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.