Testimony of

Stephen L. Swick

Chief Security Officer

American Electric Power

Before the Senate and Natural Resources Committee

Hearing on Cybersecurity Vulnerabilities to United States Critical Infrastructure

March 23, 2023

Good morning, Chairman Manchin, and Ranking Member Barrasso, members of the Committee and fellow panelists. My name is Stephen L. Swick, and I am the Chief Security Officer of American Electric Power (AEP) in which I am responsible for both physical and cybersecurity. I have led AEP cybersecurity for over 25 years. Prior to my time at AEP, I proudly served in the United States Air Force helping to establish initial cyber response capabilities in the U.S. with the Air Force cyber emergency response team (US-CERT), prior to the creation of U.S. Cyber Command.

AEP, headquartered in Columbus, Ohio, is one of the largest electric utilities in the United States, delivering electricity to more than 5.5 million customers in 11 states. AEP owns nearly 31,000 megawatts of generating capacity and delivers energy to customers over 40,000 miles of electric transmission lines - the nation's largest electricity transmission system.

Today's hearing on the steps needed to address cybersecurity vulnerabilities to the United States' energy infrastructure is part of an important conversation AEP and our industry partners have been having.

The United States energy infrastructure has a long history of facing threats, whether natural or man-made. Today's cyber threats are increasingly complex and dynamic requiring flexibility, creativity, and collaboration to address. To meet these ever-evolving challenges, AEP continues to prioritize cybersecurity through technology, collaboration, and a dedicated workforce enabling us to deliver safe, reliable, and resilient service to our customers. At AEP, we firmly believe that resilience begins with security, and security is resilience. Within the cybersecurity team we have been very fortunate to retain our talented staff while growing the program and attracting external talent as well. This has allowed us to continually mature our program to meet future demands.

Critical Infrastructure Threat Landscape

As noted in the recently released National Cybersecurity Strategy, malicious cyber activity has continued to evolve ranging from web defacements to intellectual property theft to

attacks intended to damage critical infrastructure.[1] Offensive cyber operations tools and services are now widely accessible to bad-actors of all types – from low-level criminals to nation-states. Nation-states leverage advanced capabilities to achieve their objectives through offensive cyber activity. The Ukrainian power outages from 2015, 2016 and 2022 are prime examples of how quickly vulnerabilities can lead to a significant incident. In the Office of the Director of National Intelligence Annual Threat Assessment it noted that nation-states are developing offensive cyber capabilities for the purpose of impacting critical infrastructure and particularly the electric power industry.[2] Other critical infrastructure industries, such as oil, water, and gas, face similar challenges from malicious cyber actors. To meet increasing security demands it is essential that all U.S. critical infrastructure and government partners work in concert to enhance and strengthen our defenses while quickly responding to restore service when issues arise.

Cybersecurity and Securing the Grid Today

The threat landscape is becoming increasingly dynamic. To best protect the electric grid, we must proactively identify threats, strategize how to shield against them and share relevant intelligence and mitigations across critical infrastructure to strengthen our defenses. Regardless of what we do to protect our own systems, we each are as strong as our weakest interconnected peer.

AEP recognizes that a strong foundation of security begins with secure products and technologies. As utilities across the nation integrate advanced technology to make the grid smarter and more resilient, we must remain vigilant to ensure the products and services we use are secure. Through a robust vendor review process AEP seeks out secure products and services that meet our architectural needs while offering capabilities that support risk reduction. There continue to be challenges to securing key technologies and components for the whole of the electric power industry. A robust supply chain with secure-by-design products will only become increasingly important as the entry points for attacks and vulnerabilities continue to evolve. Incentivizing the reshoring of production of certain critical grid equipment, like large power transformers, by the Federal government would be a supportive step to level the playing field for supply chain economics.

Strengthening grid security requires collaboration across the electric industry and close partnership with all levels of government. We must have unification between systems, regardless of who owns or controls those systems. The CEO-led Electric Subsector Coordinating Council (ESCC) is one venue where we continue to engage, coordinate, and share best practices to strengthen our collective security.

