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).

Testimony by Ari Schwartz

On Behalf of the

Cybersecurity Coalition

Before the

United States House of Representatives

Homeland Security Committee

Cybersecurity and Infrastructure Protection Subcommittee

on

"Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime"

March 11, 2025

INTRODUCTION

Thank you, Chairman Garbarino, Ranking Member Swalwell, and Members of the Subcommittee for inviting me to appear before you today. It is an honor to be here to discuss the critical importance of harmonizing cybersecurity regulations.

My name is Ari Schwartz, and I am the Coordinator of the Cybersecurity Coalition, the leading policy coalition representing companies that develop cybersecurity products and services.[1] In

[1] Cybersecurity Coalition is dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies. We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices, information sharing, and voluntary standards

my role, I focus on advancing efforts related to regulatory harmonization, ensuring that cybersecurity laws and standards are streamlined, effective, and efficient for businesses and the public sector alike.

Over the past 20 years, Congress has made significant efforts to ensure our Nation is protected without also overburdening the companies that run our critical infrastructure. Between 2011 and 2015, Congress debated legislation that would have centralized control of critical infrastructure protection regulatory efforts and instead, chose to leave the majority of the control to each sector's existing regulators. Congress decided that the sectors had inherent differences – including terminologies and requirements – and therefore needed to maintain separate regulatory regimes.

Meanwhile, efforts to address the evolving cyber threat landscape have prompted the development of new sector-specific and cross-sector requirements. These requirements apply not only within the private sector but also across all levels and branches of government, both in the U.S. and around the world. While necessary to secure our Nation's critical infrastructure and systems, these requirements have also resulted in a complicated, fragmented, and duplicative regulatory regime. This has created undue burdens and pressures for critical infrastructure owners and operators, making compliance both difficult and time-consuming. For example, companies face continuous updates to mapping exercises for various compliance regimes. Keeping pace with the flood of rulemaking and industry feedback opportunities requires resources: time, tracking tools, consultants, security leaders' input, and more. It is simply not a good use of limited security resources.[2]

Cyber Incident Reporting

One area where the burden of regulatory requirements on companies unquestionably continues to grow is around cyber incident reporting.

---

throughout the global community. Our members include Broadcom, Cisco, Cybastion, Google, Infoblox, Intel, Kyndryl, Microsoft, Palo Alto Networks, Rapid7, RedHat, Schneider Electric, Tenable, Trellix, Wiz and Zscaler.

[2] During the last Administration, several important steps were taken to address this issue:

The White House Office of the National Cyber Director (ONCD) launched an initiative to review cybersecurity regulations, gathering input from stakeholders.
Request for Information Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations, Office of the National Cyber Director, 88 Fed. Reg. 55694, Aug. 16, 2023, https://www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf.

Senators Peters and Lankford introduced the Streamlining Federal Cybersecurity Regulations Act, which sought to establish an ONCD-led process for developing a harmonized regulatory framework and review new regulations for alignment.
S.4630, Streamlining Federal Cybersecurity Regulations Act, 118th Cong., https://www.congress.gov/bill/118th-congress/senate-bill/4630.

Meanwhile, across the Atlantic, the European Union has acknowledged that its cybersecurity rules have created overlap and burden and is looking to streamline existing regulations, reduce administrative burdens and ensure a more cohesive approach to cybersecurity. https://commission.europa.eu/law/law-making-process/better-regulation/simplification-and-implementation_en

In many ways, incident reporting is a perfect demonstration of the broader issue. Governments continue to seek ways to utilize incident data to quickly spot patterns of incidents and respond to them. In order to get that information, there are increasing requests and requirements for more detailed incident response data to be sent to a growing number of organizations.[3] As more organizations build reporting structures for different purposes, duplication, misalignment, fragmentation, and other issues start to set in. This includes concerns around the amount and types of data fields, differing taxonomies, timeframes for reporting, and more.

Harmonizing cyber incident reporting would bring benefits to both public and private sector efforts to strengthen cybersecurity. It would improve coordination and response capabilities, enhance data quality, accelerate threat detection and mitigation, and enable more effective policymaking and resource allocation.

