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.

Statement for the Record from the Bank Policy Institute

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

"Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking"

May 1, 2024

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 of Technology and Risk Strategy for 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 and 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 feedback today on CISA's notice of proposed rulemaking to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022. We were pleased to support CIRCIA as it was being considered by Congress because it sought to develop a uniform incident reporting standard across all major sectors of the economy and would provide CISA with information it needs to better defend against attacks.

While we continue to believe that CIRCIA will play an important role in our collective defense against nation-state attacks and malicious criminals, we urge CISA to substantially revise the proposed rule in several key areas to ensure its requirements are simple and directly support CISA's ability to have better awareness of significant cyber incidents; to quickly provide useful information to critical infrastructure; and to allow cyber personnel to focus on response and recovery rather than government reporting.

As currently drafted, this proposal will require extensive efforts by critical personnel during the most critical phase of an incident and includes expectations for ongoing updates. When combined with a low threshold for reporting and other existing regulatory reporting requirements, this will add significant burden and compliance obligations.

BPI is working with our member companies and several other financial trade associations to provide a detailed response that I will be happy to share with this Committee once it is complete. In the interim, I would highlight that we believe CISA took an overly broad approach and expanded certain areas well beyond the statute. We offer the following concerns and recommendations:

1) **CISA should refine its broad interpretation of the CIRCIA statute.** CISA should apply a higher threshold for incidents that must be reported to better focus on significant cyber threats. It should also reduce the reporting elements to those that support CIRCIA's goal to quickly identify and assess risks across sectors and disseminate early alerts and mitigation measures where possible.

2) **CISA should focus on building the capability to leverage reported information for actionable purposes.** CISA should ensure it is adequately equipped to intake incident reports and has the capabilities and subject matter expertise to provide timely and actionable information back out to industry along with tools to help minimize or avoid threats. CISA should also clarify how it will protect this information and provide Sector Risk Management Agencies with information they need to fulfill their responsibilities and coordinate with entities in their sector.

3) **Congress should continue to focus on regulatory harmonization.** While we have seen progress in coordination on cyber incident notification by the prudential banking regulators, other independent regulators continue to issue rules that duplicate or conflict with CIRCIA. In particular, the SEC's cyber incident disclosure rule adds unnecessary complexity to incident response and undermines the purpose of CIRCIA by publicizing that a company has been attacked while CISA is still working to warn other potential victims and prevent further harm.

Cyber Incident Information Sharing in the Financial Sector

Financial institutions are often targeted by hostile nation-state cyber actors and criminal organizations seeking to disrupt the financial system and overall functioning of the U.S. economy. As a critical infrastructure sector, the financial services industry has acknowledged the severity of these risks and invested significant resources over more than two decades to enhance or otherwise support cyber information sharing efforts and incident response coordination.

The formation of the FSSCC and Financial Services Information Sharing and Analysis Center were both key elements in these efforts. The FSSCC strengthens the resiliency of the financial services sector by proactively identifying cyber threats, driving preparedness and coordinating crisis response.[1] The FS-ISAC shares cyber threat information and best practices with roughly 5,000 members in 70 different countries.[2] Each organization strengthens public-private cooperation through trusted, confidential forums that enable detailed information sharing and serve as a model other critical infrastructure sectors have sought to emulate.

In addition to these two settings, BPI members supported regulatory efforts to ensure timely awareness of significant cybersecurity threats facing financial institutions or critical infrastructure more broadly. The prudential banking regulators' Computer-Security Incident Notification Rule[3] is an example of this. That rule allows institutions that have suffered a potentially significant incident to satisfy their compliance obligations by notifying their primary regulator—either the Federal Reserve Board, the Office of the Comptroller of the Currency or the Federal Deposit Insurance Corporation—via a simple email or telephone call within 36 hours. This requirement balances regulators' need for early awareness of

[1] *About FSSCC*, FSSCC, https://fsscc.org/about-fsscc/.
[2] *Who we are,* FS-ISAC, https://www.fsisac.com/who-we-are.
[3] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 (Nov. 23, 2021).

significant cyber threats without diverting critical resources at affected entities who need to effectively respond.

BPI members were also broadly supportive of CIRCIA while it was being negotiated in Congress and leading up to its enactment in March of 2022.[4] As a regularly targeted critical infrastructure sector, we shared policymakers' view that the proliferation of cyber incidents represents a critical economic and national security threat. To that end, banks and other financial institutions believed CIRCIA was a unique opportunity to expand visibility, awareness and coordinated sharing of incident information across all critical infrastructure sectors to combat sophisticated and persistent cyber threats.

Financial Services Regulatory Landscape

For CIRCIA to be effective, however, it is important that CISA acknowledges existing regulatory requirements and harmonizes those with CIRCIA wherever possible. As the Cyber Incident Reporting Council's report commissioned by CIRCIA identified, there are eight distinct cyber incident reporting requirements applicable to the financial sector alone.[5] Financial institutions are also subject to rigorous supervision and examinations to determine whether they operate in a safe and sound manner. This includes on-site examiners evaluating compliance with relevant statutory requirements and whether firms implement appropriate security controls, including third-party risk management, operational risk and resiliency programs and oversight by the board of directors.

The recent adoption of the SEC's public company disclosure[6] rule adds to this already complex regulatory landscape. As BPI and many industry stakeholders have pointed out[7], the SEC's rule conflicts with the primary purpose of confidential reporting requirements like CIRCIA, creates confusion and diverts resources from critical response and recovery activities. Requiring public disclosure—particularly of ongoing incidents—puts sensitive information into the hands of hostile threat actors while shortening the timeframe agencies like CISA will have to warn other potential victims. In the first few months since the rule went into effect, we've seen malicious actors even turn the disclosure requirement into an additional extortion method used against victim companies.[8]

---

[4] Press Release, Bank Policy Institute, President Signs Omnibus, Includes BPI-Supported LIBOR and Cyber Incident Reporting Solutions (Mar. 15, 2022), https://bpi.com/president-signs-omnibus-includes-bpi-supported-libor-and-cyber-incident-reporting-solutions/; Press Release, Bank Policy Institute, Incident Reporting Law Moves Toward Finish Line as Senate Seeks to Advance Sensible Solution (Oct. 6, 2021), https://bpi.com/incident-reporting-law-moves-toward-finish-line-as-senate-seeks-to-advance-sensible-solution/.