Access to reliable intelligence on threats to the sector in near-real time improves our ability to defend our networks and implement the necessary protections. Through the public-private program Cybersecurity Risk Information Sharing Group (CRISP), members provide and receive relevant and actionable cybersecurity information to speed defense. Working closely

[1] National Cybersecurity Strategy www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[2] Office of the Director of National Intelligence Annual Threat Assessment 2023 Annual Threat Assessment of the U.S. Intelligence Community (dni.gov)

with the Energy Information Sharing and Analysis Center (E-ISAC) and the Department of Energy Cybersecurity, Energy Security, and Emergency Response (CESER) office offers participants the benefit of DOE's expertise and leading indicators from peers. AEP is an active member of both the E-ISAC and ESCC consistently sharing relevant, timely intelligence to better protect and defend the grid.

Maintaining close ties with state governments in our service territory, AEP is committed to partnering with the public utility commissions and through the National Governors Association and the National Association of Regulatory Utility Commissioners. Security is a team sport and requires all members to contribute to better understand the threat landscape and meaningful mitigations to best protect the nation. Flexible, standards rooted in practical application of security lead to greater alignment across the industry to improve all of our defenses. Current Critical Infrastructure Protection (CIP) Standards established by the North American Electric Reliability Corporation (NERC) and enforced by the Federal Energy Regulatory Commission (FERC) create a flexible foundation that allows each electric company the opportunity to weave a set of solutions and protections that works best for their unique circumstances, including grid specifications, geography, and a host of other variables. Overly prescriptive regulations can hamper our ability to quickly respond to new threats and often make achieving the intended security objectives a challenge. Crafting standards and regulations with agility to address rapidly evolving threats and technologies employed is critical for achieving the intended outcome: a more secure and resilient grid.

Creating a More Secure, Reliable and Resilient Grid

As the National Cybersecurity Strategy details, vendor integrity and product security are key building blocks for any cyber defense and resilience program.[3] Encouraging vendors to focus on security by design and being first-to-security (rather than first-to-market) would enable members of the sector, regardless of size, to have a reasonable level of confidence in their security investments knowing the products were developed with security in mind.

Another means of encouraging more mature cyber hygiene and adoption of secure products could be incentivizing investments through the recent FERC notice of proposed rulemaking.[4] AEP recommended that the Commission establish a tiered cyber and physical resilience program with a return on equity (ROE) incentive that applies to an entity's transmission rate base that incentivizes investment in measures that provide additional security for the grid. An incentive for physical and cybersecurity will encourage the adoption by utilities of a robust, holistic, and long-term approach to address grid security challenges.

While existing collaboration opportunities are an excellent start, we will need to continue to grow the depth and breadth of our public-private partnerships to best address the threats of the future. Gaining access to classified and downgraded intelligence to meet threats head on empowers the electric power industry to protect and defend the service upon which our nation

[3] Office of the National Cyber Director National Cybersecurity Strategy 2023 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf p. 4.

[4] *Incentives for Advanced Cybersecurity Investment; Cybersecurity Incentives*, Notice of Proposed Rulemaking, 180 FERC ¶ 61,189 (2022)

relies. Developing collaboration spaces like the Energy Threat Analysis Center (ETAC) pilot program offer potential avenues for deepening this partnership. Rooted in our robust partnership with DOE CESER office, AEP looks forward to engaging in venues like ETAC as the program matures and expands.

Efficiency and effectiveness within our sharing channels requires harmony among regulations and reporting requirements. For utilities like AEP that provide services in several states, competing--and at times conflicting--requirements increase the burden of sharing and can slow progress. When competing regulations or reporting requirements exist it is incumbent upon AEP to meet the highest threshold, which often translates to increased cost. As the National Cybersecurity Strategy highlights 'harmonizing regulations' is a key priority for the future.[5] By looking for common standards and efficiencies in both regulations and reporting requirements we can achieve greater speed of communication, improved clarity of message and shared understanding of key issues or concerns alongside the ability to collectively respond with greater precision.

Beyond the philosophical considerations, we need to remember that the grid does not stop at the borders of each state, each NERC region, or even international boundaries. For companies like AEP – and many others – a separate set of requirements for each jurisdiction is not just cumbersome, it potentially could be counter-productive. Consistency in a unified, risk-based approach from coast to coast supports a risk-based approach to security and therefore to resilience.

We hope this is the start of a continued dialogue and I thank you for the opportunity to address you on these issues. I would be happy to respond to any questions.

[5] Office of the National Cyber Director National Cybersecurity Strategy 2023 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf p. 8.