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)[4] was enacted in 2022, requiring critical infrastructure owners and operators to report cyber incidents and ransomware payments to the Cybersecurity and Infrastructure Security Agency (CISA). CISA formally solicited input from industry to inform this reporting structure, including which entities should report and what type of data should be reported.

The Cybersecurity Coalition is generally supportive of CIRCIA's objectives, and we acknowledge that CISA was given a difficult task to develop a reporting regime that encompasses all critical infrastructure sectors. Congress specifically required CISA to prioritize harmonization efforts to "avoid conflicting, duplicative, or burdensome requirements" across the sectors. In its proposed rulemaking, we do not believe CISA met this essential goal.[5] In particular:

- **Lack of Sectoral Engagement –** CISA did not adequately engage in working with the critical infrastructure sectors to discuss how to best harmonize existing efforts. In particular, despite the explicit mention of the need for "coordination" with the Critical Infrastructure Partnership Advisory Committee (CIPAC) and information sharing and analysis organizations in CIRCIA, CISA included almost no means of ex-parte engagement for them. The Cybersecurity Coalition believes that CISA should immediately begin meeting with the Sector Coordinating Councils under the CIPAC and the members of the Council of Information and Sharing and Analysis Center in a coordinated ex-parte process that Congress intended.

[3] The 2023 Department of Homeland Security Congressional Report, Harmonization of Cyber Incident Reporting to the Federal Government, "identified 45 different Federal cyber incident reporting requirements created by statute or regulation" being "administered by 22 Federal agencies", with another "seven proposed rules that would create a new reporting requirement or amend a current requirement, and five additional potential new requirements or amendments under consideration but not yet proposed."
https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf

[4] PL 117-103 Title V, Div Y

[5] Proposed Rule Cyber Incident Reporting for Critical Infrastructure Act Reporting Requirements, Cybersecurity and Infrastructure Security Agency, 89 Fed. Reg. 23644, Apr. 4, 2024, https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements.

CISA should also work more closely with the Office of Management and Budget and other federal agencies to facilitate reciprocity and harmonization to streamline incident reporting under CIRCIA's statutory language. This includes promoting greater collaboration between DHS; federal agencies; state, local, tribal, and territorial (SLTT) agencies; as well as international partners.

- **Overbroad Scope** – In its definition of "covered entities," rather than relying on existing definitions or trying to coordinate among existing efforts, CISA decided to create a complex new definition. It has two categories: those within critical infrastructure sectors, with exceptions for small businesses and those meeting sector-specific criteria.[6] In many cases, it may not be immediately clear whether an entity is covered by the proposed reporting requirements but because the requirements focus on size rather than what the company actually does, it almost certainly covers companies who have probably never before been considered "critical infrastructure." We do not think that this was Congress' intent.

  Also, mixing the broad scope of covered entities with a very broad definition of "covered cyber incidents," the Cybersecurity Coalition is concerned that this rule may lead to an overwhelming number of incident reports. [7] This influx of less relevant reports could burden CISA's incident reporting system, requiring significant additional resources for analysis, triage, and transformation into actionable intelligence. While the goal of CIRCIA is to ensure enough data is provided to create a comprehensive picture to inform policy and response actions, we believe that there is a point where too much data creates unnecessary noise that distracts from the core mission. CISA should prove they can effectively work with the enormous influx of data we'd expect they would receive using the existing construction of critical infrastructure and with a more modest definition of types of reports requested before considering expanding their scope.

  The Cybersecurity Coalition believes that CISA should narrow the scope of "covered entities" under CIRCIA. Instead of applying reporting requirements to all entities within critical infrastructure sectors, Congress should direct CISA to "focus on Systemically Important Entities (SIEs) that own or operate critical infrastructure systems and assets whose disruption would have a debilitating, systemic, or cascading impact on national security, the economy, public health, or public safety."[8] This would help Congress uphold its original intent to focus on the most essential infrastructure while avoiding unnecessary regulatory burden on less critical entities.

---

[6] 89 Fed. Reg 23644, 23660.

