STATEMENT OF SCOTT I. AARONSON
SENIOR VICE PRESIDENT, ENERGY SECURITY & INDUSTRY OPERATIONS
EDISON ELECTRIC INSTITUTE

BEFORE THE U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

HEARING ENTITLED "REGULATORY HARM OR HARMONIZATION? EXAMINING THE OPPORTUNITY TO IMPROVE THE CYBER REGULATORY REGIME"

MARCH 11, 2025

Introduction

Chairman Garbarino, Ranking Member Swalwell, and members of the Subcommittee, thank you for the opportunity to testify. My name is Scott Aaronson, and I am Senior Vice President for Energy Security & Industry Operations at the Edison Electric Institute (EEI). EEI is the association that represents all U.S. investor-owned electric companies, which together are projected to invest more than $200 billion this year to make the energy grid stronger, smarter, cleaner, more dynamic, and more secure against all hazards. That includes cyber threats. EEI's member companies provide electricity for nearly 250 million Americans and operate in all 50 states and the District of Columbia. The electric power industry supports more than seven million jobs in communities across the United States. I appreciate your invitation to discuss this important topic on their behalf.

We rely on safe, reliable, affordable, and resilient energy to power our daily lives, run our nation's economy, and support national security. Today, demand for electricity is growing at the fastest pace in decades, creating challenges for our nation, as well as opportunities to ensure America is home to the industries, technologies, and jobs of tomorrow. America's investor-owned electric companies are uniquely positioned to meet growing demand and to address evolving risks, while working to keep customer bills as low as possible.

EEI's Comments on Cyber Regulatory Harmonization

The electricity subsector is a part of the energy sector that is designated by National Security Memorandum/NSM-22 as one of the 16 critical infrastructure sectors whose assets, systems, and networks are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, economic security, or public health and safety. The reliance of virtually all industries on electric power means that all critical infrastructure sectors have some dependence on the energy sector.

The electric subsector employs a risk-based, defense-in-depth approach to cybersecurity, including employing a variety of tools and strategies that support existing voluntary and

mandatory cybersecurity standards and regulations, both of which are valuable tools in ensuring the cybersecurity of critical infrastructure.

Throughout the country, investor-owned electric companies are meeting and exceeding existing cybersecurity regulations and standards. As the federal government, states, and private sector work together to reduce risk holistically and continue to enhance cybersecurity protections of critical infrastructure, it is important that new cybersecurity requirements are not duplicative, conflicting, overlapping, or inefficient. Regulations that include flexibility and support for resilience, response, and recovery can help electric companies protect the electric grid. We also need to have strong partnerships in place across key sectors and with government in order to maintain the robust cybersecurity posture needed to face the realities of potential cyber warfare.

In November 2023, EEI submitted comments on the Office of the National Cyber Director's (ONCD) Request for Information on Cybersecurity Regulatory Harmonization.[1] In summary, EEI's comments recognized that cybersecurity regulations must keep pace with the evolving threat landscape. Because industry owns, operates, and secures the majority of the energy grid, the federal government should incorporate industry's subject matter expertise in developing and implementing new regulations and streamline processes from which new regulations may emerge. EEI's comments also provided examples of cybersecurity regulatory conflicts, inconsistencies, redundancies, challenges, and opportunities. Some of the key points that EEI made include:

- Effective communication between government and industry is paramount to reconciling existing and future cybersecurity regulations;
- Harmonization is needed to address the high costs and inefficiencies caused by existing regulations or standards, or both;
- Harmonization efforts also must address third-party business partners;
- In addition to federal regulations, EEI members also are subject to (and must comply with) many state, local, tribal, and territorial cybersecurity requirements and standards; and,

[1] *Comment from Edison Electric Institute*, REGULATIONS.GOV, https://www.regulations.gov/comment/ONCD-2023-0001-0039 (November 1, 2023).

- Additional matters to help harmonize cybersecurity regulations, such as:
    - Voluntary information sharing and protection;
    - Privacy laws and regulations;
    - Information handling;
    - Cloud security;
    - Contract terms; and,
    - Government coordination.

EEI's Engagement on CIRCIA

While the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) is the first federal cybersecurity reporting requirement focused specifically on reporting across all 16 critical infrastructure sectors, electric companies have been subject to similar federal reporting for years pursuant to mandates imposed by the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), the Transportation Security Administration (TSA), and the Department of Energy (DOE). These existing reporting requirements should be considered by the Cybersecurity and Infrastructure Security Agency (CISA) as it determines how to implement its own cybersecurity and incident reporting regulations.

