LOTSIXTEEN

Committee: House Energy & Commerce Subcommittee on Energy
Event: Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid
Date: December 2, 2025
Time: 10:30 AM
Place: 2141 Rayburn House Office Building

Executive Summary: Today's hearing examined the escalating cyber and physical threats to the electric grid, with bipartisan acknowledgment that adversaries, especially China, are increasingly targeting U.S. energy infrastructure. Members stressed gaps in federal-utility information sharing, uneven preparedness across rural and urban systems, and the need to accelerate grid modernization as digital technologies expand the attack surface. Lawmakers also raised concerns about vulnerabilities in foreign-made grid components, slow replacement timelines for critical equipment, and the growing intersection of AI and grid security. Members agreed that securing the grid will require stronger coordination across federal agencies, utilities, and national labs, as well as sustained investment in resilience and threat mitigation.

Member Toplines:
Chair Bob Latta (R-OH-05): Latta highlighted growing cyber and physical threats to the electric grid amid rising power demand and the loss of dispatchable baseload generation, which is increasing blackout risks. He emphasized that expanding digitization and interconnected infrastructure have widened avenues for malicious attacks, particularly from China and Russia. Latta also pointed to recent physical attacks on substations as evidence of local vulnerabilities with major community impacts. He noted that utilities vary widely in their security capabilities, underscoring the importance of industry coordination and information-sharing through entities like the Electricity Information Sharing and Analysis Center (E-ISAC) and the North American Electric Reliability Corporation (NERC).

Ranking Member Kathy Castor (D-FL-14): argued that the United States is falling behind in building a modern and resilient grid because the Trump Administration canceled major Department of Energy (DOE) projects designed to reduce blackouts and improve automated grid operations. She noted that these terminated initiatives, including microgrids and smart sensors, would have strengthened grid flexibility during storms, cyberattacks, and outages. She contrasted slow U.S. electrification with China's rapid progress and growing dominance in clean energy technologies. He stressed that meeting Artificial Intelligence (AI) driven electricity demand and addressing cybersecurity risks will require rapid deployment of grid-enhancing tools, updated regulatory structures, and continued federal support for cybersecurity programs.

Full Committee Chair Brett Guthrie (R-KY-02)[1]*:* Guthrie emphasized that America's growing dependence on interconnected and digital energy systems increases vulnerability to cyber and

[1] Opening statements were available online at the time of memo composition.

physical threats from adversaries such as China, Russia, and Iran. He noted that emerging technologies and rising power demand expand the surface area for attacks, pointing to recent large-scale AI-driven cyber incidents as evidence of escalating risks. Guthrie also highlighted the potential for AI to strengthen grid security by improving detection and response capabilities. He underscored the important role of both large investor-owned utilities and rural electric cooperatives in safeguarding the grid.

Full Committee Ranking Member Frank Pallone (D-NJ-06): Pallone stressed that cybersecurity is central to energy affordability and reliability and urged more frequent bipartisan oversight of grid security. He warned that nation-state actors, domestic extremists, and advancing AI tools are rapidly increasing the sophistication and scale of potential cyber and physical attacks, citing the year-long compromise of a Massachusetts utility by China-linked hackers as evidence of real-world risks. He argued that DOE must lead federal energy-sector cybersecurity efforts due to its technical expertise and industry relationships, but noted that recent staffing losses under Secretary Wright undermine this mission. Pallone also highlighted the need to reauthorize and evaluate existing DOE and Federal Energy Regulatory Commission (FERC) cybersecurity programs and raised concerns that recent trade and manufacturing policies have increased U.S. dependence on foreign components, creating additional supply-chain vulnerabilities.

Witness Toplines:

Michael Ball, CEO of the Electricity Information Sharing and Analysis Center and Senior Vice President, North American Electric Reliability Corporation: Ball explained that the Electricity Information Sharing and Analysis Center serves as the electricity sector's primary clearinghouse for cyber and physical threat information, supporting more than 1,900 member utilities across the United States and Canada. He emphasized that the threat landscape is increasingly complex, driven by sophisticated nation-state actors such as China, Russia, Iran, and North Korea, as well as hacktivists and criminal groups. Ball highlighted E-ISAC's role in 24/7 monitoring, incident analysis, information sharing, and programs like the Cybersecurity Risk Information Sharing Program (CRISP) and the Energy Threat Analysis Center (ETAAC) that strengthen coordination with DOE, the Department of Homeland Security (DHS), and the intelligence community. He also noted E-ISAC's efforts to improve industry readiness through major security exercises and training events.

Sharla Artz, Security and Resilience Policy Area Vice President at Xcel Energy, on behalf of Edison Electric Institute (EEI): Artz emphasized that securing electric and natural gas systems from cyber and physical threats is a top priority for Xcel Energy and EEI member companies, which collectively serve nearly 250 million Americans. She highlighted that nation-state adversaries pose advanced and persistent risks and stressed the need for timely, actionable federal intelligence to help utilities detect and mitigate malicious activity. Artz pointed to ETAAC as a critical model for real-time, bidirectional information sharing between DOE, private utilities, and federal partners including DHS, the military, and law enforcement. She also underscored the Electricity Subsector Coordinating Council's role in unifying government and industry efforts to reduce systemic risk. Artz urged Congress to authorize and fund ETAAC and reinforce

DOE's leadership as the sector risk management agency in order to strengthen national security and industry resilience.