[7] Cybersecurity Coalition Comments, Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act, June 28, 2024, https://cdn.prod.website-files.com/660ec3caef47b817df2800ae/6684487fa6bfce5ed0c2a12a_Cybersecurity%20Coalition%20-%20FINAL%20Comments%20to%20CISA%20re%20CIRCIA%20Proposed%20Rule%206.28.24%20(2).pdf.

[8] Cybersecurity Coalition Comments, Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022, Nov. 14, 2022, https://cdn.prod.website-files.com/660ec3caef47b817df2800ae/660ec3caef47b817df280233_Comments%20CISA%20CIRCIA%20RFI%20-%20Docket%20Number%202022-19551%20-%20CISA-2022-0010%2011.14.22.pdf.

- **Failure to Streamline Reporting –** The proposed rule lacks clear measures to streamline reporting processes. Although the idea of "substantially similar" reporting requirements could help address duplicative reporting across different frameworks, the definition of "substantially similar" remains unclear. The proposed rule requires CISA and relevant agencies to establish a "CIRCIA Agreement" to ensure their reporting requirements align with this standard. However, CISA retains the authority to limit exceptions for substantially similar reports to agencies with formal agreements. The Cybersecurity Coalition is concerned that this broad and prescriptive approach could reduce reciprocity and create additional burdens for entities striving to align with these standards.[9]

  The Cybersecurity Coalition believes that CISA should support efforts to streamline federal cybersecurity regulations to ensure businesses are not burdened by multiple, conflicting obligations. By passing legislation that promotes the development of standardized incident reporting processes, Congress can make it easier for companies to comply with regulatory requirements while limiting agency overreach.

The Cybersecurity Coalition would prefer to see CISA issue a new version of the proposed rule that addresses these concerns and then receive comments on that draft and issue a final rule in the timeframe originally proposed by Congress. Unfortunately, Secretary Noem has now reportedly disbanded the CIPAC,[10] which will make getting comments from all of the sectors much more difficult. We hope the Secretary will reinstate the CIPAC. If not, in order to effectively receive feedback, it will likely be necessary for CISA to simply rescind the rule and start over. This would be a disappointing outcome considering the amount of time already expended on this effort and the fact that CISA would likely miss Congress' intended timeline.

The Cybersecurity Information Sharing Act of 2015

While we are discussing the importance of using data to address and prevent cyber incidents, I would be remiss not to mention the importance of the Cybersecurity Information Sharing Act of 2015 (CISA 2015).[11] CISA 2015 provides companies liability protections when sharing a very narrowly defined set of cyber threat information.

We can think of CISA 2015 as lowering the burden on organizations by simplifying the way that companies share information amongst other companies and with the government and the purposes of that sharing. While CISA 2015 was somewhat controversial at the time of its creation, it has been anything but controversial in practice. CISA should be commended for the fine job they did with the Department of Justice in creating the complicated guidance necessary for CISA 2015.

[9] *Id.*
[10] https://subscriber.politicopro.com/newsletter/2025/03/estonias-cyber-ambassador-weighs-in-00220220
[11] 6 USC 1503

The Cybersecurity Coalition supports the reauthorization of CISA 2015. We urge this committee to take the lead in making its introduction and passage a priority. We look forward to working with you on this effort.

Conclusion

In conclusion, the path forward in strengthening our Nation's cybersecurity lies in harmonizing and streamlining regulations. It is critical that we create a regulatory environment that allows organizations to focus on meaningful cybersecurity practices rather than navigating complex, burdensome, and conflicting requirements. On behalf of the Cybersecurity Coalition, I strongly urge Congress to continue prioritizing this issue and push CISA to address key concerns in CIRCIA, including clarifying the definition of "covered entity, "refining the scope of "covered cyber incident, and ensuring reciprocity across frameworks.

We appreciate the work Congress has done, and we are committed to working alongside you to ensure cybersecurity regulations are effective and efficient. Thank you for the opportunity to testify. I look forward to your questions.

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.

Testimony of Robert Mayer
SVP, Cybersecurity
USTelecom – The Broadband Association

Before the House Homeland Security Committee's Subcommittee on Cybersecurity and Infrastructure Protection

Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime

March 11, 2025

Chairman Garbarino, Ranking Member Swalwell, and Members of the Subcommittee,

Thank you for the opportunity to testify today on the critical issues of cybersecurity incident reporting and regulatory harmonization. We are committed to strengthening the public-private partnership to bolster our national security and stay ahead of our adversaries. This Committee has an extraordinary opportunity to reset our national cybersecurity policy in ways that directly impact security outcomes.

