Chairman Robert Latta
Opening Statement—Subcommittee on Energy
"Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid"
December 2, 2025
As prepared for delivery

Good morning and welcome to today's hearing. We will examine how the electric industry is addressing cyber and physical threats to the electric grid—a key component of our nation's critical energy infrastructure.

We will look at the challenges to securing this infrastructure at a time of tremendous growth in power demand.

This hearing will help inform the Subcommittee on current initiatives and practices to secure our nation's critical electric infrastructure from the various malicious threats to the delivery of power.

This year we have frequently heard about the challenges to the reliable delivery of energy and power.

Grid operators have testified about the massive premature loss of dispatchable power in our electric grid without adequate replacement. This has resulted in increased blackout risks in certain regions of the nation during times of peak demand.

Addressing cyber and physical threats represents another challenge to the reliable delivery of energy and power. Incapacitating the grid with cyber or physical attacks can have widespread, devasting impacts, which makes security particularly vital to our nation's security, economy, our health, and welfare.

Addressing these threats is difficult. The avenues for malicious attack only increase with increased digitization, and the growing linkages of gas pipelines, new generating resources, and expanded transmission. These linkages have been rapidly increasing as the nation works to meet growing power demand, particularly from AI.

As the public security assessments note, the nation faces an evolving landscape of threats – from nation states to criminal and ideologically motivated cyber attackers.

Russia has long been a persistent threat to our energy systems. Yet China has become particularly worrisome.

Even as we race with China on AI, the U.S. intelligence community reports in its public assessments that China remains the most active and persistent threat to American critical infrastructure networks. China's proxies have pre-positioned attack capabilities in American infrastructure, to be used during a major crisis or conflict.

More local risks relating to physical attacks also threaten communities and other important infrastructure.

Just two years ago, this Subcommittee held a field hearing in North Carolina to examine the threats surrounding an attack on electric substations. The attack in question left 30,000 people without power and exposed how targeted physical attacks can impact people and industry, even the military, in critical regions.

Addressing cyber and physical threats is made more complicated by individual utilities' particular capabilities, resources, and access to threat intelligence and other information.

Our witnesses this morning can help us understand how the industry works to overcome these challenges.

We'll hear testimony from grid executives representing both investor-owned utilities and the nonprofit Cooperatives—which together cover the bulk of American electric infrastructure.

We'll also hear from the head of the Electricity Information Sharing and Analysis Center, or E-ISAC. This operation, run by the North American Electric Reliability Corporation, or NERC, provides important information-sharing services to assist industry with critical infrastructure threats.

Given that Congress has charged NERC with assuring reliability of the electric system, a perspective on what is necessary to coordinate grid security to effectively address growing vulnerabilities will be important.

We'll hear from a grid security expert at Carnegie Mellon who has been active on the National Security Council.

And, finally, we'll hear from the Associate Laboratory Director for national security at Idaho National Laboratory. He can provide insights into threats and into how the U.S. government is working to help industry be more informed about the most consequential risks, and to better plan and protect our grid.

Energy and Commerce has led on enactment of several laws over the past decade to ensure appropriate national attention to cyber and physical risks in our nation's critical energy infrastructure.
This work ranged from clarifying government authorities in the Federal Power Act to authorizing several technical assistance and information sharing programs to assist utilities of all sizes.

The hearing today should inform us as we seek to update and reauthorize various provisions that aim to make the nation more secure.