[5] DEP'T OF HOMELAND SEC., HARMONIZATION OF CYBER INCIDENT REPORTING TO THE FEDERAL GOVERNMENT 9 (2023).

[6] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896, 51944 (Aug. 4, 2023).

[7] Press Release, Bank Policy Institute, SEC Rule on Cyber Disclosure Risks Harming Investors, Exacerbates Security Risks (Jul. 26, 2023), https://bpi.com/sec-rule-on-cyber-disclosure-risks-harming-investors-exacerbates-security-risks/; Heather Hogsett, *Fool's Gold: Why the Exceptions to the SEC's Cyber Disclosure Rule Cannot and Will Not Work, and the Damage that Will Ensue*, BANK POLICY INST. (Dec. 18, 2023), https://bpi.com/fools-gold-why-the-exceptions-to-the-secs-cyber-disclosure-rule-cannot-and-will-not-work-and-the-damage-that-will-ensue/.

[8] *Ransomware gangs are now reporting to the SEC, says CrowdStrike CEO*, CNBC (Dec. 21, 2023), https://www.cnbc.com/video/2023/12/21/ransomware-gangs-are-now-reporting-to-the-sec-says-crowdstrike-ceo.html.

Implementing CIRCIA

Successful implementation of CIRCIA will provide several important benefits to our national cyber defense. If calibrated and implemented appropriately, CIRCIA will provide CISA with more information from across critical infrastructure sectors to enhance its analysis and assessment of emerging cyber threats. This in turn will improve the quality of the alerts and security services offered by CISA and other government partners and provide earlier warning to potentially affected companies so they can better protect themselves.

CIRCIA will also provide greater insight into the threats facing third parties and other service providers. Like financial institutions, threat actors have frequently targeted these entities in recent years and the proposed rule acknowledges how the compromise of a third-party service provider can "cause significant cascading impacts to tens, hundreds, or even thousands of other entities." Consistent incident reporting from those entities will provide CISA with a more complete picture of the cyber threat landscape and will also help third-party providers enhance their own incident management processes.

Benefits notwithstanding, implementing CIRCIA will be a challenge. As noted in the CIRC Report, there are 45 in-effect reporting requirements administered by 22 federal agencies—many of which have different definitions and thresholds for reporting.[9] Rather than implementing the CIRC report's recommendation to adopt a more uniform definition and threshold for a reportable cyber incident, CISA's proposed substantial cyber incident definition adds another broad term with a reporting threshold well below many other existing requirements. Streamlining those requirements is no trivial task given the divergent missions and authorities of those federal agencies—however, CISA's narrow interpretation of the "substantially similar" exemption under CIRCIA will render it unusable. As a result, entities will likely have to continue to simultaneously assess compliance with multiple notification, reporting and disclosure obligations.

There is also the challenge of getting some independent regulatory agencies to engage and support broader harmonization efforts. For example, the SEC first proposed its public company disclosure rule just eight days after the Senate passed CIRCIA. Since then, the SEC rule has created uncertainties around what cyber threat and incident information can be shared between private sector entities and has been used as an additional extortion method by ransomware criminals—all for the attenuated benefit of informing investor decision-making. This past January, the Commodity Futures Trading Commission also proposed a new rule on operational resilience that would require reporting of cyber incidents within 24 hours.[10]

CISA's 447-page NPRM is in many ways a reflection of how challenging it is to bring coherence to the fragmented cyber regulatory landscape. Articulating a definition for covered entity across 16 critical infrastructure sectors is not a straightforward exercise. At the same time though, the required data elements CISA proposes for CIRCIA reporting are expansive and, in several instances, well beyond what was contemplated by the underlying statute. For example, the rule proposes to require firms to report detailed investigative findings such as the "timeline of compromised system communications with other systems"[11] as well as "a description of any unauthorized access, regardless of whether the covered cyber incident involved an attributed or unattributed cyber intrusion, identification of any informational impacts or information compromise, and any network location where activity was observed."[12] The

[9] *Id.* at 4–5.
[10] Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants, 89 Fed. Reg. 4,709, 4758–59 (Jan. 24, 2024).
[11] CIRCIA NPRM § 226.8(a)(3)(iv).
[12] *Id*. at § 226.8(a)(2).

NPRM also proposes that reports include the "direct economic impacts to operations"[13] and even an "assessment of the effectiveness of response efforts in mitigating and responding to the covered cyber incident."[14] These requirements are broader than those contained in the CIRCIA statute and, as discussed above, will make it difficult if not impossible to leverage a report provided to another federal agency under the "substantially similar" reporting exemption.

Given the breadth and detail of the proposed reporting elements—several of which are typically unknown prior to the 72-hour reporting deadline—CIRCIA's supplemental reporting requirements would likewise become more burdensome than Congress intended. Because CISA interprets "substantial new or different information" as anything responsive to a required data field in a CIRCIA report, it is likely that an impacted entity will have to provide numerous supplemental reports during a single incident response. If not balanced appropriately, outsized compliance demands can create operational risks by consuming the time of front-line cyber personnel on reporting requirements instead of on network and enterprise security operations.