Our nation is under constant cyberattack, with estimates of up to $23 trillion in annual damages by 2027, increasing at a rate of more than 20% per year.[1] We must take immediate action to eliminate redundant or conflicting cyber regulations, which can consume up to 70% of cybersecurity resources.[2] By streamlining these requirements, we can free up critical resources for threat mitigation and incident response—at virtually no cost.

Let me reaffirm our view that it is essential we fix how the Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA) needs to be implemented. While well-intentioned, it is essential that we refine its execution to ensure consistency with the law's original intent. Specifically, key terms such as "covered incident," "covered entity," and "reasonable belief" must be clearly defined. The liability protections designed to safeguard cyberattack victims and promote candid reporting must be strengthened. As of today, none of these fundamental issues have been meaningfully addressed in a manner visible to industry, nor has our sector been substantively engaged in addressing these concerns.

We urgently need an ex parte process—which is to say a formal, transparent, and common process that encourages CISA to hear and consider industry perspectives. In fact, USTelecom spearheaded a letter by 21 organizations that formally requested that CISA establish such as process; a request that was rejected.

Had this request been granted immediately, we would have already been working together to resolve these challenges. If we do not act quickly, we will end up with a rule that does more harm than good.

---

[1] *See* The Economist, "Unexpectedly, the cost of big cyber-attacks is falling" (May 17, 2024).
[2] Chamber of Commerce, Briefing with Majority and Minority Staff of Senate Homeland Security and Government Affairs Committee (May 29, 2024).

We must also recognize that this law does not exist in isolation. The patchwork of federal, state, and sector-specific cyber incident reporting requirements presents an ever-growing burden on organizations attempting to comply with multiple, often conflicting, mandates. Fortunately, there is a strong lawmaker interest to harmonize cyber regulations, including incident reporting requirements.

We believe the Office of the National Cyber Director (ONCD) should play a leading role in rationalizing cybersecurity regulations and incident reporting regimes. Solving the problem of fragmented state laws will require clear federal preemption, complemented by robust safe harbor provisions. This work must be prioritized, as it is directly tied to our national security.

We believe it is important that Congress acts now. We do not have time for further studies, requests for information, commissions, or pilot programs. Every moment spent delaying reform provides adversaries with additional opportunities to undermine our collective security. We must move swiftly and decisively to enhance our cybersecurity posture.

Major recent cybersecurity incidents have highlighted the importance of a stronger and more coordinated information sharing and incident response partnership between the federal government and the private sector. Congress advanced that project with the Cybersecurity Information Sharing Act of 2015, which is set to sunset in September 2025. We ask that Congress extend the Act, and establish additional policies to improve the public-private partnership.

Key pillars for improve this partnership include:

- ***There Should Be a Single Responsible Federal Agency for Major Cybersecurity Incidents.*** In the midst of a major incident, an operator's cybersecurity team is tightly focused on understanding and mitigating the challenge, and may be coordinating with other affected entities and/or with one or more law enforcement or national security agencies. It is practically difficult and often inadvisable to pull away from those operational imperatives to engage in briefings or other general information sharing and analysis activities (which takes substantial time and effort) with multiple government stakeholders absent concrete benefits to doing so.
    - Accordingly, Congress should ensure a unified, whole-of-government approach to major cybersecurity incidents: In the wake of a major incident with national security implications, a single "Responsible Agency" should have formal responsibility for (i) coordinating with the private sector and (ii) overseeing government information-sharing during a cybersecurity event.

- ***Power to Suspend Reporting Obligations***. Congress should grant the Responsible Agency the power to suspend all federal, state, and contractual reporting obligations upon a finding that doing so is in the national interest. Otherwise, the existing patchwork of reporting regimes (e.g., FCC, SEC, CIRCIA, government contracts, private contracts) could cause highly sensitive information to be promulgated in a haphazard manner.

