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

Updated Memorandum

January 10, 2026

MEMORANDUM

TO: Members of the Subcommittee on Energy
FROM: Committee Majority Staff
RE: Hearing titled "Protecting America's Energy Infrastructure in Today's Cyber and Physical Threat Landscape"

I. INTRODUCTION

The Subcommittee on Energy will hold a hearing on Tuesday, January 13, 2026, at 10:15 a.m. (ET) in 2123 Rayburn House Office Building. The hearing is entitled, "Protecting America's Energy Infrastructure in Today's Cyber and Physical Threat Landscape." The hearing will review the following legislation:

- H.R. ____, Energy Threat Analysis Center Act of 2026
- H.R. ____, Energy Emergency Leadership Act
- H.R. ____, Rural and Municipal Utility Cybersecurity Act
- H.R. ____, Securing Community Upgrades for a Resilient Grid (SECURE Grid) Act
- H.R. ____, Pipeline Cybersecurity Preparedness Act

II. WITNESSES

Panel 1

- **Alex Fitzsimmons**, Acting Undersecretary of Energy and Director of the Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy

Panel 2

- **Scott I. Anderson**, Senior Vice President, Energy Security and Industry Operations, Edison Electric Institute;
- **Adrienne Lotto**, Senior Vice President of Grid Security, Technical and Operations Services, American Public Power Association;
- **Nathaniel J. Melby, Ph.D.**, Vice President and Chief Information Officer, Dairyland Power, on behalf of National Rural Electric Cooperative Association (NRECA); and,
- **Rebecca O'Neil**, Research Principal, Infrastructure, Energy and Environment Directorate, Pacific Northwest National Laboratory.

III. BACKGROUND

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* (Assessment) notes that state actors targeting critical infrastructure include Russia, China, Iran, and North Korea.[1] 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."[2]

The U.S. Department of Homeland Security's 2025 *Homeland Threat Assessment* notes that "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 major crisis or conflict with the United States."[3] In one recent instance, the PRC was associated with a cyber campaign publicly known as Volt Typhoon, which gained access to information technology systems of multiple critical infrastructure organizations, including energy systems, to enable lateral movement to the operational technology assets to disrupt functions.[4] Threats also include criminal—and terror-related—cyber attacks, as well as physical attacks.

Both governmental and non-governmental entities are charged with ensuring the reliability of the nation's bulk power system—the interconnected electricity transmission network—through standards and regulations. Through the Energy Policy Act of 2005,[5] Congress provided the Federal Energy Regulatory Commission (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.

---

[1] 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.
[2] *Id.* at 11.
[3] U.S. Dept. of Homeland Security, *Office of Intelligence and Analysis Homeland Threat Assessment* (2025), https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf.
[4] *Id.*
[5] Pub. L. No. 109-58.

These critical infrastructure protection (CIP) reliability standards[6] 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.

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,[7] and more recently with the Fixing America's Transportation Act (FAST Act).[8] 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 Energy SRMA, DOE coordinates with multiple Federal and State agencies and collaborates with energy infrastructure owners and operators on activities associated with identifying vulnerabilities and mitigating incidents that may impact the energy sector. To perform these duties effectively, DOE must account for each interrelated segment of the nation's energy infrastructure, including pipelines, which are subject to an array of other Federal authorities. In a January 24, 2018, letter, the Committee wrote to Secretary Perry to better understand the level of coordination among governmental agencies.[9] In response, Secretary Perry noted that "a coordinated government approach to the cyber and physical security of pipelines, led by the Department of Energy, is essential to ensuring the safe and reliable flow of energy across the U.S."[10]

The Transportation Security Administration (TSA) also has certain responsibilities related to security for pipelines. The Aviation and Transportation Security Act of 2001[11], which established the Transportation Security Administration within the Department of Transportation, authorized the agency "to issue, rescind, and revise such regulations as are necessary" to carry out its functions.[12] TSA was transferred to the Department of Homeland Security, created under the Homeland Security Act of 2002.[13] The Implementing Recommendations of the 9/11 Commission Act of 2007[14] directs TSA, in consultation with the Pipeline and Hazardous Materials Safety Administration, to promulgate pipeline security regulations and carry out necessary inspection and enforcement if the agency determines that regulations are appropriate.[15]

---

[6] North American Reliability Corporation, *CIP – Critical Infrastructure Protection*, https://www.nerc.com/standards/reliability-standards/cip (lasted visited Nov. 24, 2025).
[7] Pub. L. No. 95-91.
[8] Pub. L. No. 114-94.
[9] Letter from H. Comm. Energy and Commerce to Scott Perry, Sec. of Energy, U.S. Dept. of Energy (Jan. 24, 2018), https://d1dth6e84htgma.cloudfront.net/02_20180124_DOE_cb92ee81b7.pdf.
[10] Letter from Sec. Rick Perry to Chairman Greg Walden, H. Comm. Energy and Commerce (Mar. 13, 2018), https://docs.house.gov/meetings/IF/IF03/20180314/107999/HHRG-115-IF03-20180314-SD053.pdf.
[11] Pub. L. No. 107-71.
[12] Pub. L. No. 107-71.
[13] Pub. L. No. 107-296.
[14] Pub. L. No. 110-53.
[15] Pub. L. No. 110-53.