In May 2024, EEI had the opportunity to testify during this subcommittee's hearing entitled, "Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking."[2] EEI testified that one of our member electric companies estimated they could file roughly 65,000 reports through 2033 under the proposed rule — vastly exceeding CISA's estimate of more than 200,000 total reports during that period. In addition, our testimony highlighted that the Department of Homeland Security's (DHS) Cyber Incident Reporting Council (CIRC) report on harmonization identified that there currently are 45 different federal cyber incident reporting requirements

[2] *Statement of Scott Aaronson*, CONGRESS.GOV, https://www.congress.gov/118/meeting/house/117105/witnesses/HHRG-118-HM08-Wstate-AaronsonS-20240501.pdf (May 1, 2024).

administered by 22 federal agencies.[3] We recommended that CISA thoroughly explore opportunities to limit duplicative reporting through the "substantially similar" exception of CIRCIA, and through the establishment of CIRCIA Agreements with federal counterparts. EEI's testimony also identified several areas for enhancement of the proposed rule, including:

- Scope of substantial cyber incident definition;
- Volume of information requested;
- Workforce burden;
- Data preservation requirements; and
- Protection of information.

Following the hearing last May, EEI has continued to engage with CISA on CIRCIA. In July 2024, EEI submitted three sets of comments on the proposed rule. The first set of comments was sent on behalf of EEI's member electric companies and included feedback that was discussed in the May hearing, including:

- CISA's proposed definition of "substantial cyber incident" is too broad and therefore must be narrowed in scope;
- The amount of information required under the proposed rule is excessive, significantly increasing a covered entity's reporting burden while often contributing little analytical value;
- CISA must do all it can to protect reported information from threat actors and recognize its own limitations;
- The proposed rule's data-preservation requirements are unduly onerous;
- The proposed rule includes contrasting interpretations of the term "promptly" as it relates to the timeframe within which covered entities must submit supplemental reports;
- CISA's proposed marking requirements need clarifying; and
- Harmonizing existing and proposed cybersecurity requirements is vital.[4]

---

[3] *Harmonization of Cyber Incident Reporting to the Federal Government*, DHS.GOV, https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf (September 19, 2023).

[4] *Comment Submitted by Edison Electric Institute*, REGULATIONS.GOV, https://www.regulations.gov/comment/CISA-2022-0010-0452 (July 5, 2024).

The second set of comments was sent on behalf of the communications sector, electricity subsector, and financial services sector, encouraging CISA to limit the scope and raise the threshold for incident reporting by amending the definition of a substantial cyber incident in the final rule.[5] Cosigners of these comments included some of the most sophisticated critical infrastructure owners and operators across the United States, including the American Bankers Association, American Public Power Association, Bank Policy Institute, EEI, National Rural Electric Cooperative Association, NTCA—The Rural Broadband Association, Securities Industry and Financial Markets Association, and USTelecom—The Broadband Association.

The third set of comments was sent on behalf of more than 50 organizations seeking clarification on whether trade associations would be considered "covered entities" that are required to report cyber incidents to CISA under the proposed rule.[6] The uncertainty around the inclusion of associations, which serve members within critical infrastructure sectors—but which do not own or operate critical infrastructure—in the definition of a covered entity is just one example of the ways in which CISA's proposed rule is out of scope. These comments were intended to ensure CISA appropriately tailors reporting requirements to provide only the most relevant information necessary to protect homeland security.

Also in July 2024, subcommittee Chairman Andrew Garbarino,[7] subcommittee Ranking Member Eric Swalwell, full committee Ranking Member Bennie Thompson, Rep. Yvette Clarke,[8] as well as then-Senate Homeland Security and Government Affairs Committee Chairman Gary Peters,[9] submitted comments on the proposed rule. The feedback provided by Congress suggested that CISA mischaracterized or failed to meet the congressional intent of CIRCIA. Universally, congressional leaders have encouraged CISA to refine the scope of definitions and to meaningfully incorporate industry feedback in the final rule.

---

[5] *Comment Submitted by ABA, APPA, BPI, EEI, NRECA, NTCA, SIFMA, USTelecom*, REGULATIONS.GOV, https://www.regulations.gov/comment/CISA-2022-0010-0254 (June 28, 2024).
[6] *Comment Submitted by National Association of Manufacturers and 50 other trade associations*, REGULATIONS.GOV, https://www.regulations.gov/comment/CISA-2022-0010-0320 (July 3, 2024).
[7] *Comment Submitted by Congressman Andrew R. Garbarino*, REGULATIONS.GOV, https://www.regulations.gov/comment/CISA-2022-0010-0464 (July 9, 2024).
[8] *Comment Submitted by CHS – Ranking Member Bennie G. Thompson, Ranking Member Eric Swalwell, Rep. Yvette Clarke*, REGULATIONS.GOV, https://www.regulations.gov/comment/CISA-2022-0010-0463 (July 9, 2024).
[9] *Comment Submitted by Homeland Security and Government Affairs Committee*, REGULATIONS.GOV, https://www.regulations.gov/comment/CISA-2022-0010-0424 (July 3, 2024).

