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

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

HEARING ENTITLED "SURVEYING CIRCIA: SECTOR PERSPECTIVES OF THE NOTICE OF PROPOSED RULEMAKING"

MAY 1, 2024

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 Security and Preparedness at the Edison Electric Institute (EEI). EEI is the association that represents all U.S. investor-owned electric companies. 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. EEI's member companies invest more than $150 billion annually to make the energy grid stronger, smarter, cleaner, more dynamic, more flexible, and more secure against all hazards, including cyber threats. I appreciate your invitation to discuss this important topic on their behalf.

The energy grid powers our way of life and is critical to America's security and economic competitiveness. Today, demand for electricity is growing dramatically across the economy to support evolving customer needs, as well as critical technologies like artificial intelligence and the proliferation of data centers that connect our digital lives. Ensuring a secure, reliable, resilient energy grid is a responsibility that EEI's member companies and the electricity subsector take extremely seriously.

Threat Landscape

For years, the U.S. intelligence community has warned of the potential for malicious nation-state exploitation of U.S. critical infrastructure. Today, we know from our federal partners that People's Republic of China state-sponsored cyber actors known as Volt Typhoon have compromised multiple U.S. critical infrastructure providers with the intent of disrupting operational controls, including in the energy sector.[1] With the increasingly complex geopolitical threat landscape and the sophistication of ransomware operations by transnational organized

[1] *CISA and Partners Release Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance*, CISA.GOV, https://www.cisa.gov/news-events/alerts/2024/02/07/cisa-and-partners-release-advisory-prc-sponsored-volt-typhoon-activity-and-supplemental-living-land (February 7, 2024).

criminals, we have seen an uptick in threats to critical infrastructure organizations across all sectors. These threats are a stark reminder of the need to continue to harden U.S. critical infrastructure.

Critical infrastructure security is a shared responsibility and a national imperative. While most critical infrastructure is owned by the private sector, government at all levels can and must play a role in protecting it, especially when it comes to defending against nation-state actors. Cyber incident reporting may support government efforts to protect U.S. critical infrastructure by creating visibility into cross-sector cyber risk, but reporting also should be supplemented with federal support to mitigate risk and harden the critical infrastructure assets that are vital to national security.

Harmonization of Federal Cyber Incident Reporting

EEI recognizes the Committee's intent in passing the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) was to enhance and to standardize cyber incident reporting to improve the federal government's visibility into cyber threats and to allow the government to share information quickly with critical infrastructure owners and operators across all 16 sectors. According to the Cyberspace Solarium Commission, prior to the passage of CIRCIA, the federal government lacked a mandate to collect cyber incident information reliably, systemically, and at the scale necessary to differentiate campaigns from isolated incidents and to support the development of more generalized conclusions.[2] However, it is important to note that the Cybersecurity and Infrastructure Security Agency's (CISA's) new cyber incident reporting requirements are being developed among an existing patchwork of federal and state incident reporting requirements. Harmonization is paramount.

As part of CIRCIA's mandate, the Department of Homeland Security's (DHS's) Cyber Incident Reporting Council (CIRC) issued a report on harmonization of cyber incident reporting to the federal government. That report identified several key findings, including that there are currently

[2] *Cyberspace Solarium Commission Report*, CYBERSOLARIUM.ORG, https://cybersolarium.org/march-2020- csc-report/march-2020-csc-report/ (March 2020).

45 different federal cyber incident reporting requirements administered by 22 federal agencies.[3] Given this context, CISA should thoroughly explore opportunities with federal counterparts to limit duplicative reporting through the "substantially similar" exception of CIRCIA. This exception includes "when a covered entity reports substantially similar information in a substantially similar timeframe to another Federal agency pursuant to an existing law, regulation, or contract when a CIRCIA Agreement is in place between CISA and the other Federal agency."[4] Accounting for and leveraging these existing incident reporting requirements should be a priority for CISA.