The proposed data elements are also relevant for another important aspect of CIRCIA's implementation—CISA's capability to intake reported information and provide timely and useful alerts back out to potentially impacted entities. This includes providing clarity for how CISA will share reported information with Sector Risk Management Agencies and other law enforcement partners. Equally important will be how CISA protects this very sensitive information once submitted as it will quickly become a target for attackers and could put covered entities at risk if breached. In the final rule, CISA should carefully calibrate the information required in CIRCIA reports with its own ability to leverage that information in furtherance of some actionable purpose. As currently constructed, the proposed rule requires information beyond CISA's direct statutory mandate and above what is necessary "to enhance situational awareness of cyber threats across critical infrastructure sectors."[15]

Recommendations

As noted above, BPI is working on a comprehensive response to the CIRCIA NPRM. Based on our discussions with banks and other financial institutions thus far, we offer three recommendations for CISA and the Committee's consideration:

1) ***CISA should refine its broad interpretation of the CIRCIA statute*.** CISA should revise the definition of "substantial cyber incident" to ensure a higher threshold for reporting and avoid over-reporting of incidents that cause minimal harm or impact. For instance, the requirement to report a "disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services" lacks an impact threshold and could lead to a large number of immaterial or less significant incidents being reported. The CIRCIA statute had additional language for this prong referencing disruptions to business or industrial operations "including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability."[16] While Congress may not have intended to limit this threshold exclusively to those three scenarios, it does indicate a specific operational disruption much narrower than the one outlined in the proposed rule.

[13] *Id.* at § 226.8(a)(4).
[14] *Id.* at § 226.8(a)(4)(i)(2).
[15] 6 U.S.C. § 681a(a).
[16] 6 U.S.C. § 681b(c)(2)(ii).

CISA should also reduce the reporting requirements to information that supports CIRCIA's goal to allow CISA to quickly identify and assess risks across sectors and provide early alerts and mitigation measures where possible. Covered entities should not be required to share sweeping investigative findings or details that are often not available until weeks or months after an incident.

In its proposed rule, CISA interprets the CIRCIA statute well beyond Congress's intent that CIRCIA promote "shared awareness of the cyber threats across the public and private sectors"[17] and not become a large-scale data collection exercise. For example, CISA acknowledges that the data elements proposed for CIRCIA reports exceed those specified by Congress in the statute. In fact, CISA's proposal outlines a level of granularity never seen before in incident reporting regimes and will make harmonizing cyber incident reports across federal agencies even more challenging.

To fulfill its goal of better awareness of cyber threats across critical infrastructure sectors, Congress recognized CISA would need to be notified of substantial incidents within a relatively short timeframe—hence the 72-hour reporting requirement. Nevertheless, when CIRCIA was enacted, Congress was careful to note the legislation sought to strike "a balance between getting information quickly and letting victims respond to an attack without imposing burdensome requirements."[18] CISA's proposed rule would disrupt that balance by requiring information that is often unknown within 72 hours and as a result significantly increasing supplemental reporting demands.

2) ***CISA should focus on building the capability to leverage reported information for actionable purposes.*** CISA estimates that over 316,000 companies will be considered covered entities under the final rule. When combined with the breadth of the proposed substantial cyber incident definition, CISA is likely to receive far more than the 15,000 annual incident reports it now anticipates. If CISA is to preserve its productive and collaborative relationship with the private sector, it is critical to assemble the necessary infrastructure, staff and communication channels to analyze and disseminate actionable cyber threat information to potentially impacted entities.

   It is also vital that CISA clearly articulate a process that will allow SRMAs, including the U.S. Treasury Department, to quickly be notified of an incident and to access information the SRMA may need to coordinate response efforts within their respective sectors. The financial services sector has a strong and collaborative relationship with Treasury that includes incident response playbooks and a communication plan. Both of these include coordination with regulators and interconnect with other national response mechanisms. The sector has experienced several ransomware attacks in the last year that impacted the sector to varying degrees. In each instance, Treasury played a vital role in the early stages by working with firms and regulators to assess impacts and potential downstream effects. Critical in this coordination is Treasury's ability to quickly access incident information while avoiding the need for various government agencies to contact the affected entity. CISA should clarify how this process will work once CIRCIA reporting is in place and how it will preserve and support the role of SRMAs.

---

[17] S. REP. NO. 117-249, at 2 (2022), https://www.congress.gov/117/crpt/srpt249/CRPT-117srpt249.pdf.

[18] Press Release, U.S. Sen. Homeland Sec. Comm., Peters & Portman Landmark Provision Requiring Critical Infrastructure to Report Cyber-Attacks Signed into Law as Part of the Funding Bill (Mar. 15, 2022), https://www.hsgac.senate.gov/media/dems/peters-and-portman-landmark-provision-requiring-critical-infrastructure-to-report-cyber-attacks-signed-into-law-as-part-of-funding-bill/.

3) ***Congress should continue to focus on regulatory harmonization*.** With CIRCIA, Congress took an important step towards establishing a harmonized cyber incident reporting standard across critical infrastructure. In 2023, the Biden Administration similarly identified harmonizing and streamlining existing regulation as a strategic priority in its National Cybersecurity Strategy[19], and the CIRC issued its report on harmonization with several recommendations for Congressional action.[20]

   Despite these efforts, independent regulators like the SEC and CFTC continue to offer their own disparate standards for incident reporting which will contribute to growing burnout and attrition among key cybersecurity personnel. According to a recent survey of large financial institutions, Chief Information Security Officers report spending between 30 to upwards of 50 percent of their time on regulatory compliance, with several firms noting that their security teams spend more than 70 percent of their time on compliance activities. As regulations continue to expand in number and scope, cybersecurity teams will have less time to adjust to rapid technological change. This presents considerable operational risk—particularly as hostile actors move to weaponize emerging technologies like artificial intelligence and quantum computing.

   With that being the case, we encourage Congress to explore legislative solutions to further harmonization efforts. The CIRC report's recommendation that Congress remove any barriers to harmonization and drive adoption of model definitions, timelines and thresholds for cyber incident reporting[21] could be beneficial if applied across all federal agencies to include independent regulatory agencies. It is vital that Congress make clear to regulators that they must recognize existing federal requirements and leverage the CIRCIA reports, rather than continue to issue new incident reporting requirements. This may be the most effective forcing function to achieve increased streamlining moving forward.