- **Expanded Government Sharing of Actionable Cybersecurity Information.** Whether sharing information about a specific incident or a potential or known threat, the government should focus on getting detailed, actionable tactical information in the hands of the private sector personnel responsible for protecting communications networks.
    - ***Security Clearances for Private Sector Leaders.*** Private sector CISOs and other key cybersecurity professionals should be granted security clearances (subject to appropriate vetting). Security clearances should not be tied to whether an individual is involved in a particular government project or program.
    - ***Secure transfer mechanisms.*** Congress should fund a streamlined method for government agencies and the private sector to securely transmit and receive sensitive information.

- ***Promote Meaningful Private Sector Sharing of Sensitive Information.*** Policies for promoting information sharing need to promote voluntary private sector information sharing:
    - ***Confidentiality of information shared by industry.*** Enact legislation that would create major penalties for individuals within the government that breach confidentiality or share information without authorization during a national security cyberattack investigation. The private sector will not share highly sensitive information with the government if there is a risk government employees receiving the information will leak it.
    - ***Immunity for information shared by industry.*** Establish a strong "Reverse Miranda" regime where information shared by a private actor cannot be used against it in any future action or proceeding.
    - ***Limited number of recipients.*** Private actor needs assurances that sensitive information it shares will only be available to a small number of government officials and companies. Operators will not meaningfully share information if the pool of recipients is too large or includes potentially untrusted persons/entities.

We must also be willing to reconsider policies that have failed to produce meaningful security benefits. One such example is the Securities and Exchange Commission's (SEC) cyber disclosure requirements, which, rather than enhancing security, have inadvertently provided malicious actors with a roadmap to exploit vulnerabilities. These mandates must be reassessed to prevent them from serving as a tool for cybercriminals.

In conclusion, success in cybersecurity requires close collaboration between industry and government, including Congress and the Office of the National Cyber Director. We must act now to ensure that our cybersecurity policies are well-reasoned, well-informed, and designed to maximize efficiency and effectiveness. By fixing CIRCIA's implementation, harmonizing cyber regulations, and eliminating unnecessary burdens, we can strengthen our nation's cyber defenses and uphold our commitment to protecting national security.

Thank you for the opportunity to testify today. I look forward to your questions.

Testimony of Heather Hogsett

Bank Policy Institute Senior Vice President, Deputy Head of BITS

Before the U.S. House Subcommittee on Cybersecurity and Infrastructure Protection

"Regulatory Harm or Harmonization? Examining the Opportunity to Improve the Cyber Regulatory Regime"

March 11, 2025

Chairman Garbarino, Ranking Member Swalwell and Honorable Members of the Subcommittee, thank you for inviting me to testify. I am Heather Hogsett, Senior Vice President and Deputy Head of BITS, the technology policy division of the Bank Policy Institute.

BPI is a nonpartisan policy, research and advocacy organization representing the nation's leading banks. BPI members include universal banks, regional banks and major foreign banks doing business in the United States. BITS, our technology policy division, works with our member banks as well as insurance, card companies and market utilities on cyber risk management, critical infrastructure protection, fraud reduction, regulation and innovation.

I also serve as Co-Chair of the Financial Services Sector Coordinating Council Policy Committee. The FSSCC coordinates across the financial sector to enhance security and resiliency and to collaborate with government partners such as the U.S. Treasury and the Cybersecurity and Infrastructure Security Agency, as well as financial regulatory agencies.

On behalf of BPI member companies, I appreciate the opportunity to provide input on the status of the Cyber Incident Reporting for Critical Infrastructure Act, as well as the state of cybersecurity regulation, and ways to potentially harmonize existing requirements. There is an urgent need to reduce overlapping and duplicative regulatory requirements that present considerable challenges for many critical infrastructure entities. Financial institutions experience these challenges acutely when complying with a multitude of incident reporting requirements and during cyber-specific supervisory examinations conducted by numerous financial regulatory agencies.

As the government surveys the current cyber regulatory landscape in search of increased efficiencies, it should prioritize: (1) streamlining cyber incident reporting requirements to allow cyber personnel to focus on response efforts; and (2) consolidating cyber regulatory requirements and supervision.