Electricity Subsector Cyber Incident Reporting

While the CIRCIA proposed regulations are the first federal cybersecurity requirements focused specifically on reporting across all critical infrastructure sectors, the electricity subsector has been subject to similar reporting to other federal entities for years, including through the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards and the U.S. Department of Energy (DOE) Electric Emergency Incident and Disturbance Report OE-417 form. EEI appreciates CISA's commitment to working with DOE, the Federal Energy Regulatory Commission (FERC), and NERC to explore the applicability of the proposed rules' substantially similar reporting exception to enable entities subject to CIRCIA and either or both the CIP Reliability Standards or Form OE–417 requirements to be able to comply through the submission of a single report to the federal government.

Pursuant to the Federal Power Act and through FERC oversight, the electricity subsector is subject to NERC's CIP Reliability Standards that cover cyber and physical security requirements, including CIP–008–6: Cyber Security—Incident Reporting and Response Planning. Entities found in violation of CIP standards face penalties that can exceed $1 million

[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] *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements Proposed Rule*, GOVINFO.GOV, https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf (April 4, 2024).

per violation per day. These mandatory standards continue to evolve using the process created by Congress to allow for input from subject matter experts across the industry and government.

DOE's Office of Cybersecurity, Energy Security, and Emergency Response also requires certain energy sector entities to report certain cybersecurity incidents to DOE pursuant to 15 U.S.C. 772(b). As the energy sector's sector risk management agency (SRMA), DOE uses Form OE–417 to collect information from the electricity subsector relevant to DOE's overall national security and National Response Framework responsibilities.

In July 2023, the Securities and Exchange Commission (SEC) adopted rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. In addition to cyber incident reporting through NERC, DOE, and the SEC, EEI member companies now also will be subject to CIRCIA's reporting requirements once implemented through CISA's final rule. EEI has expressed concerns with the public disclosure of a cyber incident through the SEC rules, especially before the incident is mitigated, and we value Chairman Garbarino's leadership on this issue. Public reporting provides details on vulnerabilities and attack vectors that may become a useful roadmap for malicious actors. This may make the entity, and others, a target for ongoing or similar attacks.

The SEC, CISA, and all other federal regulators must recognize the inherent sensitivity of and the need for protection of information regarding cybersecurity, including the risks associated with cybersecurity incident disclosure, and must allow reasonable flexibility regarding the governance of cybersecurity.[5] EEI appreciates the SEC's willingness to include a national security or public safety delay for disclosure, but more must be done to harmonize federal reporting requirements and to limit disclosure of sensitive cyber incidents that may provide insights to adversaries. While the introduction of public reporting through the SEC rules following the passage of CIRCIA runs counter to the CIRC harmonization report's recommendations and the National Cybersecurity Strategy's intent, EEI remains committed to

[5] *Edison Electric Institute Comments on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, SEC.GOV, https://www.sec.gov/comments/s7-09-22/s70922-20128366-291140.pdf (May 9, 2022).

working with government partners to streamline and to harmonize federal cyber incident reporting.

In addition to these mandatory incident reporting requirements, the industry also uses voluntary cybersecurity standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, DOE's Cybersecurity Capability Maturity Model (C2M2), and, most recently, DOE's Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources (DER) that are being developed in partnership with state regulatory bodies through the National Association of Regulatory Utility Commissioners (NARUC).

Through these standards and voluntary regimes, the U.S. energy grid benefits from a baseline level of security. While these standards are important, regulations alone are insufficient given the dynamic threat environment, and they must be supplemented by industry-government partnerships and coordinated response and recovery efforts. The electric power industry appreciated the chance to contribute to the drafting of the proposed rule through sector-specific listening sessions and through comments to CISA's request for information. The industry aims to continue this collaborative partnership to harmonize reporting requirements and to reduce the burden on covered entities in the energy sector.

Areas for Improvement in the Proposed Rule

This Committee left the definitions of a covered entity, cyber incident, covered cyber incident, and substantial cyber incident up to the rulemaking process to allow for industry input on the definitions included in the proposed rule. The electric power sector is grateful for the chance to partner with CISA and DOE as our SRMA to focus the scope and scale of these definitions in a way that prioritizes both security and operational continuity, as well as transparency for the public, policymakers, and other sectors.

