

**Chairman Robert Latta**  
**Opening Statement—Subcommittee on Energy**  
**Subcommittee Markup of 5 Bills**  
**February 4, 2026**  
*As prepared for delivery*

Today the Energy Subcommittee will mark up five bills that will update and enhance programs to help ensure the physical and cyber security of our nation’s electric grid.

These bills, two of which we have moved through the Committee in past Congresses with strong bi-partisan support, also strengthen the Department of Energy’s ability to carry out its energy emergency functions.

At our legislative hearing three weeks ago, witnesses emphasized the importance of robust collaboration between industry, states, and the federal government to ensure secure energy systems.

These bills will strengthen this work by enhancing DOE’s existing energy sector authorities and by providing new tools to ensure fuller industry involvement.

We consider these bills today against the backdrop of growing threats to our energy systems—including advanced threats from our adversaries.

As noted in recent hearings, Communist China remains the most active and persistent threat to American critical infrastructure networks. Its proxies have pre-positioned attack capabilities in American infrastructure, to be used during a major crisis or conflict.

Addressing these and related threats is difficult and can be resource intensive.

The interconnected nature of our energy systems requires constant intelligence sharing, clear visibility into threat landscapes, and sufficient resources to fill gaps in security protections, particularly for rural and small utility service territories.

The bills we will consider today take important steps to accomplish this and more.

H.R. 7305, the Energy Threat Analysis Center Act of 2026, led by the gentlelady from Florida’s fourteenth congressional district and the gentleman from Colorado’s eighth congressional district, authorizes a program that improves information sharing and coordination on threat analyses that impact the power sector.

A key ingredient of this program involves two-way sharing of information between grid operators and the intelligence community to their mutual benefit: improving the ability to assess risks and threats and then how to act upon that information.

H.R. 7258, the Energy Emergency Leadership Act, led by the gentlelady from Florida’s fifteenth congressional district and the gentleman from Ohio’s first congressional district, represents long-

time bipartisan policy of this Committee to strengthen the ability of DOE to carry out its energy sector security and emergency functions.

The bill requires the energy emergency and security functions at DOE are led by an Assistant Secretary, confirmed by the Senate. This will ensure the Department has the focused and accountable leadership that will strengthen intergovernmental and energy sector collaboration.

H.R. 7266, the Rural and Municipal Utility Cybersecurity Act, led by the gentlelady from Iowa's first congressional district and the gentlelady from Virginia's fourth congressional district, provides targeted funding and technical assistance so small utilities, electric co-operatives, and public power agencies have the resources to secure their critical electric systems—including systems serving military installations.

Of course, as we heard during our legislative hearing, States are critical to energy security. They have unique visibility into the interconnected relationships, risks and vulnerabilities related to the energy systems within their borders.

H.R. 7257, the SECURE Grid Act, which I sponsored with my colleague from California's seventh congressional district, builds upon the existing State Energy Security Plan framework to expand the visibility of potential threats to local electric distribution and supply chain networks.

Finally, as the Sector Risk Management Agency for the energy sector, DOE must have visibility over the whole energy sector, which as we heard in the legislative hearing is comprised of increasingly interconnected systems.

Because of this, DOE actively works not only with the power sector, but also the oil and gas sector to prepare and respond appropriately to emergencies.

DOE's technical capabilities and central role in Federal energy coordination make it well positioned to improve the complex layers of communication necessary for energy sector security.

H.R. 7272, the Pipeline Cybersecurity Preparedness Act, led by the Subcommittee Vice Chairman from Texas's fourteenth congressional district and the gentlelady from Michigan's sixth congressional district, does just this.

It builds on DOE's leadership to establish a non-regulatory program to improve the coordination and other assistance across the energy sector, states, and the federal government with regard to the security and resilience of pipelines and other facilities that deliver the nation's oil and gas—and are necessary for reliable energy and power.

All told, these bills advance the important bipartisan work of this Subcommittee to protect critical energy infrastructure.