Finally, in October 2024, EEI, along with more than 20 organizations, sent a letter to CISA regarding the status of CIRCIA implementation, specifically requesting the establishment of an ex parte process to enhance stakeholder engagement and facilitate ongoing dialogue for its implementation.[10] The letter urged CISA to:

- Adopt an ex parte process for ongoing stakeholder engagement;
- Narrow the scope of CIRCIA to enable a positive cycle of information sharing and actionable insights;
- Proactively harmonize CIRCIA implementation with existing regulatory requirements to optimize operational response; and,
- Strengthen safeguards for information and protections against liability to support cyberattack victims and foster candor in reporting.

To date, CISA has not established an ex parte process and the status of the remaining recommendations remains unknown.

Opportunities for CIRCIA and Recommendations for Congress

Nearly a year after this subcommittee's hearing and EEI's testimony on CIRCIA, we are in a period of transition with a new Administration and a new Congress. Change brings opportunity—and I urge this subcommittee to leverage this opportunity to help CISA improve implementation of CIRCIA.

As we stated in our comments on the proposed rule, EEI and its members wholly endorse the policy objectives underpinning CIRCIA. CIRCIA is an important law with an important goal of identifying and mitigating cyber risks across all sectors of the economy, and I appreciate this committee's leadership in shepherding this effort forward these last several years. When CIRCIA was enacted, Congress emphasized that the legislation sought to strike a balance between enabling CISA to receive information quickly and allowing the impacted entity to respond to an attack without imposing burdensome requirements. Details matter when it comes to how

[10] *Cross-sector Letter on CIRCIA Implementation*, CYBERSCOOP.COM, https://cyberscoop.com/wp-content/uploads/sites/3/2024/10/10.29.24-Cross-sector-Letter-on-CIRCIA-Implementation68.pdf (October 29, 2024).

CIRCIA, or how any mandatory cyber incident reporting regime, is implemented. We need our most skilled cyber experts to be spending the majority of their time protecting America's critical infrastructure, not filling out paperwork.

When evaluating how best to proceed, I encourage Congress to consider that:

- A final CIRCIA rule could help mitigate attacks and the disruptions they cause to American individuals and businesses. Therefore, improving the existing proposal and finalizing the rule by the fall 2025 deadline, as mandated by statute, may be preferable to issuing a new proposed rule. A new proposal may cause confusion and unnecessary delays, as well as increase costly paperwork for both covered entities and the federal government.
- CISA faces several challenges in improving the existing proposal to better align with congressional intent. These include difficulties in collaborating with industry stemming from the lack of an established ex parte process, as well as issues related to natural attrition and staff turnover following the change in Administration. Additionally, uncertainty around congressional appropriations may impact CISA's ability to effectively intake incident reports by the end of 2025.

Recommendations for Congress:

1. Conduct oversight regarding the current status of CIRCIA, including staffing levels, resource needs, the projected timeline for final rule completion, and anticipated future engagement with industry stakeholders.
2. Facilitate coordination amongst congressional committees of jurisdiction to:
    a. Ensure alignment between CISA, Sector Risk Management Agencies, and other regulators, confirming that CIRCIA Agreements are developed in compliance with the law's substantially similar reporting exception; and
    b. Review concerns with existing federal reporting requirements, including the national security concerns associated with the public disclosure of incidents required by the U.S. Securities and Exchange Commission.

3. Further clarify CISA's role in cybersecurity regulatory harmonization in relation to other federal entities, such as DHS and ONCD; and assess the next steps for the CIRC at DHS, as well as the legislative proposals recommended by CIRC in its harmonization report.
4. Reauthorize the *Cybersecurity Information Sharing Act of 2015 (CISA 2015)*, a pivotal law that encourages and protects cyber threat information sharing between the government and the private sector. While CISA 2015 is more about information sharing than incident reporting, both are essential to strengthening our collective cyber defenses to meet the evolving threat landscape.

Conclusion

Thank you again to this Committee for holding today's hearing and for your ongoing efforts to strengthen America's energy security. EEI's member companies are committed to working with federal partners and stakeholders across all sectors to achieve cyber regulatory harmonization that prioritizes and enhances U.S. critical infrastructure security. We appreciate the bipartisan support of this committee in ensuring we get CIRCIA right and we look forward to continuing our collaboration to protect the safety, security, and well-being of all Americans.