The Honorable Bob Latta (R-OH)

The Infrastructure Investment and Jobs Act (IIJA) included the Cyber Sense Act and Enhancing Grid Security through Public Private Partnerships Act, both of which I had championed in previous Congressional sessions. These bills sought to improve cybersecurity equipment testing and leverage expertise of government agencies through public private partnerships.

a. Can you discuss how these provisions have assisted cybersecurity protection since the implementation through IIJA?

The cybersecurity provisions enacted through the IIJA have strengthened the industry's cybersecurity position. The IIJA's emphasis on public-private partnerships has enhanced coordination between industry and federal agencies including the Department of Energy (DOE), the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS CISA), and national laboratories. These partnerships have improved information dissemination, accelerated threat intelligence sharing, and supported the development of tools and best practices for our industry.

The expansion of the Energy Cyber Sense program, in particular, has improved visibility into the cybersecurity of industrial control and operational technology products. These supply chains support a resilient, secure energy grid. By providing independent testing and identifying vulnerabilities, the program has enabled electric companies to make more informed procurement decisions and incentivized vendors to build more secure products. The program also has encouraged collaboration with industry and government partners to further the security of the nation's energy infrastructure.

The Honorable Brett Guthrie (R-KY)

1. DOE is the energy sector authority and must work with other agencies and States. To do this effectively, it must have a culture of constant learning and improvement, which will benefit the whole federal approach to support the energy sector.

a. Would you speak to the importance of a culture of constant learning and constant improvement for the stakeholders you represent?

Every incident and exercise is an opportunity to learn. The electric sector works with federal and state partners to create tools and technologies that enhance situational awareness and support information sharing for emerging threats. Given the evolving nature of cyber and physical threats to critical infrastructure, as well as an uptick in more frequent and severe extreme weather, electric companies foster an environment of constant learning to incorporate lessons from these incidents and through participation in training exercises that inform "blue sky" operations.

For example, EEI hosts an annual National Response Event tabletop exercise, a sector-wide simulation that brings together partners from government and across critical sectors to model grid disruptions and test coordinated response and recovery efforts. EEI also supports the development of industry training and exercises conducted by DOE (e.g., Clear Path), the Electricity Information Sharing and Analysis Center's (E-ISAC's) biannual Grid Ex series, and other security agencies, informing curricula, sharing the operational needs of industry, and providing actionable feedback following real and simulated events.

The Honorable Rick Allen (R-GA)

1. The Savannah River National Lab (SRNL) is adjacent to my district. As I mentioned in the first panel, national labs play a critical role in grid security.

a. How can national labs be leveraged to use their trained cyber operators to enhance security operating technologies?

The national labs combine technical expertise and test environments that most utilities and vendors are unable to replicate on their own. Cyber operators at several of the labs are involved in DOE's CyTRICS and CyOTE programs which are helpful to industry practitioners in testing critical components used in the energy sector and detecting anomalous behavior in operational technology (OT) environments. Five of the national labs also contribute analytic and technical expertise to the Energy Threat Analysis Center, or ETAC. ETAC is a program jointly run by DOE CESER and industry partners to share actionable strategies to find and mitigate cyber threats to US critical energy infrastructure. These resources

help utilities understand vulnerabilities to their systems before product deployment and offer mitigative measures to protect against threats. The labs' cyber experts are also leveraged in training programs for industrial control systems and OT defense to advise security officers of the tactics, techniques, and procedures being used by adversaries. Given the expertise and equipment available at the national labs, potential areas where they could be more fully leveraged to enhance securing operating technologies include hands-on training, red team and validation exercises, supply chain testing, and utility support after cyber incidents.

The Honorable Mariannette Miller-Meeks (R-IA)

1. Congress passed significant cybersecurity provisions in the Infrastructure Investment and Jobs Act, including the authorization for ETAC and RMUC. Your member companies have been working with these programs for several years now. From the investor-owned utility perspective:

a. Have the IIJA cyber provisions fulfilled the needs of the electricity sector, or do gaps remain?

The Energy Threat Analysis Center (ETAC) was formed by the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) in 2023. ETAC began as a pilot program authorized by the IIJA to provide the private energy sector operational support for cyber resilience.

ETAC brings together government experts and energy sector personnel to analyze cyber threats towards critical energy infrastructure. Within that mission, ETAC objectives include strengthening collective energy sector defense and resilience, facilitating communication between industry and government on threats or likely threats, and further understanding the risks posed to national security by threat actors or adversaries.

The ETAC is a first-of-a-kind operational collaborative that convenes experts from the DOE and the energy sector to identify, analyze, and mitigate cyber threats to critical energy infrastructure. Through the ETAC analysis, threat intelligence and mitigation guidance are developed and distributed to utilities nationwide. The products developed by ETAC are shared through the E-ISAC with the entire sector

to help raise awareness of potential threats and make mitigative measures available. Without it, energy infrastructure owners and operators would lose the central mechanism for fusing intelligence with real-world grid operations that enable them to deliver the insights, warnings, and mitigation strategies to protect national security and the reliability of the electric grid.