Conclusion

The financial services sector has long supported the early and confidential sharing of cyber threat and incident information. Early awareness of threats helps firms respond and calibrate additional security measures that can prevent malicious activity or minimize its impact. CIRCIA represents an important step towards expanding this type of awareness and information sharing across all critical infrastructure sectors. If its requirements are appropriately balanced, CIRCIA will help reduce attacks and the disruption they cause to individuals, businesses, our economy and our way of life.

It is imperative that we work together to ensure the final reporting requirements of CIRCIA balance CISA's needs for early incident information while not disrupting critical incident response and remediation activities. As currently drafted, CIRCIA would add significant requirements to an already challenging and complex set of government reporting requirements. It will also overwhelm CISA with information that is not needed or useful to fulfill the goals of better situational awareness and timely information sharing with critical infrastructure.

---

[19] WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY 1, 9 (2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
[20] DEP'T OF HOMELAND SEC., HARMONIZATION OF CYBER INCIDENT REPORTING TO THE FEDERAL GOVERNMENT 34 (2023).
[21] *Id*.

We are committed to continuing to work with CISA and this Committee to refine the proposed rule and ensure its successful implementation.

Testimony of Robert Mayer

Senior Vice President
Cybersecurity and Innovation
USTelecom – The Broadband Association

U.S. House of Representatives Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

Hearing on

Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking

May 1, 2024

Chairman Andrew Garbarino, Ranking Member Eric Swalwell, Members of the Subcommittee, thank you for convening this hearing on implementation of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), perhaps the most important of the foundational cybersecurity-related statutes Congress has passed. My name is Robert Mayer, and I am the Senior Vice President, Cybersecurity and Innovation at USTelecom and serve as the Chair of the Communications Sector Coordinating Council and Co-Chair of the DHS ICT Supply Chain Risk Management Task Force.

It is absolutely crucial to our national security that CISA, critical infrastructure entities, and other government agencies work collaboratively to implement Congress's vision for this law – to deepen and operationalize the partnership between government and industry that is indispensable to our defense against cyber threats.

As this Subcommittee is well aware, the United States' adversaries – China, Russia, Iran, North Korea – are increasingly becoming an aggressive military alliance, and those governments and their criminal proxies have extremely sophisticated cyber capabilities. We need close and well-coordinated teamwork between government and industry to ensure our defense.

CIRCIA can be a profoundly powerful tool in deepening this collaboration and teamwork, and I implore the Subcommittee to push this principle relentlessly in the years to come.

Unfortunately, parts of our government risk undermining this principle, as we increasingly see a rigid regulatory mindset focused on prescriptive compliance rather than dynamic teamwork. This manifested last week in the FCC's misguided order that will impose 20th century utility-based prescriptive regulations on Internet Service Providers — including even in the realm of cybersecurity — which are investing billions of dollars to innovate for the 21st century.

As the most dynamic and innovative nation in history, we need to recognize that our defense against these threats requires us to deepen our collaboration. We need to double down on, not undermine, the government-industry partnership. At this very moment, and literally every moment, experts in government and private industry are working shoulder to shoulder to outwit and outpace highly

organized efforts to infiltrate our nation's critical infrastructure. That is the only approach that will work.

Thankfully, the launch of CIRCIA can help get this right, because CIRCIA – if properly implemented – is fundamentally about collaboration and holistic situational awareness. Now, it is incumbent on government and industry partners to roll up our sleeves and collectively begin the work of translating Congress's directions into operational reality.

To be clear, CIRCIA implementation is an enormous task – CISA estimates that 300,000 entities will be covered by its requirements – and it will take years and multiple iterative exchanges between government and critical infrastructure entities to fully mature. Here again, the more collaboration and partnership we practice, the more we can develop mutual understanding and expectations of what is needed and how to achieve it.

There are several areas in particular that we believe need our collective attention.

For one, we need clarity on the terms and definitions in the rule. Without sufficient specificity, this is difficult to accomplish. The proposed scope of "covered entities" and "covered cyber incident" are expansive and currently lack key guidance that cybersecurity practitioners will need, as they seek to provide CISA with information that is responsive to the agency's mission.

Moreover, it is imperative for our government partners to recognize the substantial cyber resources that will be allocated to assess whether an event meets the reporting criteria. The industry requires more precise definitions and clear reporting thresholds. Without these, there is a real risk that, in an effort to comply with the law, the industry will report numerous events that could easily overwhelm CISA's capacity to act on the information. Such overreporting could unnecessarily burden government resources and undermine the effectiveness of CIRCIA. It is crucial to establish definitions that are not excessively broad, as overly inclusive terms could divert essential resources away from cyber defense and towards regulatory compliance for its own sake.

Critically, we believe that covered cyber incidents should only be those pertaining directly to the mission of CISA and avoid unproductive and disproportionate focus on routine events.

It is also important to underscore that partnership implies reciprocity. To fulfill CIRCIA's purpose, CISA needs to establish mechanisms of rapidly disseminating valuable defensive advisories to critical infrastructure entities while also supporting victims as they respond to highly debilitating attacks.

The estimated cost to industry of these new requirements is $1.4 billion over eleven years, and it is estimated the federal government will incur costs of $1.2 billion over the same timeframe. Collectively, our nation needs a return on this investment and for the law to achieve its aims. We will work with CISA to ensure that meaningful incident reports lead to broader situational awareness and to increased operational preparedness and response capabilities.

It is also vital that we achieve harmonization and efficiency in reporting. Our members, from the smallest to the largest, have expressed concern about the substantial resources they will need to dedicate to complying with a rapidly growing patchwork of incident reporting requirements. Our ask from federal government partners is this: Providers need to be able to submit reports to a single agency. It will be essential to streamline the contents of reports as much as possible – by developing a common format – while allowing a variety of flexible reporting mechanisms that could ideally be tailored to the unique needs of organizations.

