House Energy & Commerce Committee's Subcommittee on Energy January 13, 2026, Hearing on

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

Questions for the Record Submitted to Adrienne Lotto, Senior Vice President of Grid Security, Technical & Operations Services, the American Public Power Association

Submitted March 19, 2026

The Honorable Brett Guthrie (R-KY)

1. DOE is the energy sector authority and must work with other agencies and States. To do this effectively, it must have a culture of constant learning and improvement, which will benefit the whole federal approach to support the energy sector.

a. Would you speak to the importance of a culture of constant learning and constant improvement for the stakeholders you represent?

A culture of constant learning and improvement is critical to APPA's members due to the ever-evolving nature of the energy sector. While large energy infrastructure projects (e.g., power plants, substations, pipelines) are fairly static, the conditions shaping how energy is produced, delivered, and consumed are continually shifting. This includes factors such as the resource mix and composition of energy supply, load growth and demand patterns, grid technology and innovation, market structures and pricing, policy and regulation, and risks and other resilience concerns. The threat landscape, including cybersecurity threats, is also rapidly evolving as technological developments continue to enable the proliferation and refinement of offensive and defensive cyber capabilities.

APPA's public power utility members experience these changes daily in their operations. Learning and improvement are both essential for adapting to these changes in real time, and reliably and affordably keeping the "lights on" for millions of Americans. It is also important that the Department of Energy (DOE) and its state and federal partners continue to keep pace with these changes to ensure alignment with current challenges and risks public power utilities face, as well as the solutions necessary to address them.

2. All the bills included in this hearing reflect measures that would support constant learning and improvement, whether through improved leadership, assistance and sharing, or coordination. How would these be useful to strengthen your work to safeguard and respond to threats?

Improved leadership, assistance, information sharing, and coordination materially strengthens public power utilities' ability to prevent, withstand, and recover from cyber and physical threats. Many of public power utilities face challenges (e.g., resources, staffing, access to intelligence) that make it difficult to keep pace with the threat landscape. In partnership with DOE, APPA provides training, resources, and other support to mitigate some of these challenges.

APPA's strategic priorities for strengthening grid security involve both improving public power utilities' preparedness posture and facilitating response and recovery. We aim to help our members reduce the likelihood of

compromise, as well as the consequences of successful attacks. DOE programs like the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program (RMUC) are contributing directly to these efforts. RMUC supported the creation of a cybersecurity maturity program that allows APPA members to get a baseline of their proficiency in core cybersecurity practices and improve them over time, including using APPA-developed products.

The Honorable Mariannette Miller-Meeks (R-IA)

1. You described RMUC as a 'once in a generation opportunity' for under-resourced utilities. Through APPA's Cyber Pathways Program, you're supporting public power utilities with assessments, training, and a new designation program. Can you share:

a. Concrete examples of how RMUC funding has improved cybersecurity posture at specific public power utilities?

RMUC funding has improved the cybersecurity posture at public power utilities by providing them with training and hands-on exercise experience. In 2025, APPA held two exercises in its Safe Haven exercise series. In conjunction with those exercises, APPA partnered with the Los Alamos National Laboratory to provide a half-day cyber incident response training funded through the RMUC program to 55 exercise participants from 15 utilities. The training and subsequent exercise helped participants improve their utility's ability to respond to a disruptive cyber event.

APPA also used RMUC funding to send public power utility personnel to DOE's state-of-the-art Liberty Eclipse full-scale exercise, where two participants were able to hone their skills in defending real grid infrastructure from simulated cyberattacks in a safe, testing environment. This unique experience provided participants with an opportunity to move beyond theoretical discussions and see the results of their defensive actions in real time, identifying successful strategies and lessons learned that can help them secure their own infrastructure. Liberty Eclipse also included instructional courses from the Idaho National Laboratory and other industry-leading practitioners.

In March 2026, APPA is launching the Cybersecurity Accelerator Program (CAP) that will help public power utilities self-assess and improve their cybersecurity capabilities and program maturity. This RMUC-funded program will be available for free to all of APPA's utility members.

APPA undertook efforts to increase participation in information sharing and incident response programs, such as cyber mutual assistance, with a focus on utilities supporting critical infrastructure. This program allows participating electric utilities to more easily share cybersecurity expertise and resources in the event of a cybersecurity incident, improving utility response capabilities.

b. What percentage of your members have been able to access RMUC resources?

APPA provides RMUC resources to all of its public power utility members through a variety of methods. For example, APPA held regional cybersecurity training events to reach members that typically are unable to travel to obtain such experience. Additionally, APPA is developing trainings, assessments, and resources that can be accessed online or offered virtually to ensure all members can avail themselves of RMUC funded resources.

As stated in my earlier response, APPA's RMUC funding includes a multi-year agreement that involves the creation of cybersecurity programing and resources. Our CAP Program, which will be available for free to all

APPA public power utility members, will help them self-assess and improve their cybersecurity capabilities and program maturity.

APPA is also developing and updating resources to help public power utilities improve their cyber incident response capabilities, including a fundamentals guide for building an effective incident response plan and an OT-specific tabletop scenario to supplement APPA's tabletop in a box resource. These resources will be released later in 2026 and will be available for free to all of APPA's public power utility members. In addition, APPA will be using RMUC funding this year to produce virtual webinars, available free and on demand to members, with cybersecurity instruction targeted at those utilities that have limited travel budgets and that require the ability of their staff to learn at their own pace.

c. How critical is the reauthorization and streamlining of technical assistance for ensuring no public power utility is left behind?

It is critical to continue this work to ensure that all public power utilities have access to resources tailored specifically to them and their unique challenges, especially for small, resource-constrained municipal utilities. In addition to the resources mentioned above, recently released RMUC funding for a new APPA project will support the development of in-house training and toolkits for cybersecurity incident response plans for utilities, which is based on lessons learned from working extensively with a working group in the initial years.

