North American Electric Reliability Corporation
QFR Responses for December 2, 2025, Cybersecurity Hearing
House Energy and Commerce Subcommittee on Energy

The Honorable Robert Latta (R-OH)

1. Your testimony underscores the importance of collaboration between industry, the government, and our national labs. Smaller utilities can be responsible for critical power infrastructure as consequential as large utilities.

A. It is true that smaller utilities can be responsible for critical and consequential power infrastructure. The E-ISAC works closely with the trade associations of public power utilities (American Public Power Association) and rural electric cooperatives (National Rural Electric Cooperative Association) as well as their members to ensure these utilities receive timely and actionable threat information.

a. You reference the CRISP 30 and oil and natural gas programs aimed at smaller utilities, why are these important for assuring power-sector security?

A. Given the strategic locations of some medium and small utilities near critical defense facilities, supporting them is essential to our national defense. Often resource constrained by budgeting processes and the need to provide affordable power to the communities they serve in addition to the defense facility, these utilities are at a security disadvantage without support. These utilities also often provide gas and water services to the community and bases. Nation-state adversaries routinely probe the industry's defenses, looking for less defended networks.

Support from DOE and the War Department help raise the security baseline of small and medium utilities that serve defense infrastructure. It must be done in a coherent and coordinated fashion, and include the relevant ISACs (electricity, natural gas, water) to ensure the industry has the best possible defense posture against geopolitical threats.

2. What specific risks do Chinese-manufactured inverters—found in solar, battery, and other energy technologies—pose to the security and reliability of the U.S. electric grid?

A. Any device or component that is manufactured in an adversarial nation has the potential to allow unexpected or unauthorized remote connectivity to the device and the system it is connected to. In the case of inverters, as increasing numbers appear on the grid in response to the significant demand for additional power, the potential risk for an adversary to influence reliable power delivery also grows. Even if the devices or components are not designed for intentional malice or misoperation, unexpected connectivity via Bluetooth or other transmitting components could create a pathway for a skilled adversary unauthorized access to the device.

3. What short-term and long-term strategies should the U.S. government take to mitigate the threat created by having Chinese-manufactured inverters on the electric grid?

A. The risks presented by the increased attack surface of devices such as inverters can be mitigated through a variety of methods, not the least of which is compliance with NERC's mandatory and enforceable standards for NERC registered entities. Additional network architecture steps, security reviews, criticality analyses, cyber-informed engineering, software and hardware bill of materials review, and procurement terms can mitigate unexpected connectivity, as long as it is supplemented by actionable information sharing on specific threats and capabilities. The E-ISAC facilitates the sharing of these best practices, threat information, and awareness of the potential risks in partnership with the ETAC, DOE, the national labs, and the E-ISAC's Vendor Affiliate Program partners.

4. What collaboration between the private and public sectors is needed to develop countermeasures to protect the U.S. grid against these vulnerabilities?

A. Continued threat information sharing via government, industry, and the E-ISAC is an essential countermeasure to the threat posed by internet connected devices found in the power grid. The Energy Threat Analysis Center (ETAC) presents a unique opportunity to address this threat and industry risk by allowing an operational collaboration space where the industry context can be added, tested, and applied to information sharing products. Additional collaboration through programs like the Cybersecurity Risk Information Sharing Program (CRISP) provides an opportunity for near real-time, two-way information sharing of netflow data with DOE to identify cyber threats and potential unexpected remote connectivity. Greater collaboration with the Original Equipment Manufacturers (OEMs) that design, build, deploy, and sometimes operate inverter technology creates the opportunity to develop devices that are secure by design. The E-ISAC plays a critical role in facilitating this private and public sector coordination on collective defense, sharing information and providing forums for collaboration through its Vendor Affiliate Program.

5. What regulatory measures should be imposed to prevent the proliferation of embedded technologies in inverters to secure critical infrastructure, like the U.S. electric grid?

NERC's Cyber Security Supply Chain Risk Management Reliability Standards require entities to document and implement supply chain cyber security risk management plans for their high and medium impact BES (Bulk Electric System) Cyber Systems which require, in part, the identification and assessment of product risks as well as methods for determining active vendor remote access sessions (including individual or system-to-system communications). Consistent with FERC Order 912, NERC is currently undertaking revisions to the Cyber Security Supply Chain Risk Management Reliability Standards that would establish specific timing requirements for evaluation of equipment and vendors, require a process for managing identified risks, and extend these requirements to any devices connected to CIP-protected systems in the same network zone of trust.

Additionally, NERC staff are collaborating with industry through the Reliability and Security Technical Committee Supply Chain Subcommittee to develop guidance regarding the validation of vendor responses provided when assessing product risks.

6. How might ongoing Trump Administration efforts to onshore supply chains and promote domestic manufacturing in the energy sector protect the U.S. electric grid from national security risks?

A. Efforts to ensure that supply chains produce high quality, cyber secure, and resilient systems and devices should enable greater reliability and security of the U.S. electric grid. Some features that domestically manufactured and on-shored equipment should include are:

- Operating systems that require strong access authentication procedures (complex passwords, multi-factor authentication)

- Changing default passwords and closure of non-necessary access device ports (default closed)

- Rapid and transparent vendor cyber compromise notifications

- Thoroughly tested and vetted third-party suppliers

The Honorable Mariannette Miller-Meeks (R-IA)

1. EISAC receives threat intelligence from multiple sources. What makes ETAC unique? Why do we need a dedicated fusion center at NREL to bridge the gap between classified intelligence and actionable security measures for utilities? And what would the electricity sector lose if ETAC didn't exist?

A. The E-ISAC benefits industry and the grid being at the center of a complicated and wide-ranging information sharing ecosystem. A key recent element of that system is the **Energy Threat Analysis Center**. The ETAC is unique among operational collaboration centers in that it has private sector representatives side by side with government, intelligence, and national laboratory experts at the unclassified and classified levels. The E-ISAC is a core founding partner of the ETAC, providing the ETAC with a cross-industry perspective of threats, as well as a trusted dissemination channel.

ETAC analysts meet regularly to review threats, provide industry context and recommendations to the sector that is not available from any other sources. Recently, geopolitical events have highlighted the unique value of the ETAC in that it is able to look at sensitive threat information only available to the intelligence community, and then compare it with what is seen on partner networks. Furthermore, the ETAC can reach back across industry expertise to provide context, but also guidance on how to detect and mitigate threats in the energy sector, a subject matter expertise that is not currently found in government.

Being located in middle of the continent enables greater participation among industry organizations and national labs, as well as an efficient and existing connection to government

classified networks. If the ETAC were unavailable, it would take significant investment in new resources to reestablish the facility either at another national lab or existing site and may preclude the regular participation due to geographic distance and travel by utilities.