Finally, we call on CISA to establish ex parte communications for the CIRCIA rulemaking. This is a critical step toward ensuring a robust regulatory framework that reflects the intricate realities of cybersecurity in critical infrastructure sectors. As CISA now possesses enhanced regulatory powers, it is imperative that the agency adopts a transparent and open process akin to that employed by other regulatory bodies. This approach will facilitate continuous and meaningful input from industry stakeholders, whose expertise and firsthand experience are invaluable for crafting regulations that are not only effective but also practical. Such a process would not only enhance the quality and applicability of the regulatory outcomes but also bolster the credibility and trustworthiness of CISA as a regulatory authority in the eyes of the industries it regulates.

Deep and persistent collaboration is the key to achieving Congress's intent in implementing CIRCIA, and USTelecom and its members will continue to work closely with CISA, our sector risk management agency, through the Communications Sector Coordinating Council and other fora, and by actively participating in the CIRCIA rulemaking process. For decades, we have engaged consistently with CISA, its predecessors, and other government agencies to provide information about cyber threats and to advance law enforcement investigations, and we will continue to deepen and evolve that practice.

We seek the government's continuing partnership in making that a reality. I look forward to your questions.

Openpolicy

April. 29, 2024

Testimony of
Dr. Amit Elazari, J.S.D. , CEO and Co-Founder of OpenPolicy
Before the United States House Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection hearing entitled,
"Surveying CIRCIA: Sector Perspectives on the Notice of Proposed Rulemaking"

Wednesday, May 1, 2024, 2:00 PM ET
310 Cannon House Office Building

Chairman Garbarino, Ranking Member Swalwell, and distinguished members of the Subcommittee, on behalf of OpenPolicy and our community of innovative companies, thank you for the opportunity to testify today on the *Cyber Incident Reporting for Critical Infrastructure Act* or (CIRCIA).[1] We appreciate your leadership in supporting the passage of CIRCIA, and commend your critical role in conducting oversight of the Law's implementation process. We very much welcome the opportunity to continue working with this Subcommittee.

At a time when threats to our nation have never been more profound, and the consequences for human lives, critical infrastructure, and the foundational institutions on which we rely, have never been more prominent, the majority of businesses and critical infrastructure providers still stand defenseless against persistent and existential cyber threats. These threats have only expanded with the advancement of AI; the convergence of operational technology (OT), IoT, and IT systems; and the growing sophistication of adversaries.

CIRCIA, perhaps the most comprehensive legislative action on cybersecurity in decades, presents a critical opportunity to increase the government's situational awareness, reduce cyber risk, and move us collectively forward in the endless asymmetric fight against adversaries seeking to undermine U.S. national and economic security.

But, as I must emphasize - only If implemented properly.

My name is Amit Elazari, and I am the CEO and Co-Founder of OpenPolicy, a small business and technology company (otherwise known as a "startup"). I'm also the former Head of

[1] 6 U.S.C. 681–681; Public Law 117–103, as amended by Public Law 117–263 (Dec. 23, 2022).

Openpolicy

Cybersecurity Policy at Intel Corporation, served as Chair of the Cyber Committee of the Information Technology Industry Council (ITI), and was a member of the IT-Sector Coordinating Council (SCC) Executive Committee.

In addition to my current role, I teach at the University of California at Berkeley in the Master in Information and Cybersecurity Program and serve as an advisor to the UC Berkeley Center for Long-Term Cybersecurity. I also co-founded Disclose.io, whose body of work related to establishing authorization for third-party "good faith" security research (ethical, or "friendly" hacking) is referred to in the CIRCIA proposed implementing rule ("Rule" or NPRM").

In my capacity as a cyber policy expert, I engaged extensively in the stakeholder process as CIRCIA was drafted, and am now actively engaged in the rulemaking process. Today, I'm honored to share my views, and the view of the OpenPolicy community, on the progress made regarding CIRCIA implementation and the proposed rule.

By way of background, OpenPolicy[2] is the world's first policy intelligence and engagement technology platform, aiming to democratize access to the policy-making process for entities of all sizes by leveraging AI. OpenPolicy is a small business and perhaps the smallest member of the IT Sector Coordinating Council.

OpenPolicy collaborates with and represents leading innovators that develop cutting-edge technologies to enhance cybersecurity and protect critical infrastructure. OpenPolicy members include some of the world's leading AI, IoT, and botnet prevention security companies such as ***Armis, Human Security, FiniteState, HiddenLayer, Kiteworks, Cranium AI,*** and more. Our members' solutions are used extensively by the critical infrastructure community and among federal agencies to protect against malicious attacks.

My testimony identifies concrete policy recommendations that seek to align the Rule and CISA's implementation process with Congressional intent. I also want to highlight the Rule's impact on small businesses. This Committee is right to reflect on the implementation of CIRCIA, given its mandate, and also because of changes in the policy landscape, technology itself, and the threat landscape since both CIRCIA's enactment and the RFI release. OpenPolicy applauds you for facilitating this discussio.[3]

---

[2] www.openpolicygroup.com.

[3] CIRCIA requires covered entities to report to CISA covered cyber incidents within 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred and ransom payments made in response to a ransomware attack within 24 hours after the ransom payment has been made. See 6 U.S.C. 681b(a).

Openpolicy

Background

Recent events underscore the urgent need to strengthen national security and defense, and the opportunity CIRCIA has to advance government situational cyber awareness.

