BRETT GUTHRIE, KENTUCKY
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED NINETEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-3641
Minority (202) 225-2927

**MEMORANDUM** November 28, 2025

TO: Members of the Subcommittee on Energy
FROM: Committee Majority Staff
RE: Hearing titled "Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid"

---

## I. INTRODUCTION

The Subcommittee on Energy has scheduled a hearing for Tuesday, December 2, 2025, at 10:30 a.m. (ET) in 2141 Rayburn House Office Building. The hearing is entitled, "Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid." The hearing will review how electric utilities and other energy entities, in coordination with the federal government, prepare and respond to cyber and physical threats to the electric grid, as well as threats to other critical energy infrastructure.

## II. WITNESSES

- **Michael Ball,** CEO of the Electricity Information Sharing and Analysis Center and Senior Vice President, North American Electric Reliability Corporation
- **Sharla Artz,** Security and Resilience Policy Area Vice President at Xcel Energy, on behalf of Edison Electric Institute
- **Tim Lindahl**, President & CEO of Kenergy, on behalf of National Rural Electric Cooperative Association (NRECA)
- **Zach Tudor,** Associate Laboratory Director, National & Homeland Security, Idaho National Laboratory
- **Harry Krejsa,** Director of Studies for the Carnegie Mellon Institute for Strategy & Technology

## III. BACKGROUND

Our nation's energy infrastructure provides essential fuel to all critical infrastructure sectors. According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the energy sector serves one of the four lifeline functions, which means that its reliable operation is

so critical that a disruption or loss of energy function will directly affect the security and resilience of other critical infrastructure sectors.[1]

The nation's electric power system is a major component of the energy sector. This system's vast networks of high voltage transmission lines, generating resources, local distribution lines, and other critical infrastructure ensure the delivery of adequate and reliable supplies of electricity. Threats and hazards that could incapacitate or destroy certain components, assets, or systems in these networks could cause substantial, potentially widespread, harm to national security, economic security, public health and safety. These networks are owned and operated by utilities with varying ownership structures across various regulatory regimes depending on the region.

Both governmental and non-governmental entities are charged with ensuring the reliability of the nation's bulk power system—the interconnected electricity transmission network—pursuant to various standards and regulations. Under the Energy Policy Act of 2005,[2] Congress provided FERC with the authority to approve mandatory cybersecurity standards proposed by the Electric Reliability Organization (ERO). The North American Electric Reliability Corporation (NERC) currently serves as the ERO. NERC proposes reliability standards for planning and operating the North American bulk power system. These critical infrastructure protection (CIP) reliability standards[3] address physical security and cybersecurity of critical electric infrastructure. NERC also operates information sharing programs (see below) that are operationally isolated from its standards enforcement processes.

***Physical and Cyber Threats to Critical Electric Infrastructure***

The United States faces an evolving landscape of threats to critical infrastructure, from sophisticated nation states to ideologically or criminally driven "hacktivist" campaigns. The *Annual Threat Assessment of the U.S. Intelligence Community* notes that state actors targeting critical infrastructure include Russia, China, Iran, and North Korea.[4] While Russia has long been considered to have the most sophisticated capabilities, according to the most recent Assessment, the Peoples Republic of China (PRC) "remains the most active and persistent threat to U.S. government, private-sector, and critical infrastructure networks."[5]

The U.S. Department of Homeland Security's 2025 *Homeland Threat Assessment* notes: "PRC state-sponsored cyber actors have pre-positioned cyber exploitation and attack capabilities for disruptive or destructive cyber attacks against U.S. critical infrastructure in the event of a

---

[1] U.S. Department of Homeland Security, *Energy Sector-Specific Plan* (2015), U.S. DHS, https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.
[2] P.L. 109-58.
[3] North American Reliability Corporation (NERC), *CIP – Critical Infrastructure Protection*, NERC, https://www.nerc.com/standards/reliability-standards/cip (lasted visited Nov. 24, 2025).
[4] Office of Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Mar. 2025), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.
[5] *Id.* at 11.