Cyber Incident Reporting

To better align incident reporting requirements, government agencies should consider: (1) substantial revisions to CISA's proposed rule to implement the *Cyber Incident Reporting for Critical Infrastructure Act* ("CIRCIA"); (2) rescinding the SEC's Cyber Incident Disclosure Rule; and (3) directing federal agencies to stop issuing duplicative requirements and instead leverage CIRCIA as Congress intended.

Revise the CIRCIA Proposed Rule

Almost a year ago, I testified before this Subcommittee shortly after CISA released its proposed rule.[1] During that hearing, I noted our members' concerns that CISA's proposal reflected an overly broad reading of the underlying statute and would add significant compliance obligations on frontline cyber personnel during the most critical incident response phase. As we move closer to the statutory deadline for CISA to issue its final rule, our members maintain those same concerns.

Financial institutions supported CIRCIA as it was being considered by Congress because it proposed a uniform incident reporting standard for critical infrastructure and sought to enhance CISA's ability to combat sophisticated cyber threats. Because CISA's proposal fell short of that aspiration, we—along with several other financial trade associations—recently reiterated this viewpoint in a letter to Department of Homeland Security Secretary Noem and Office of Management and Budget Director Vought requesting that they withdraw the current proposal and re-issue it more in line with congressional intent.[2] While the current proposal is too broad in scope, we continue to believe that CIRCIA, if properly calibrated, can enhance our collective defenses and mitigate threats from foreign adversaries.

For that enhancement to be most effective, it is also important that Congress reauthorize the *Cybersecurity Information Sharing Act of 2015* ("CISA 2015").[3] The information, antitrust, and liability protections in CISA 2015 are imperative for public-private information sharing and provide the legal clarity companies need to share information not only with CISA but with other companies across critical infrastructure. The protections in CISA 2015 are also incorporated by reference in CIRCIA—making their reauthorization all the more critical. The expiration of the legal framework provided in the Act could substantially disrupt information sharing—leaving us all less prepared to confront emerging cyber risks.

As we noted in our joint financial trades response to CISA's proposal last June, it is critical that CISA's final rule not extend beyond the authorities granted to it under the statute.[4] Bipartisan members of this

---

[1] *Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking Before the Subcomm. on Cybersecurity and Infrastructure Protection of the H. Comm. on Homeland Security*, 118th Cong. (2024) (statement of Heather Hogsett, Senior Vice President, Technology & Risk Strategy for BITS, Bank Policy Institute).

[2] Letter from the American Bankers Assoc., Bank Policy Inst., Inst. of Int'l Bankers, & Sec. Industry & Fin. Markets Assoc., to Kristi Noem, Secretary, Dep't of Homeland Sec. & Russell T. Vought, Director, Office of Mgmt. & Budget (Feb. 28, 2025), https://bpi.com/wp-content/uploads/2025/02/CIRCIA-Letter-to-Noem-Vought-2.28.25.pdf.

[3] Consolidated Appropriations Act, Pub. L. No. 114-113, Div. N, Title I—Cybersecurity Information Sharing Act, 129 Stat. 2935 (2015), 6 U.S.C. § 1501.

[4] American Bankers Assoc., Bank Policy Institute, Institute of International Bankers, & Sec. Industry & Financial Markets Assoc., Comment Letter on Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements (Jun. 28, 2024), https://bpi.com/wp-content/uploads/2024/06/CIRCIA-Reporting-Requirements-Comment-Letter.pdf.

Committee, along with Senator Peters, submitted comments emphasizing that same view.[5] These responses were enormously helpful for reiterating congressional intent, and we thank you for your leadership.

To adhere more closely to the CIRCIA statute, the final rule should limit reporting to information directly related to an actionable purpose—like detecting signs of a widespread vulnerability. Narrowing reporting data elements in this way would help give life to CIRCIA's "substantially similar" exception—something that would be unavailable to covered entities under the breadth of the current proposal. It would also lessen the burden of the supplemental reporting requirements which, as currently drafted, would likely require entities to file multiple additional reports during a single incident. Finally, CISA's rule should have reasonable thresholds for reporting above the standard proposed in the current *substantial cyber incident* definition that would likely cause a flood of reports on low-risk incidents.

