two key pillars of grid security, and ETAC is a promising example of those foundational pillars.

Energy Emergency Leadership Act

In 2013, Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience (PPD-21) – established a national policy on critical infrastructure security and resilience. PPD-21 tasked DHS with coordinating the overall federal effort to promote the security and resilience of critical infrastructure. However, recognizing existing statutory and regulatory authorities of specific departments and agencies, as well as their unique knowledge and specialized expertise, PPD-21 wisely identified 16 critical infrastructure sectors and designated a Sector Risk Management Agency (SRMA) for each sector to "serve as a day-to-day Federal interface for the dynamic prioritization and coordination of sector-specific activities," among other tasks. DOE is the SRMA for the energy sector; CESER leads DOE's cybersecurity and energy security mission.

The Energy Emergency Leadership Act would expand the list of functions that the Secretary of Energy must assign to assistant secretaries under the DOE Organization Act to include energy emergency and energy security functions, including responsibilities with respect to energy infrastructure, security and resilience, emerging threats, cybersecurity, supply, and emergency planning and preparedness, coordination, response, and restoration. Given the ever-changing cyber and physical threats to energy infrastructure, APPA believes it is reasonable for these essential functions to report to an Assistant Secretary.

Pipeline Cybersecurity Preparedness Act

A reliable and affordable supply of natural gas is critical to ensuring a resilient and reliable power grid. In 2024, natural gas was responsible for 43.7 percent of total U.S. generation.[1] While the electric and natural gas industries have long been intertwined, the relationship has become more critical in recent years as a larger share of electricity is generated using natural gas. The Pipeline Cybersecurity Preparedness Act would require DOE to, in consultation with appropriate federal agencies and stakeholders, establish policies, procedures, and programs to enhance the cyber and physical security of pipelines. Given the growing dependency of electric utilities on secure and reliable pipelines to deliver natural gas fuel, APPA supports the goals of the bill. In a similar vein, please note APPA supports higher standards for delivery, notification, and transparency from the natural gas industry [see APPA Resolution 24-10, "In Support of a Reliable and Affordable Supply of Natural Gas."[2]]

---

[1] https://www.eia.gov/energyexplained/electricity/electricity-in-the-us-generation-capacity-and-sales.php

[2] https://www.publicpower.org/system/files/documents/24-10%20In%20Support%20of%20a%20Reliable%20and%20Affordable%20Supply%20of%20Natural%20Gas%20-%20FINAL.pdf

SECURE Grid Act

States have been required to have State Energy Security Plans (SESP) on file with DOE since the 1990s. Section 40108 of the Infrastructure Investment and Jobs Act revised the list of topics a SESP must address in its plan for the state to be eligible for federal financial assistance. The SECURE Grid Act would reauthorize the program, which expired in October 2025, until 2030 and add requirements for what must go into SESPs, primarily having to do with supply chain security and threats to local distribution utilities. Close coordination among industry and government partners at all levels is imperative to deterring attacks and preparing for emergency situations. Many public power utilities already work with their state governments on SESPs, and APPA is supportive of codifying this work in the SECURE Grid Act.

Conclusion

Thank you again for holding this hearing. As outlined in my testimony, the industry's commitment to security and its 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 in this committee and more broadly 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.