EEI joined several other critical infrastructure organizations in requesting an additional 30 days to analyze the lengthy proposal sufficiently, to determine the potential impacts to the energy sector, and to ensure harmonization between existing and other developing reporting

requirements.[6] Additional time will allow our industry to develop thoughts on areas for improvement in the proposed rule. EEI is presently working closely with its member companies in this regard, but we preliminarily have identified the following opportunities for enhancement:

1. Scope of substantial cyber incident definition;
2. Volume of information requested;
3. Workforce burden;
4. Data preservation requirements;
5. Protection of information.

1. Scope of Substantial Cyber Incident Definition

CISA is proposing to define the term "covered cyber incident" to mean a "substantial cyber incident." Under CIRCIA, covered entities would be required to report a substantial cyber incident, including "unauthorized access to a covered entities' information system or network, or ***any*** nonpublic information contained therein, that is facilitated through or caused by either a compromise of a cloud service provider, managed service provider, other third-party data hosting provider, or a supply chain compromise."[7] The inclusion of "***any*** nonpublic information" and "third-party data hosting provider or a supply chain compromise" in this definition is very broad, which may result in CISA receiving far more incident reports than it is capable of triaging.

Unfortunately, the unauthorized access to ***any*** nonpublic information is a common occurrence in the United States. In 2023 alone, there were 3,205 known compromises, more than 1,400 public data breach notices, and more than 353 million total victims.[8] In addition, the exploitation of the MOVEit vulnerability in 2023 exemplified the impact a supply chain compromise can have. During this event, 102 entities were impacted directly, however, "1,271 organizations were indirectly affected when information stored in or accessed by a MOVEit product or service was

[6] *Joint Trades Letter Requesting an Extension on CIRCIA Comments*, USCHAMBER.COM, https://www.uschamber.com/security/cybersecurity/joint-trades-letter-requesting-an-extension-on-cisa-comments (April 5, 2024).
[7] *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements Proposed Rule*, GOVINFO.GOV, https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf (April 4, 2024).
[8] *2023 Was the Worst Year Yet for Data Breaches in Every Way—Except One*, PCMAG.COM, https://www.pcmag.com/articles/2023-was-the-worst-year-yet-for-data-breaches (February 26, 2024).

compromised via a vendor."[9] Therefore, it may be more appropriate for CISA to require reports from third-party service providers who disclose non-public information, rather than require reports from the companies themselves that are the victims of the disclosure of non-public information. As CISA has championed in its Secure by Design initiative, the onus should be on the producers and developers of products, rather than on consumers and end users.[10] EEI recommends that CISA consider scaling back this definition to cover only the most risky and impactful incidents. This also may help CISA prioritize resources and mitigations for those incidents that rise to a higher threshold.

2. Volume of Information Requested

The proposed rule estimates CISA will receive 210,525 CIRCIA reports through 2033, at a cost of $1.2 billion for the government and $1.4 billion for industry. Given the total number and cost of reports expected, EEI recommends that CISA reconsider the volume of information it is requesting from covered entities.

As mentioned, the electricity subsector already is required to report cyber incidents through NERC, DOE, and the SEC. As the sector's statutorily designated Electric Reliability Organization and SRMA, respectively, NERC and DOE have the sector-specific expertise necessary to process the content of energy sector cyber incident reports. In contrast, a recent report by the U.S. Government Accountability Office found that CISA has insufficient staff with the requisite operational technology skills, including a lack of threat hunting and incident response expertise in the energy sector.[11] Both CISA and industry would benefit from the development and implementation of reporting requirements that would result in the production of a manageable amount of information for all affected parties. To this end, it may be advisable for CISA to consider reviewing the type of information requested by NERC CIP–008–6 and OE-

[9] *2023 Data Breach Report*, IDTHEFTCENTER.ORG, https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/ (January 25, 2024).
[10] *Secure by Design*, CISA.GOV, https://www.cisa.gov/securebydesign (April 2024).
[11] *Cybersecurity Improvements Needed in Addressing Risks to Operational Technology*, GAO.GOV, https://www.gao.gov/assets/d24106576.pdf (March 2024).

417, respectively, to help it formulate reporting requirements that are not unduly burdensome for either CISA or industry but that comply with CIRCIA's information-reporting requirements.