Rescind the SEC Cyber Incident Disclosure Rule

Before the SEC finalized this rule in 2023, the financial sector raised significant concerns with its requirement to publicly disclose ongoing cyber incidents.[6] Chief among those concerns was that publicly disclosing ongoing and unremediated cyber incidents could impair a victim company's ability to respond or otherwise exacerbate harm to the company, its shareholders, and customers. Unfortunately, those reservations were realized in November 2023 when ransomware group AlphV weaponized the public disclosure requirement as an additional ransom payment extortion method by reporting its own victim to the SEC.[7] Given the pervasiveness of ransomware attacks, it is misguided to provide cybercriminals with an additional means to inflict financial harm on victim companies.

The public disclosure element of this rule is also problematic because it directly conflicts with the purpose of confidential incident reporting requirements. Although there are numerous confidential reporting rules across the government, all generally aim to limit harm and warn potential downstream victims. Once an incident is publicly disclosed, however, that task becomes much more difficult to achieve. Using CIRCIA as an example, CISA will only have 24 hours to confidentially share threat indicators before an incident is publicly disclosed under the SEC rule. That leaves vulnerable companies with virtually no time to implement those controls before the incident is disclosed to the world. Rescinding the requirement that companies publicly disclose ongoing cyber incidents will help eliminate unnecessary exposure to these threats.

---

[5] Representative Andrew Garbarino, Comment Letter on Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements (Jul. 3, 2024); Representatives Bennie G. Thompson, Yvette D. Clarke, & Eric M. Swalwell, Comment Letter on Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements (Jul. 3, 2024); Senator Gary Peters, Comment Letter on Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements (Jul. 2, 2024).

[6] Bank Policy Institute, American Bankers Assoc., Independent Community Bankers of America, & Mid-Size Banking Coalition of America, Comment Letter on Proposed Rules Regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Requirements (May 9, 2022), https://bpi.com/wp-content/uploads/2022/05/05.09.22-BPI-ABA-ICBA-MCBA-SEC-Comment-Letter-2022.05.09.pdf; Fin. Services Sector Coordinating Council, Comment Letter on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, https://www.sec.gov/comments/s7-09-22/s70922-20128382-291285.pdf.

[7] *AlphV files an SEC complaint against MeridianLink for not disclosing a breach to the SEC*, DATABREACHES.NET (Nov. 15, 2023), https://databreaches.net/2023/11/15/alphv-files-an-sec-complaint-against-meridianlink-for-not-disclosing-a-breach-to-the-sec/.

Stop Duplicative New Requirements and Leverage CIRCIA

The financial sector complies with as many as ten distinct incident reporting requirements in the U.S. alone.[8] Many of these obligations were instituted over the past few years as agencies seemingly rushed to put out their own—and often conflicting rules. We understand that agencies have unique missions and therefore different information needs. Nonetheless, the patchwork of current requirements across the government is past the point of helpful and now diverts finite resources away from incident response to filling out government forms.

There are three general categories these rules fall into: (1) incident notification; (2) confidential incident reporting; and (3) public incident disclosure. At one end of the spectrum, incident notification rules tend to be early during an incident investigation and simple—such as a phone call or email. They are used to inform an agency of an issue without requiring extensive data elements. We support and recognize the value of incident notification requirements for agencies with operational responsibilities or emergency authorities within critical infrastructure. An example of this is the financial regulatory agencies' Interagency Computer-Security Incident Notification Rule issued after substantive consultation with financial institutions.[9]

Confidential incident reporting requirements—like CIRCIA—involve more detailed responses and therefore often have slightly longer reporting timeframes. They serve to provide government with information to assess whether an incident might be widespread across different firms or sectors, to provide early warning to other entities or to contain an incident.

At the opposite end of the spectrum is the SEC disclosure rule which requires publicly alerting investors and others of an incident, regardless of whether mechanisms are in place—such as a software patch or the ability to disconnect from compromised networks—to prevent harm from spreading. As described above, this prioritization of investors' desire for information over critical incident response activities can exacerbate harm.