The CEO-led Electricity Subsector Coordinating Council (ESCC)[16] 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)[17] and facilitates the timely bi-directional sharing of unclassified and classified threat information with energy 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.

Several cybersecurity initiatives have been enacted in recent years. The Infrastructure Investment and Jobs Act (IIJA),[18] enacted several cybersecurity provisions, including the Enhancing Grid Security through Public-Private Partnerships Act and the Cyber Sense Act developed by Energy and Commerce Members. The IIJA provisions also authorized a program that developed the Energy Threat Analysis Center (ETAC), a public-private partnership pilot that convenes government and industry experts to analyze and advise on emerging threats,[19] and the Rural and Municipal Utility Advanced Cybersecurity (RMUC) Grant and Technical Assistance Program, to advance cybersecurity at electric cooperatives, non-profit municipal, and small investor-owned utilities, both of which are addressed in the legislation under consideration.

IV. LEGISLATION

A. H.R. ____, Energy Threat Analysis Center Act of 2026

This legislation would reauthorize the DOE program authorized in section 40125(c) of the IIJA,[20] which established an Energy Threat Analysis Center. The legislation would reauthorize the program through 2031. In addition, the legislation provides clarifying language for carrying out the program, relating to collaboration and intelligence sharing between the Federal government and the energy sector to strengthen collective defense, response, and resilience.

B. H.R. ____, Energy Emergency Leadership Act

This legislation would amend the Department of Energy Organization Act[21] to include energy emergency and energy security among the functions that the Secretary of Energy shall assign to an Assistant Secretary. The legislation provides that the functions assigned to an Assistant Secretary under this amendment would include responsibilities with respect to energy infrastructure, security and resilience, emerging threats, cybersecurity, supply and emergency planning, coordination, response, and restoration and would include the provision of technical assistance, support, and response capabilities with respect to energy security threats, risks, and incidents to State, local, and Tribal governments and the energy sector. The legislation provides

---

[16] *See* Electric Subsector Coordinating Council (2026), https://www.electricitysubsector.org.
[17] *See* Electricity Information Sharing and Analysis Center (2025), https://www.eisac.com/s/.
[18] 42 U.S.C. § 18724.
[19] U.S. Dept. of Energy, *Energy Threat Analysis Center*, https://www.energy.gov/ceser/energy-threat-analysis-center-0 (last visited Nov. 24, 2025).
[20] 42 U.S.C. § 18724(c).
[21] Pub. L. No. 95-91.

that the Secretary of Energy shall ensure the functions under this amendment are performed in coordination with relevant Federal agencies. (Substantially similar legislation passed the House in the 116th, 117th, and 118th Congresses.)

C. H.R. ___, Rural and Municipal Utility Cybersecurity Act

This legislation would reauthorize the Rural and Municipal Utility Advanced Cybersecurity (RMUC) Grant and Technical Assistance Program, authorized in section 40124 of the IIJA,[22] through October 31, 2030. The program provides technical and financial assistance to eligible entities, which include rural electric cooperatives, municipally owned utilities, and small investor-owned utilities, to protect and harden the systems against cyber threats and to increase participation in cybersecurity threat information sharing programs. The legislation also amends the underlying statute to streamline financial assistance application processes to ensure funding is allocated to small and rural entities that need it most.

D. H.R.____, Securing Community Upgrades for a Resilient Grid (SECURE Grid) Act

This legislation would amend requirements for State Energy Security Plans, authorized by section 366 of the Energy Policy and Conservation Act, to consider threats to local distribution alongside bulk-power systems, as well as supply chain and weather-related threats and vulnerabilities. This bill also requires coordination with suppliers of manufactured components and infrastructure in the electric grid to improve understanding of supply chain risks. The bill would also clarify that the Department of Energy is not required to approve State Energy Security Plans.

E. H.R. ____, Pipeline Cybersecurity Preparedness Act

This legislation would require the Secretary of Energy, pursuant to the Secretary's statutory authorities, to carry out a program to coordinate Federal agencies, States, and the energy sector to ensure the security, resiliency, and survivability of natural gas pipelines, hazardous liquid pipelines, and liquefied natural gas (LNG) facilities. The program would establish policies and procedures to coordinate analysis and information sharing; coordinate responses to and recovery from physical and cyber incidents impacting the energy sector; develop for voluntary use cybersecurity applications, technologies, and analytical tools; perform pilot demonstration projects with the energy sector; and establish workforce development and security curricula for such pipelines and LNG facilities. The legislation does not provide new regulatory authority and further provides that it shall not be construed to modify the authority of any other Federal agency other than DOE with respect to natural gas pipelines, hazardous liquid pipelines, and LNG facilities. (Substantially similar legislation was reported favorably by the Committee in the 115th, 116th, and 117th Congresses.)

---

[22] 42 U.S.C. § 18723.

V. STAFF CONTACTS

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