Responses to Questions for the Record from Sharla Artz, on behalf of EEI and Xcel Energy

The Honorable Robert Latta (R-OH)

1. Access to information and technical fixes through E-ISAC or the threat analysis centers is critical.

a. Is it also essential to have internal programs and planning—a well trained workforce—to use this information effectively?

Access to timely threat intelligence and actions from the E-ISAC and threat analysis centers, like the ETAC, are essential, but they are not sufficient on their own. The value of that information depends on the sector's ability to operationalize it, which requires strong internal programs, planning, and a trained workforce.

Critical energy infrastructure owners and operators are defending daily against threats from a range of adversaries to safeguard the nation's essential services. The electric sector implements security risk mitigation programs and engages with government partners to create tools, technologies, and processes that improve visibility into critical control systems and enhance situational awareness and information sharing for emerging threats. Through the development of comprehensive plans, asset owners and operators are ready to respond and recover quickly when incidents occur.

At Xcel, all personnel—from cybersecurity analysts to control room operators to field technicians—must understand cyber risks and their potential impacts and are encouraged to build skillsets and learn through experience with stretch assignments, apprenticeships, and leadership opportunities. Xcel conducts regular exercises, provides risk-based strategies and tools, and focuses on continuous improvement to ensure the intelligence our analysts receive is translated into investments in resilience and protection of our most critical systems and assets.

EEI also supports electric companies in the development of a skilled, world-class workforce. The organization's "Culture of Security" initiative, led by investor-owned utility CEOs, fosters a proactive and comprehensive approach to ensure that security is embedded throughout organizations. Companies are encouraged to assess their security maturity, share best practices, and conduct peer reviews aiming to protect against evolving threats while maintaining a secure and resilient grid. Training programs can reduce the likelihood of breaches, minimize human error, and, overall, improve the security posture of an organization, making them an indispensable component of a comprehensive security strategy.

The Honorable Brett Guthrie (R-KY)

1. As we've discussed at length in the Committee this Congress, huge demand growth for electricity presents new risks to be managed by NERC, grid operators, and utilities of all sizes.

a. How do Xcel and EEI approach this issue?

Xcel is experiencing unprecedented load growth, but at the same time, we are committed to ensuring new large loads do not increase costs for existing customers, maintaining reliability, and balancing energy and water use. Xcel Energy expects to invest more than $60 billion within the next five years to strengthen and expand our energy infrastructure. The plan will include transmission and distribution system upgrades, new natural gas and renewable generation, and a modernized grid.

At the industry level, EEI and its member companies are pursuing a broad reliability and resource adequacy strategy that includes more than $1.1 trillion in projected grid investments by 2029, to include resilience and hardening, support for the domestic energy mix, streamlined permitting, and cost allocation guardrails to ensure large load customers pay their fair share while maintaining system reliability.

The Honorable Mariannette Miller-Meeks (R-IA)

1. Energy affordability and the dominance needed to win the AI race both rely on the availability of electrical equipment that allow the grid to function safely. The inability to procure parts is a significant threat to the grid; if a utility cannot procure a switchgear or a transformer or some other critical component, then the grid doesn't work. The supply chain for this electrical equipment is already under massive pressure to produce more products to meet unprecedented energy demand, and the constancy of massive, devastating wildfires nationwide threatens to add even more burden.

Over the past decade, the frequency and severity of wildfires has increased the legal exposure for domestic manufacturers of critical grid components by incentivizing plaintiffs to seek additional compensation from producers despite no fault being found with their products. This legal risk is putting our domestic supply chain in a serious dilemma: continue making safe, reliable, and badly needed products for the grid and still get sued when a wildfire happens, or stop providing products, go out of business, and leave utilities to source their products from China.

My bill, the Limiting Liability for Critical Infrastructure Manufacturers Act seeks to give domestic manufacturers much needed legal certainty. So instead of spending more and more capital on hedging frivolous legal risk, they can invest that money in hiring American workers and expanding facilities to make the products we all rely upon.

In June, a report from Stanford University entitled "Wildfire: An Updated Look at Utility Risk and Mitigation" noted that "an approach to wildfire mitigation which reduces the likelihood of electric infrastructure igniting catastrophic fires is key not only to protecting the safety of homes and communities threatened by fires, but also to the future development of the energy system."

a. Utilities need a reliable supply chain to obtain safe and secure products critical electrical equipment for their systems and keep costs low for their customers. Being able to quickly source this equipment and get these critical grid components is necessary for utilities to rebound from wildfires as well as to prevent them. Therefore, would you agree that utilities have an interest in ensuring their domestic grid component producers remain viable as part of national fire mitigation strategies? If yes, would that include providing liability protections to reduce unwarranted and costly litigation?

Utilities rely on a strong and reliable domestic supply chain to acquire the safe and secure electric equipment necessary to operate the grid and keep costs affordable. The ability to rapidly source transformers, switchgear, and other critical components is important to restoring service after an incident but also for implementing mitigations to reduce the risk to cyber and physical threats, like wildfires, in the first place. Targeted liability protections that would allow manufacturers to focus resources on expanding capacity and investing in innovation could help strengthen the reliability of the grid.

2. 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?

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. The ETAC analysts are working daily to connect industry data and context with government intelligence to reduce risk across the energy sector. These are analysts that understand grid operations and adversarial tactics are working together daily at the ETAC to exchange information, collectively analyze threats, and create actionable information for industry.

The E-ISAC is the broad information sharing and alerting body for the electricity sector. It distributes threat intelligence and mitigation guidance to utilities nationwide. The products the ETAC develops are shared through the E-ISAC with the entire sector to help raise awareness of potential threats and make defensive measures available

With the energy sector being the most critical of critical infrastructure, and on which all others rely, the ETAC is essential. The ETAC has more than demonstrated its value by delivering actionable guidance across the electric sector to address two of the most significant cyber threats the United States has faced this decade. Without it, energy infrastructure owners and operators would lose the central mechanism for fusing intelligence with real-world grid operations that enables them to deliver the insights, warnings, and mitigation strategies to protect national security and the reliability of the electric grid.