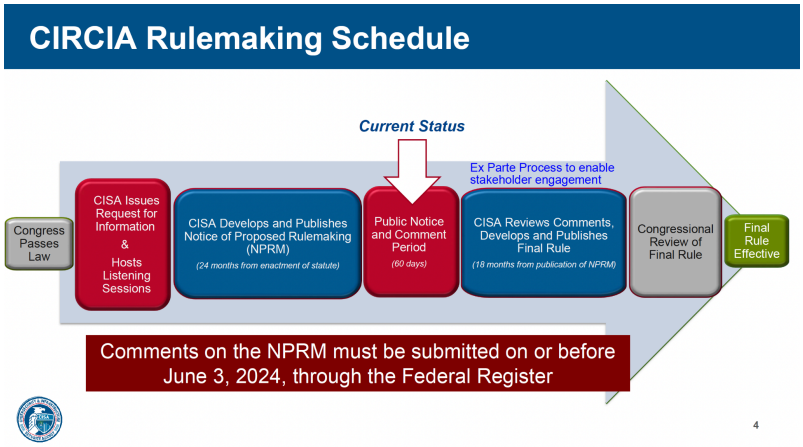
The promise CIRICIA holds relies on the ability of CISA to quickly intake reports, allocate resources, and provide support to entities affected by cyber incidents. CISA seeks to identify trends and swiftly disseminate this information to network defenders. Such proactive sharing will help alert other potential targets about emerging and existing threats and ideally prevent them from succumbing to similar attacks.

This use of information from the time an incident is reported, in support of immediate remediation but also to further longer-term prevention - is what CIRCIA aims to achieve and is meant to enhance our collective security. **Congress intended for CIRCIA to not only improve government awareness of cyber incidents but also to enhance security resilience throughout the entire ecosystem and ultimately advance risk reduction.**

The effectiveness of CIRCIA and its underlying regulations should be measured not only by how efficiently information from reported cyber incidents is examined, enriched, and transferred, but also by how that information is leveraged to improve the security of the entire ecosystem, i.e., in a manner proportional to the cost (estimated in $U.S. billions). Achieving this goal will entail a unified federal policy for leveraging the reported information to increase cyber resilience. This will require actions that extend beyond CIRCIA and the Rule. But the Rule, implemented correctly, presents a critical opportunity to advance this goal.

On the matter of Rulemaking process:

The landscape will continue to change - The Rulemaking process on CIRCIA should enable "ex parte" filings and engagements in the 15 months that follow the comment period



[ex parte comment process added, source: CISA]

CISA's 450-page NPRM on CIRCIA was released on April 4, 2024. Indeed, CISA's comprehensive and diligent work has resulted in an extensive Rule that will have a significant impact on our nation, its security posture, and definitions that will have a profound impact on small businesses and the startup/innovation community. The majority of impacted entities may not be able to bring their unique point of view forward during this timeframe, and most lack the resources and access to government affairs professionals.

CISA has engaged extensively with stakeholders via the RFI, and various listening sessions, yet the critical phase of the regulatory development process ***begins now*** - with the release of the Proposed Rule, the Comments Consideration and adjudication process, and preparation for Final Rule release. **Thus, we encourage CISA not only to extend the comment period and continue with the stakeholder engagement process but to also create a process that will allow for additional "ex parte" meetings and filings on the Rule. This should be accompanied by a transparent process for ex parte filings publication, similar to the proposed rules processes conducted and operated by the Federal Communications Commission or the Copyright Office.**[4]

Such a process would ensure that perspectives could be provided in a transparent and inclusive manner to CISA as the policy, technology, and threat landscape evolves in the 15-month period that follows the NPRM release and after the comment period has ended.

---

[4] See, for the FCC, 47 CFR §§ 1.1200–1.1216, and Federal Communication Commission, "Ex Parte Resources", https://www.fcc.gov/proceedings-actions/ex-parte/general/ex-parte-resources. See, for the Copyright Office, 37 CFR §§ 201, 205, U.S. Copyright Office, Ex Parte Communications, https://www.copyright.gov/rulemaking/ex-parte-communications/.

This would enable additional engagement and better alignment on the Rule, following the formal comment period.[5]

On matters of policy:

The cumulative cost of compliance burden, due to the proposed scope and expansion of liability, should be balanced and reciprocated with increased cyber resilience and risk reduction value

The record on stakeholder engagement reflects consensus on underlying concerns associated with definitions and issues proposed to be addressed in the Rule:

- **Complexity and Regulatory Duplicity** (among federal agencies and regulators, states and federal laws, and other applicable global regimes, such as E.U. NIS 2.0 directive) that will result in duplicative reporting, information and data overload, "noise", and extensive compliance burden on entities, including on small businesses, during the critical, "fire-fighting" period of incident response, when resources are limited. There is an urgent need for "harmonization" and streamlining of requirements.
- Concerns related to the definition of "covered cyber incident" capturing "**too much**" and in a manner that does not advance CISA's situational awareness, but rather overwhelms CISA.
- Concerns related to the **chilling effect of expanded liability,** which may hinder the public-private partnership model that undergirds information-sharing and threat mitigation practices today with the U.S. government and CISA, in particular.
- Concerns related to the **scope of covered entities** and impact on smaller businesses.
- Concerns related to the adverse impact to privacy and security due to increased information sharing, in certain cases, and the case of sharing sensitive "vulnerability" information in particular.

[5] OpenPolicy conducted meetings and filed "ex parte" comments on a recent Cybersecurity policy related Rule and Order released by the FCC, which were ultimately cited in the final Order. We find this process to be very useful and essential in a case where the evolving landscape merits continued, transparent engagement during the long period of comments adjudication, and particularly beneficial for small businesses who may not be able to engage on NPRM by the end of the comment period. We acknowledge the robust engagement processes already done by CISA, and further encourage CISA to continue and expand its engagement processes with innovative companies and small businesses, especially for sectors where they serve a large proportion of the impacted community, such as the DIB.