EEI also has concerns with CISA's ability to obtain the resources necessary to triage the volume of information it proposes to request. The DHS FY24 budget request included $98 million[12] for CIRCIA for the staffing, processes, and technology necessary for successful implementation; however, the final FY24 appropriations package included just $73.9 million, $23 million below the request.[13] Despite the $116 million requested for CIRCIA in FY25, EEI remains concerned with CISA's ability to have the mechanisms in place to handle the information it is requesting from covered entities appropriately.[14]

3. Workforce Burden

As this Subcommittee has explored, the national cybersecurity workforce shortage is a major challenge across all critical infrastructure sectors. With more than 448,000 cybersecurity job openings in the U.S., the energy sector is no exception to this challenge.[15] The volume and content of the required CIRCIA reports will create a significant burden for the energy sector's cybersecurity workforce. EEI recommends CISA consider reducing this burden by prioritizing the implementation of interagency information sharing agreements and by ensuring submission requirements are similar to the industry's submission requirements for NERC CIP-008 and OE-417. A 2018 DOE Multiyear Plan for Energy Sector Cybersecurity found that federal incident reporting guidelines were driven by compliance more than process improvement and that coordination among reporting mechanisms could be valuable.[16] The need to focus on requirements that are outcome-based rather than compliance-based remains necessary to reduce the workforce burden of reporting multiple times to the federal government.

---

[12] *FY 2024 Budget in Brief*, DHS.GOV, https://www.dhs.gov/sites/default/files/2023-03/DHS%20FY%202024%20BUDGET%20IN%20BRIEF%20%28BIB%29_Remediated.pdf (April 2023).
[13] *Division C—Department of Homeland Security Appropriations Act, 2024*, HOUSE.GOV, https://docs.house.gov/billsthisweek/20240318/Division%20C%20Homeland.pdf (March 2024).
[14] *FY 2025 Budget in Brief*, DHS.GOV, https://www.dhs.gov/sites/default/files/2024-03/2024_0311_fy_2025_budget_in_brief.pdf (April 2024).
[15] *Cybersecurity Supply/Demand Heat Map*, CYBERSEEK.ORG, https://www.cyberseek.org/heatmap.html (April 2024).
[16] *Multiyear Plan for Energy Sector Cybersecurity*, ENERGY.GOV, https://www.energy.gov/ceser/articles/doe-multiyear-plan-energy-cybersecurity (March 2018).

4. Data Preservation Requirements

The proposed rule requires that, regardless of whether a covered entity submits a CIRCIA Report or is eligible for an exception from reporting, it must preserve data and records related to the covered incident or ransom payment for no less than two years from the date of submission or the date the submission would have been required. The proposed rule estimates data preservation costs to total more than $306 million, which is the largest category of costs following the initial familiarization costs of implementation. EEI recommends that CISA consider reducing the proposed data-retention threshold to help ease costs and, instead, should allow those resources to be leveraged for security mitigation measures.

5. Protection of Information

The current cyber threat landscape proves that no entity, public or private, is immune to cyber risk. In fact, CISA itself recently identified a threat actor's exploitation of two of its key systems, the Infrastructure Protection Gateway and Chemical Security Assessment Tool.[17] Upon finalization and implementation of CISA's CIRCIA regulations, the cyber incident reporting information for all 16 critical infrastructure sectors will be in the possession of one federal agency, CISA, thereby making it an extremely attractive, high-value target. Given this reality, it is imperative that any information entrusted to CISA be protected sufficiently from cyber threat actors.

Conclusion

Thank you again for holding this hearing. The electricity subsector and EEI's member companies are committed to advancing our strong cybersecurity posture and remain committed to working with both public and private partners across all sectors to comply with incident reporting requirements in a way that prioritizes and enhances critical infrastructure security. We appreciate the bipartisan support that cybersecurity legislation historically has enjoyed in this Committee

[17] Kapko, Matt, *CISA Attacked in Ivanti Vulnerabilities Exploit Rush*, CYBERSECURITYDIVE.COM, https://www.cybersecuritydive.com/news/cisa-attacked-ivanti-cve-exploits/709893/ (March 11, 2024).

and the work that you have done to enhance the energy sector's cybersecurity posture. We look forward to working together to continue to bolster critical infrastructure security and resilience for the safety, security, and well-being of all Americans.