STATEMENT OF SCOTT AARONSON, EDISON ELECTRIC INSTITUTE SENIOR VICE PRESIDENT, SECURITY AND PREPAREDNESS

JOINT FERC-DOE SUPPLY CHAIN RISK MANAGEMENT TECHNICAL CONFERENCE

DECEMBER 7, 2022

Thank you for the opportunity to speak at today's Supply Chain Technical Conference to discuss supply chain security challenges related to the Bulk-Power System, ongoing supply chain-related activities, and potential measures to secure the supply chain for the grid.

Edison Electric Institute is the association that represents all investor-owned electric companies in the United States. Our members provide electricity for more than 235 million Americans and operate in all fifty states and the District of Columbia. As a whole, the electric power industry supports more than seven million jobs in communities across the United States. EEI's member companies own and operate generation, transmission, and distribution facilities in regions in all areas of the country, both inside and outside of RTOs and ISOs. EEI member also are responsible for ensuring safe, reliable service and invest more than $120 billion annually to make the energy grid smarter, cleaner, more dynamic, more flexible, and more secure to provide affordable and reliable electricity to customers.

The pace of changes to the grid and the ever-evolving threat landscape will continue to challenge the effectiveness of the tools and processes used by electric companies, the Electric Reliability Organization, the Commission, and the Department of Energy (DOE), to address these risks. The need for coordination and information sharing among these stakeholders to

support grid reliability, resilience and security are imperative. In light of these considerations, innovative methods and strong partnerships are needed to address these changes and challenges. Collaboration among policymakers and regulators at the local, state, regional, and federal levels; customers; interdependent sectors; and electric companies are critical so that actionable information and intelligence can be shared, and solutions can be identified.

Improving supply chain security and developing enhanced risk mitigation measures are necessary steps to safeguard the Bulk-Power System. EEI members use a defense-in-depth philosophy that is prioritized, risk-based, and flexible such that it recognizes the unique threats individual electric companies face due to their system design and topology, customer base, and existing security controls, including mandatory Reliability Standards. The NERC Standards provide a solid foundation for strengthening the industry's supply chain and security posture. Reliability Standard CIP-013-1 requires electric companies to evaluate and address cybersecurity risks from vendor products and services during system planning and procurement. To comply with the standard, electric companies use their supply chain cyber security risk management plans in procurement processes (e.g., request for proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan). Importantly and appropriately, Reliability Standard CIP-013-1 does not require any specific controls or mandate "one-size-fits-all" requirements due to the differences in needs and characteristics of electric companies and the diversity of Bulk-Power System environments, technologies, and risks. Rather, the standard takes a flexible approach to allow responsible entities to establish organizationally defined processes that integrate a cybersecurity risk management framework into the system development lifecycle. To

aid in the development of standard contractual provisions, EEI and its members have developed *Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk* which is available publicly on the EEI website.

A critical issue that needs attention is the limited visibility vendors have into their own supply chains, particularly with respect to software, firmware, and digital subcomponents associated with the electric equipment they sell to electric companies. As a result, those vendors often cannot provide the information needed by electric companies to verify that their equipment does not contain risky components or subcomponents. Electric companies will continue to work with vendors to investigate and determine the identity of their component providers as much as possible. However, stakeholders, including electric companies, vendors and suppliers, need assistance from our federal regulatory and intelligence community partners to develop actionable and practical information regarding the specific nature of supply chain risks. Given that Bulk-Power System equipment has many discrete components, continued and actionable information sharing by government who has additional visibility and information on the nature of threats to national security, is needed to assist electric companies in identifying and addressing supply chain threats to our infrastructure.

It is imperative that solutions to mitigate supply chain risks consider potential impacts that may result from implementing broader, one-size-fits all methods due to the potential for long-lead times in equipment and software procurement. Enhancing supply chain security and developing improvements to risk mitigation measures are underway, but more work and collaboration between the industry and the government are needed. At the same time, any regulations or actions should avoid disrupting these established supply chains and markets and

incorporate cost considerations to minimize the financial impact on electric companies and their customers to ensure the continued reliability and affordability of the nation's energy supply.

Electric companies do not depend on the CIP standards alone to protect their systems against security threats. These set a baseline for security, but security programs are tailored to each company's unique operating and business environments to mitigate supply chain and security risk as threats and vulnerabilities change. Companies engage in multiple approaches and coordinate with the Electricity Information Sharing and Analysis Center ("E-ISAC"); federal agencies including DOE, FERC/NERC, Department of Homeland Security, the FBI, and intelligence community; and state (and where applicable, local) governments to identify and mitigate threats. Improving security of the Bulk-Power System supply chain requires a strong partnership among electric companies, vendors, policymakers, and regulators at all levels. This coordination is imperative to ensure alignment on the understanding of grid security to identify both appropriate and cost-effective priorities. Electric companies welcome and need additional information to identify and mitigate threats to critical electric infrastructure both in the supply chain for equipment used going forward and for equipment currently on the Bulk-Power System. Timely bi-directional sharing of actionable unclassified and, in some cases, classified threat information and using advanced collection, analysis, and dissemination tools to identify threat patterns and trends across the electric power industry are two critical approaches to reducing risk.

This information sharing may include the potential need for closed communication on national security threats. Robust and timely actionable information about the nature of threats when vulnerabilities are identified by the federal government and suppliers is a key and critical process that is needed to help electric companies react to and mitigate threats to the supply chain.

Therefore, it is important for government to think about critical infrastructure using the same risk-based, defense-in-depth philosophy used by electric companies to prioritize and protect the Bulk-Power System.

Public-private partnerships are, and will continue to be, essential to address certain cybersecurity and supply chain threats. Electric companies currently engage in information sharing and testing programs that identify threats and vulnerabilities and incorporation of indicators of compromise; participate in communities for sharing cyber, physical, and supply chain risks; and facilitate close coordination among industry and government partners at all levels, and through the Electric Subsector Coordinating Council in particular. Classified and unclassified information sharing protocols must continue to mature and remain flexible among government and industry to address threats to the Bulk-Power System in the evolving threat landscape. This should include sharing information regarding entities, vendors, or products that government agencies have identified as national security threats and, consequently, potential threats to the electric grid.

I appreciate the opportunity to participate in this technical conference as it provides a needed forum to discuss the critical issues associated with supply chain risk management. We look forward to collaborating in considering solutions that support our collective efforts to ensure continued reliability and security of the supply chain.