Legislation that builds on the IIJA pilot and codifies ETAC would enhance grid security and national defense. Efforts by this committee to formalize ETAC would allow it to continue providing value to the critical energy infrastructure owners and operators who maintain these systems that underpin the grid.

b. What additional authorities, resources, or programs would strengthen your members' ability to defend against sophisticated nation-state adversaries?

Beyond authorization of ETAC, continued support for a long-term reauthorization of the protections in CISA 2015 remain a priority for our members. A clean reauthorization is the most direct path to ensuring that the industry's current information sharing pathways are not adversely impacted. A long-term reauthorization of the protections in CISA 2015 afforded to sharing cyber threat indicators and defensive measures may also provide the certainty needed to pursue additional threat information sharing programs within the energy sector, and potentially between energy and other critical infrastructure sectors.

As the Committee explores new areas of authorization that may be valuable, expanding on the types of information that can be protected, including data identified from real-time system operation or other operational technology, would be a positive next step in the evolution of information sharing. Oftentimes cyber intrusions from a threat actor present as anomalies on a real-time system before they are identified as cyber threat indicators. Sharing threat data immediately with critical non-regulatory partners, both private sector and government, would help identify an intrusion more quickly and ultimately help inform the broader sector of a potential threat.

Separately, any efforts to identify and promulgate a replacement for the Department of Homeland Security's Critical infrastructure Partnership Advisory Council (CIPAC) helps bolster the industry government collaboration that is essential to risk identification and mitigation.

c. Are there specific areas where you've seen the most value from federal partnership, and areas where more work is needed?

The most value comes from partnerships that combine government intelligence, national laboratory expertise, and utility operational experience in a way that produces timely, actionable guidance. As a primary example, ETAC collaborates across government with support from DOE's Office of Intelligence and Counterintelligence, DOE's National Laboratories (namely the National Laboratory of the Rockies) and the Cybersecurity and Infrastructure Security Agency (CISA). Examples of the value of that collaboration include the development and release of a joint advisory to address threats to energy infrastructure posed by the Volt Typhoon hacking group. Stemming from this work, ETAC stakeholders are also working together to build an information technology (IT) platform that can pull together different streams of cyber threat data from government and industry partners.

Further, while our members continue to be successful in one-off partnerships with the vendor community, the energy sector especially benefits when the national lab complex studies critical equipment for potential vulnerabilities. Continued support and appropriate scaling for the Energy Cyber Sense portfolio at the Department of Energy would be valuable to critical infrastructure owners and operators.

The government can also continue to support industry through education and training programs that help ensure the availability of skilled workers to meet both the buildout needed to serve rising data center power demand and the need for the engineers and cybersecurity professionals required to protect the grid of tomorrow.

Finally, strengthening the coordination and strategic direction between the Department of Energy and the Department of War will enhance the private sector's ability to deliver secure and reliable power to utility customers, including military installations and critical defense facilities.

2. Iowa State University is leading CyDERMS, a regional cybersecurity center focused on securing Distributed Energy Resources. As we integrate millions of new devices, we're dramatically expanding the attack surface of our grid. At the same time, we're deploying AI and machine learning tools to detect attacks and manage

these distributed systems. This creates a paradox: we're using high-tech AI solutions to secure increasingly complex systems, but that technology itself could be a vulnerability.

a. How do you think about this balance?

For the investor-owned community, reliability and security are core responsibilities. While AI can offer benefits to the grid and the systems that manage energy infrastructure, it must be integrated and used with careful deliberation to ensure reliability and security are not compromised. Building on existing risk management frameworks such as those from NIST and other established practices, energy companies are adopting AI where it can provide clear value, but with utmost caution and close attention to the protection of sensitive company and operational data and the reliable operation of the grid. The industry sees incredible promise in AI tools, and energy companies are using and will continue to use them, where tested and validated, to make the grid more reliable and secure.

b. Are there certain applications where simpler, lower-tech approaches might actually be more secure?

Complex technologies like AI can introduce risk, and therefore, in certain operational settings, simpler, lower-tech approaches may be more secure and appropriate. For example, forecasting is an area where AI is already being used, but AI grid operation is still in the research phase.

c. How do we ensure that the AI tools we're deploying to defend the grid don't become the vector for attack?

Like other technologies, AI is being tested and secured, evaluated for risk, and validated before integration. Currently, AI is being used as an assistance tool for analysts and operators, not to replace operator decisions or critical grid functions. Relying on existing frameworks and trusted best practices helps to ensure that technologies being used on the grid are strengthening reliability and security and not creating new attack surfaces.