The Rule proposes a broad scope on many of these issues, notably the definitions of covered entities, incidents, and required fields. It notes however CISA's goal is to "achieve the proper balance among the number of reports being submitted, the benefits resulting from their submission….". Our overarching recommendation is to ensure that the ***cumulative impact and increased costs*** associated with such expansion, will in fact, result in ***additional value*** to risk reduction and enahnced cyber resilience.

To that end, OpenPolicy proposes the following policy recommendations:

To ensure enhanced situational awareness of cyber threats across critical infrastructure sectors "translates" into enhanced cyber resilience and risk reduction, CISA should consider:

- Additional reports, support functions, and public-private partnership structures focused on impacted under-resourced entities for information sharing and cyber resilience resources.
- Robust consideration to ensure that state-of-the-art secure and diverse sets of technology solutions, including AI capabilities, are used to intake incident reports,[6] review them, respond, and enable real-time mitigation in a way that supports entities' ability to transition from "remediation" to "prevention".[7]
- Alignment of other CISA, and other government-supported, resources (including programs such as CDM) to the nexus of threats, indicators, and compromises "spotted" via the reporting.
- Increased funding and resources to support the intake of remediation solutions and overall resilience of critical infrastructure, including federal infrastructure, to attacks - embodying the zero trust and secure by design culture.

---

[6] One method of technology adoption could be adopting standardized reporting forms supported by advanced programmatic and technological capabilities, whereby CISA can quickly operationalize, anonymize and share data with the industry in a way that is not attributed to specific entities. This approach ensures that incident information, rather than being relegated to solely routine threat reports, is transformed into actionable intelligence that can be immediately utilized to protect entities and enhance industry awareness and preparedness. The primary purpose of this reporting requirement should be to deliver critical and practical information in real time, enabling frontline cyber defenders to thwart attacks. Clarifying this goal will significantly aid in addressing the tactical details of the final rule. It would not only ensure that it meets its intended objectives effectively but also foster the overall resilience and awareness of the entire cyber ecosystem.

[7] CISA notes, the concern from "noise" increased scope (as illustrated by a broader set of "entities", "incidents", and "reporting fields"), "can be mitigated through technological and procedural strategies." [Rule, at 23652-3]. More attention and resources should be provided in support of such ***technological and procedural strategies***, to achieve the desired "translation" effect. CISA also recognizes further the breadth of duplicity and also that agencies may have different motivations in requesting such information.

Openpolicy

Our continued focus should be ***preventing attacks, not only remediating them***. The volume of reports should be calibrated in service of this cause. Achieving this goal will entail a broader technical and programmatic collaboration between all federal agencies involved, as well as the adoption of technology solutions.

To summarize, CISA was tasked with regulatory development and proposed definitions seeking to balance these inquiries with the underlying congressional intent of CIRCIA. The NPRM reflects a ***cumulative extended scope*** of proposed definitions with respect to covered entities, the scope of incidents to be reported, the application on small businesses, and the potential (and actual risk) for duplicative burden for reporting.

Overall this approach reflects a higher "cost" and "burden" that needs to be accompanied by a balanced "value", and progress in situational awareness and risk reduction - thereby enabling a significant "giving back" component.

Further action is needed to reduce the potential cost associated with regulatory duplicity and the potential for liability

CISA has acknowledged both the concerns of stakeholders associated with a complex reporting landscape and the need for further action on this matter.[8]

We recommend the following:

- CIRCIA Agreements, geared to enable information-sharing mechanisms and the underlying technology architecture to support such sharing in a secure manner, should be ***prioritized, resourced and achieved***. The Rule clarifies that good-faith efforts to reach such agreements would be made. However and as demonstrated by policy actions in the last two years, achieving this goal requires a more holistic and deliberate effort from all agencies involved and Congress. As the Congressional Research Report on CIRCIA puts it:

  > "It seems unlikely that federal regulators will relinquish their specific reporting requirements in deference to CISA because existing regulations and the proposed CIRCIA rule *serve different purposes*."[9]
  > (emphasis added).

[8] "In an attempt to minimize the burden on covered entities potentially subject to both CIRCIA and other Federal cyber incident reporting requirements, CISA is committed to exploring ways to harmonize this regulation with other existing Federal reporting regimes, where practicable and seeks comment from the public on how it can further achieve this goal." Id. at 23653.

[9] Congressional Research Service, CIRCIA: Notice of Proposed Rule Making: In Brief, April 11, 2024.

- One of the focal points of the CIRCIA agreements should be addressing the potential overlap with reporting requirements applicable to the Defense Industrial Base (DIB), under DFARS clause 252.204-7012. This path will reduce the considerable burden on a sector that is largely composed of small businesses (see below). This approach could be enabled by two related policy actions that recently matured. First, The DoD DFAR is soon to be revised,[10] thereby enabling further harmonization, despite the difference in scope of the "incident" definition.[11] Second, the DoD recently announced supporting infrastructure that can potentially enable a CIRCIA Agreement.[12]
- Congress should conduct oversight and perhaps even act in service of achieving additional CIRCIA agreements and reducing duplicity, when practical and desired, to achieve agency alignment.
- The need for harmonization and reducing duplicity is clear.[13] **The path towards reducing regulatory duplication, including with globally applicable regimes, should move away from aspirational and exploratory, toward actionable and practical - and such efforts will likely require a common technology architecture, where additional resources may be needed.**
- **On legal liability, we recommend enhanced "due process" mechanisms for covered entities.** We are concerned about liability protection erosion in the case of good-faith disagreements between CISA and the covered entity. As drafted, liability protection measures are "abandoned" once a subpoena is issued but without intervening process. While CIRCIA provides CISA the ability to use its subpoena power, the current NPRM does not include further consideration, or a "curing" process, an arbitration process, or other procedures to deliberate with CISA, in

[10] The Defense Acquisition Regulations Council Director has recently tasked a team with rule development, exploring a revision for DFARS clause 252.204-7012, DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (See DFARS Case 2023-D 024, has described, on the DFARS Open Cases Report, https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf.