Tim Lindahl, President & CEO of Kenergy, on behalf of the National Rural Electric Cooperative Association (NRECA): Lindahl stressed that electric cooperatives face constant and increasingly sophisticated cyber threats, compounded by the resource limitations of rural service territories. He noted that co-ops serve 42 million Americans, including critical facilities, yet must absorb high security costs without shareholder support. He highlighted NRECA tools such as the Threat Analysis Center and Cyber Goals Program that help co-ops strengthen cyber hygiene and prioritize risks. Lindahl called for strong federal partnerships, urging DOE to quickly distribute Rural and Municipal Utility Cybersecurity program funds and for Congress to reauthorize the program. He concluded that continued federal support is essential to ensuring rural communities are not left behind in grid security.

Harry Krejsa, Director of Studies for the Carnegie Mellon Institute for Strategy & Technology: Krejsa warned that China is preparing to target U.S. defense and civilian infrastructure in a potential Taiwan conflict and that aging, partially digitized grid systems create exploitable vulnerabilities. He argued that full modernization is required because separating operational and digital networks is no longer practical in today's interconnected environment. Krejsa highlighted that digitally native technologies such as battery storage, smart inverters, and virtual power plants can create a more resilient, distributed, and self-healing grid. He cautioned, however, that China dominates the supply chains for many of these components, posing strategic risks. He urged Congress to strengthen coordination between energy and national security agencies and invest in secure, domestically manufactured technologies.

Zach Tudor, Associate Laboratory Director, National & Homeland Security, Idaho National Laboratory: Tudor warned that China, Russia, Iran, and North Korea are already embedded in U.S. infrastructure networks and are positioning themselves to disrupt critical services during a future crisis. He emphasized that aging, interconnected energy, water, telecommunications, and pipeline systems create cascading vulnerabilities, citing China's Volt Typhoon activity and incidents like the Colonial Pipeline attack as evidence. Tudor outlined Idaho National Laboratory's capabilities in testing and securing industrial control systems through programs such as Cyber-Informed Engineering and Cyber Testing for Resilient Industrial Control Systems. He highlighted the need to strengthen public–private partnerships, expand cybersecurity grant programs, and increase investments in national laboratory capabilities.

Major Takeaways:

Foreign Threats:

- Rep. **August Pfluge**r (R-TX-11) pointed out Chinese-made inverters and persistent PRC campaigns like Volt Typhoon; witnesses stated that utilities are more alert to the threat but still rely heavily on basic resilience practices.
- Rep. **Doris Matsui** (D-CA-07) warned that Chinese grid equipment could embed exploitable access points.
    - Krejsa called for a risk-based screening approach, while Tudor underscored how deeply Chinese components are embedded across U.S. power electronics.

- Rep. **Mariannette Miller-Meeks** (R-IA-01) pointed to coordinated activity from China, Russia, Iran, and North Korea, emphasizing the need to rebuild domestic manufacturing capacity for transformers and inverters; witnesses agreed these dependencies heighten strategic risk.
- Rep. **Troy Balderson** (R-OH-12) referenced U.S.–China Commission findings on sabotage vulnerabilities.
    - Tudor explained that the grid's age, scale, and decentralized ownership structure leave the United States especially exposed.

<u>Information Sharing:</u>

- Rep. Pfluger and Rep. **Russell Fry** (R-SC-07) pressed utilities on whether intelligence is reaching them quickly enough.
    - Lindahl and Artz noted progress but said smaller providers still struggle to access timely, actionable information.
- Rep. Miller-Meeks asked about federal coordination, and Ball stressed the importance of empowering E-ISAC as a central hub for multi-directional sharing between industry and government.
- Rep. **Lizzie Fletcher** (D-TX-07) highlighted CRISP and ETAAC as model programs for translating classified threat data into operational guidance.
- Rep. **Laurel Lee** (R-FL-15) asked whether companies hesitate to report incidents
    - Ball stated that uncertainty around liability protections can discourage openness.

<u>Physical Security Risks:</u>

- Rep. **Randy Weber** (R-TX-14) raised the Moore County substation attack as an illustration of targeted physical sabotage.
    - Witnesses responded that hardening alone cannot address the full range of threats, and emphasized better monitoring and detection.
- Rep. **Kim Schrier** (D-WA-08) asked about transformer replacement timelines after physical attacks.
    - Artz explained efforts to broaden spare transformer availability and standardize procurement to shorten delays.
- Rep. Miller-Meeks and Rep. Schrier also underscored wildfire risks and equipment shortages, highlighting the need for improved vegetation access and long-lead component planning.

<u>Cybersecurity Risks:</u>

- Rep. **Nick Langworthy** (R-NY-23) warned that removing natural gas as a backup fuel increases community vulnerability during cyber-induced outages
    - Tudor noted that hospitals, water systems, and emergency services are among the first affected.
- Rep. **Diana DeGette** (D-CO-01) emphasized that a diverse energy mix strengthens resilience, countering arguments that only conventional fuels ensure security, witnesses broadly agreed diversified resources reduce systemic risk.

- Rep. Schrier raised AI-enabled threats, and Ball acknowledged that adversaries are already probing AI tools for coordinated attacks, prompting NERC to reassess CIP protections.
- Rep. Balderson focused on how AI can accelerate both attack and defense capabilities
    - Tudor described ongoing national lab work to model adversary use of AI while cautiously developing defensive tools.
- Rep. **John James** (R-MI-10) argued that rapid deployment of inverter-based and digital technologies is outpacing cybersecurity standards.