When enacting CIRCIA, Congress intended that it be "the primary means for reporting of cyber incidents to the Federal Government, that such reporting be through CISA, and that the required rule occupy the space regarding cyber incident reporting."[10] Because Congress was clear on this point, other federal agencies should not create their own duplicative confidential reporting requirements.[11] Incident notification and disclosure requirements should also be reviewed to ensure they are critical to the

---

[8] DEP'T OF HOMELAND SEC., HARMONIZATION OF CYBER INCIDENT REPORTING TO THE FEDERAL GOVERNMENT 9 (2023); U.S. DEP'T OF HOUSING & URBAN DEVELOPMENT, FED. HOUSING ADMIN., MORTGAGEE LETTER 2024-23, REVISED CYBER INCIDENT REPORTING REQUIREMENTS (2024); U.S. DEP'T OF HOUSING & URBAN DEVELOPMENT, GINNIE MAE, APM 24-02, CYBERSECURITY INCIDENT NOTIFICATION REQUIREMENT (2024).

[9] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 12 C.F.R. § 53 (2021).

[10] Sen. Rob Portman, Comment Letter on SEC Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure 4 (May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128391-291294.pdf.

[11] *See* U.S. DEP'T OF HOUSING & URBAN DEVELOPMENT, FED. HOUSING ADMIN., MORTGAGEE LETTER 2024-23, REVISED CYBER INCIDENT REPORTING REQUIREMENTS (2024); U.S. DEP'T OF HOUSING & URBAN DEVELOPMENT, GINNIE MAE, APM 24-02, CYBERSECURITY INCIDENT NOTIFICATION REQUIREMENT (2024); CFTC Operational Resilience Framework for Futures Commission Merchants, 89 Fed. Reg. 4706 (Jan. 24, 2024).

agency requiring them and do not interfere with confidential reporting. Instead, agencies should leverage CIRCIA and enter into sharing agreements with CISA to receive relevant cyber threat information.

Consolidate Cyber Regulatory Requirements and Supervision

Financial institutions are continuously examined by the Office of the Comptroller of the Currency, Federal Reserve and Federal Deposit Insurance Corporation, among others,[12] and often have hundreds of examiners on site to review their cybersecurity practices. According to a survey of our member firms, bank Chief Information Security Officers now spend 30-50 percent of their time on compliance and examiner management. The cyber teams they oversee spend as much as 70 percent of their time on those same functions. In the leadup to exams, financial institutions routinely receive over 100 requests for information, followed by 75 to 100 supplemental requests during an exam. Of those requests, firms report that roughly 25 percent duplicate requests from other agencies.

The cumulative effect of overlapping exams and regulatory requirements has created numerous unintended consequences. First, and as noted above, frontline cyber personnel now have significantly less time to perform their day-to-day security responsibilities as their bandwidth is consumed by compliance work. Relatedly, firms have paused or extended timeframes for completing strategic program improvements to prepare for emerging threats. Finally, staff retention has become an issue as financial institutions report morale problems and burnout among staff driven by excessive compliance demands and rapid response deadlines.

Looking forward, there should be a careful review of the current regulatory regime to ensure it is calibrated appropriately. This should include actively exploring how to consolidate regulatory responsibilities in a way that better balances the oversight obligations of regulators and the security realities of private companies. Moreover, supervisory activities should primarily focus on outcomes and not box-checking procedural exercises unrelated to actual risk. Structured accordingly, regulators will better understand the true cybersecurity maturity of the firms they oversee and regulated entities will have the time they need to defend against sophisticated and well-resourced foreign threat actors.

Conclusion

We welcome the Committee's attention to this important issue. The financial sector has and will continue to support confidential information sharing to provide early warning and help prevent malicious attacks. This includes CIRCIA, which, if appropriately tailored to the statute and congressional intent, will substantially improve awareness of cyber threats across the most important sectors of our economy. Harmonizing regulatory requirements is not a trivial task, but we are committed to working with this Committee and other federal agencies like CISA to advance that worthwhile goal.

[12] Other U.S. financial regulators include the Commodity Futures Trading Commission, Consumer Financial Protection Bureau, National Credit Union Administration, Securities and Exchange Commission, and state banking agencies.