major crisis or conflict with the United States."[6] In one recent instance, the PRC was associated with a cyber campaign publicly known as Volt Typhoon, which gained access to the information technology systems of multiple critical infrastructure organizations, including energy systems, to disrupt critical functions.[7]

Threats also include criminal- and terror-related cyber as well as physical attacks. For example, on February 6, 2023, the Department of Justice announced the arrest of two individuals for planning to attack five electric power transmission substations around Baltimore, Maryland. On December 25, 2022, four electric distribution substations in the Tacoma, Washington area were physically attacked, allegedly with malicious intent by two individuals in a burglary scheme, causing millions of dollars in damage and cutting power to some 30,000 utility customers. Three weeks earlier, unknown perpetrators attacked two substations in Moore County, Nort Carolina, causing an extended blackout for 45,000 area customers.

The subcommittee held a field hearing on physical threats like these in June 2023.[8] Although such attacks may be localized, the ability to restore services remains challenging and risks substantial, life threatening disruptions to communities, along with harm to critical industry and security installations.

***Government-Industry Collaboration***

Congress has provided the Department of Energy (DOE) with a range of emergency response and cybersecurity authorities affecting multiple segments of the energy sector, beginning with the Department of Energy Organization Act,[9] and more recently with the Fixing America's Transportation Act (FAST Act).[10] Enacted in 2015, the FAST Act designated DOE as the Sector-Specific Agency, now termed Sector Risk Management Agency (SRMA), for cybersecurity for the energy sector. The law also provided the Department with several authorities to respond to threats to energy systems, including authority under the Federal Power Act relating to grid security emergencies and critical defense electric infrastructure.

As the SRMA, DOE leads federal efforts to coordinate with the electric sector. The CEO-led Electricity Subsector Coordinating Council (ESCC)[11] serves as the principal liaison between the Federal government and the electric power sector in coordinating efforts to prepare for national-level incidents or threats to critical infrastructure. The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership, funded by DOE and industry. CRISP is managed by the Electricity Information Sharing and Analysis Center (E-ISAC)[12] and facilitates the timely bi-directional sharing of unclassified and classified threat information with energy

---

[6] U.S. Department of Homeland Security, *Office of Intelligence and Analysis Homeland Threat Assessment* (2025), U.S. DHS, https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf.
[7] *Id.*
[8] *See Enhancing America's Grid Security and Resilience: Hearing Before Subcomm. Energy of the H. Comm on Energy and Commerce, 118th Cong. (Jun. 16, 2025)*.
[9] P.L. 95-91.
[10] P.L. 114-94.
[11] *See* Electric Subsector Coordinating Council (2025), https://www.electricitysubsector.org.
[12] *See* Electricity Information Sharing and Analysis Center (2025), https://www.eisac.com/s/.

sector partners. The E-ISAC, which works with DOE and the ESCC, is run by NERC and is operationally isolated from NERC's enforcement processes. DOE also operates the Energy Threat Analysis Center (ETAC), a public-private partnership pilot that convenes government and industry experts to analyze and advise on emerging threats.[13]

Identifying and safeguarding against hazards and threats to the electric grid, including physical and cybersecurity threats by malicious actors, requires constant attention to plan, prevent, and respond, as well as to restore power services should they be lost. It involves close attention by utilities and coordination with industry and government authorities. This hearing will provide an opportunity to deepen understanding about how the electric industry works to secure the grid from such hazards and threats.

## IV. ISSUES

- What are the challenges to addressing cyber and physical security threats in U.S. energy infrastructure, including the electric grid, pipelines, and gas facilities;
- What is necessary for effective utility-government collaboration on cyber and physical threats to energy infrastructure;
- What are the challenges with addressing cyber and physical threats for nonprofit, municipal and rural utilities;
- What is DOE's role as the Sector Risk Management Agency;
- What are FERC and NERC's role in addressing cyber and physical risks; and
- What are the emerging cyber risks with respect to AI and load growth?

## V. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Mary Martin, Peter Spencer, or Andrew Furman of the Committee Staff at (202) 225-3641.

[13] U.S. Department of Energy (DOE), *Energy Threat Analysis Center*, https://www.energy.gov/ceser/energy-threat-analysis-center-0 (last visited Nov. 24, 2025).