[11] Compared to the CIRCIA proposed rule definition, covered entities in the Defense Industrial Base (DIB) Sector are already obligated to report cybersecurity incidents in a substantially similar timeframe (72 hours) pursuant to DFARS clause 252.204-7012, see *Safeguarding Covered Defense Information and Cyber Incident Reporting*. In contrast, the current scope of the DIB sector reportable incidents is narrower, and focuses on compromises of Controlled Unclassified Information while the CIRCIA proposed rule outlines a broader scope for "covered incident".

[12] On March 12th, 2024, DoD published the Defense Industrial Base Cybersecurity Activities (DIB CS) final rule, which expands eligibility to DoD's voluntary incident reporting and cyber threat intelligence sharing program to all DIB entities (rather than just cleared defense contractors).These revisions will allow all defense contractors who own or operate an unclassified information system that processes, stores, or transmits covered defense information to benefit from bilateral information sharing.

[13] See also the National Cybersecurity Strategy, at p. 11, "The Federal Government must coordinate the authorities and capabilities of the departments and agencies that are collectively responsible for supporting the defense of critical infrastructure".

good-faith, the amount of information requested prior to CISA leveraging its subpoena power, while enabling the entity to maintain liability protection (see § 226.14(d)(1), and ps. 23735). We recommend further consideration and Congressional oversight to ensure a measured approach in the Final Rule implementation on this topic.

Small Businesses First "Mindset"

Although the CIRCIA proposed rule affects many small entities across all critical infrastructure sectors, its impact on the ***DIB Sector*** small business community is profound. Defense security compliance ***Industry Expert Jacob Horne*** provided some striking analysis:[14]

- Nearly a quarter of all affected entities are in the Defense Industrial Base Sector
  - Of the 316,244 affected entities, CISA estimates 72,000 of them are in the DIB
- 17% of entities affected by the CIRCIA proposed rule are DIB SMBs
  - DoD has stated that roughly 75% of the DIB is made from small and medium-sized businesses

  That amounts to 54,000 of the 72,000 DIB entities in Table 1 Affected Population, by Criteria (see NPRM, at 23742).
- 98% of affected entities are SMBs, 17% of affected SMBs are in the DIB

  o Of the 316,244 covered entities, CISA estimates that 310,855 would be considered small entities (See, *Id*. at 23763).

	DIB Sector	Wire/Radio Comms	Critical Manufacturing	Financial Services
% Total Affected Entities	23%	20%	12%	12%
% Total Costs	16%	14%	9%	9%

See Table 1 and Table 10 of the NPRM, *Id.*

We, therefore, recommend prioritizing "scoping" activities (such as achieving CIRCIA agreements) impacting small businesses that are profoundly impacted by the Rule, such as the DIB small business community.

[14]See also Jacob Horne, Sum IT Up Podcast: CIRCIA Rulemaking and Double Incident Reporting for the DIB, available at: https://www.summit7.us/blog/circia-rulemaking?hs_amp=true.

,

Openpolicy

Summary

The Congressional intent for CIRCIA is “preserv[ing] national security, economic security, and public health and safety”, and assisting the federal government with increasing situational awareness and visibility to cyber threats in support of a broader mission to achieve systemic risk reduction for the United States and its underlying critical infrastructure. This ultimate value, of increasing cyber resilience merits additional proportionality between the cost, and value of and processes CISA and the federal government will exercise to “give back” to impacted communities who bear the implementation cost. This balance may require more resources and additional infrastructure to “rapidly deploy resources” and better diverse, state-of-the-art solutions to stay ahead of malicious actors and deploy alerting systems. It will further require those who need to alert the government - to have solutions, and “alert systems”, to spot issues, and to intake alerts and process them into action. To achieve cyber resilience we must approach CIRCIA implementation in the context of the broader common fabric of cybersecurity policy efforts, implemented in the U.S and globally.

Creating the architecture, technically, procedurally, and programmatically, and the culture, that truly achieves the underlying risk reduction goal of CIRCIA will require action from CISA, and other agencies, that may extend beyond the Rule, but proper implementation of CIRCIA can result in considerable progress. Much progress has been made - we will continue to rely on Congress's relentless attention to this matter, as we move forward with CIRCIA’s implementation.

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

Dr. Amit Elazari
CEO and Co-Founder
OpenPolicy

Openpolicy

About OpenPolicy

OpenPolicy[15] is the world's first policy intelligence and engagement technology platform, aiming to democratize access to the policy-making process for entities of all sizes by leveraging AI. OpenPolicy collaborates with and represents leading innovators who develop cutting-edge technologies to enhance cybersecurity and protect critical infrastructure. OpenPolicy members include some of the world's leading AI, IoT, and botnet prevention security companies such as *Armis, Human Security, FiniteState, HiddenLayer, Kiteworks* and more. Our members' solutions are used extensively by the critical infrastructure community and among federal agencies to protect against malicious attacks. OpenPolicy aims to represent the voice of smaller entities and innovators, which are at the forefront of developing solutions to address emerging threats. We strive to focus on actionable policy recommendations to advance our collective goal to secure and protect the nation. OpenPolicy has engaged on policies related to IoT security, AI security, software security, OT security and cloud security. OpenPolicy previously submitted written testimony for the record for this esteemed Subcommittee on Security Threats to Water Systems.[16] And while we have been operating less than a year, OpenPolicy is honored to be quoted and recognized by the White House, the Federal Communication Commission, the Department of Justice, and other government agencies for our substantive contributions to the policymaking process. We believe there is tremendous potential for increasing the voice of innovative companies, including cybersecurity solutions providers, in the policy-making process.

[15] www.openpolicygroup.com.

[16] Subcommittee Hearing, on Cybersecurity and Infrastructure Protection hearing entitled, "Securing Operational Technology: A Deep Dive into the Water Sector", Feb. 6, 2024.