2. Iowa State University is leading CyDERMS, a regional cybersecurity center focused on securing Distributed Energy Resources. As we integrate millions of new devices, we're dramatically expanding the attack surface of our grid. At the same time, we're deploying AI and machine learning tools to detect attacks and manage these distributed systems. This creates a paradox: we're using high-tech AI solutions to secure increasingly complex systems, but that technology itself could be a vulnerability.

a. How do you think about this balance?

This is indeed a paradox and one that we, the entire sector, and federal regulators – including the Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC) are carefully researching and working through. AI technology must be a supplement to – not a replacement for – human oversight and accountability. Moreover, existing cybersecurity fundamentals like defense-in-depth are just as applicable to new technology as they are to existing technology.

b. Are there certain applications where simpler, lower-tech approaches might actually be more secure?

There are instances where simpler, lower-tech approaches may be more secure. Electric utilities and relevant partners and stakeholders will have to assess the risks on a case-by-case basis to determine when a lower-tech solution may be more appropriate. The industry also has mandatory cybersecurity standards developed by NERC and approved by FERC that ensure a baseline protection level for key assets to the nation's electric system.

c. How do we ensure that the AI tools we're deploying to defend the grid don't become the vector for attack?

While there will always be risks associated with digital systems, there are approaches that can drastically reduce the likelihood of AI tools becoming the vector for attack. The first is to ensure utilities and other entities are following fundamental cybersecurity practices. The second is ensuring that AI developers follow secure-by-design

approaches, incorporating security as a key design and development concept, and building critical security controls into the architecture of those AI tools. Both approaches limit potential vulnerabilities associated with the use of AI.

The Honorable Laural Lee (R-FL)

1. As you know, the DOE is the Sector Risk Management Agency (SRMA) for the energy sector, leading efforts to protect critical energy infrastructure.

a. The Energy Emergency Leadership Act reinforces DOE's energy security mission, both against cyber and physical threats. Given this important role, why is it important to assign energy emergency and security responsibilities to an Assistant Secretary at DOE?

Assigning energy emergency and security responsibilities to an assistant secretary is important because it ensures that DOE has a senior, accountable leader with the authority to coordinate at the speed and scale that modern threats require. An assistant secretary provides the peer-level standing needed to convene leaders across government and industry, prioritize resources, and drive unified execution.

2. In your written testimony, you discussed the Cyber Risk Intelligence Sharing Program, or "CRISP," which involves the DOE, Pacific Northwest National Laboratory, and the E-ISAC.

a. Can you elaborate for us on how CRISP works in facilitating information sharing?

CRISP is a mature public-private partnership that enables trusted, timely, and actionable cyber threat information sharing between energy sector owners/operators and the U.S. government. It does this by combining technical data collection, expert analysis, and bidirectional intelligence exchange in a way that individual organizations cannot replicate on their own.

At a high level, CRISP works by turning voluntary, anonymized data into sector-wide situational awareness, and then returning that insight back to participants in an actionable form. Participating organizations install sensors that collect network traffic metadata at or near the internet perimeter, allowing utilities to contribute real-world data without exposing sensitive business details.

b. How has CRISP helped with identifying and mitigating cybersecurity threats?

In addition to the collection and sharing of raw, anonymized data through CRISP, the program includes analysis from Electricity Information Sharing and Analysis Center (E-ISAC) analysts, DOE, and multiple National Laboratories to provide additional context and insights. Analysts seek to identify indicators of compromise and patterns in the data, including emerging threat actor behavior and other trends that can help utilities detect and mitigate IT risks. Analysis can also include specific alerts about unusual or known malicious activity, analysis of threat actor tactics, techniques, and procedures, and recommended mitigations.

c. Why are programs like CRISP important to the municipal utilities that you represent?

CRISP is critical in supporting a sector-wide threat picture that no single utility – regardless of ownership model – would be able to achieve. Programs like CRISP that can collect and process data on a national scale and leverage industry-leading subject matter expertise to provide timely, real-world threat information are essential for securing grid systems against cyber threats. This information helps utilities improve internal detection and response, prioritize defensive approaches and investments, and adjust security operations based on observed threat activity.

3. You also mentioned that the utility industry regularly conducts exercises to prepare for emergency situations, including the Safe Haven exercise, which was supported by DOE's Office of Cybersecurity, Energy Security, and Emergency Response.

a. Can you tell us more about what this exercise involved?

The Safe Haven exercise was APPA's first cyber/physical tabletop exercise. Its purpose was to assess how public power utilities would prepare for, respond to, and recover from a cybersecurity incident that results in physical damage to critical electric infrastructure. The exercise focused on three objectives – internal incident preparation and response, external collaboration and communication, and updating APPA plans and procedures in support of its public power members.

The Safe Haven exercise was conducted at two locations to reflect the diverse range of communities served by our members. The first session was hosted by Kansas Municipal Utilities in McPherson, Kansas, in October 2025 and brought together 46 participants from 20 utilities across Kansas and Oklahoma. The second session was held at Snohomish Public Utility District in Everett, Washington, in November 2025 with 40 participants representing eight utilities from Washington and Oregon.

Together, these sessions provided a valuable opportunity for public power utilities to practice response actions, strengthen partnerships, and enhance resilience against emerging cyber physical threats.

b. Why is it important to regularly engage in these types of emergency exercises?

Regular emergency exercises are essential because they give public power utilities and their external partners the opportunity to build relationships that will be critical to a unified, coordinated response to incidents. Exercises also allow utilities to test plans and procedures, identify gaps, and ensure that power can be restored as quickly and as safely as possible under stressful and rapidly evolving conditions.