Testimony by Ari Schwartz

On Behalf of the

Cybersecurity Coalition

Before the

United States House of Representatives

Homeland Security Committee

Cybersecurity and Infrastructure Protection Subcommittee

on

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

March 11, 2025

INTRODUCTION

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

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

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

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

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

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

Cyber Incident Reporting

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

[6] 89 Fed. Reg 23644, 23660.

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

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

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

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

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

The Cybersecurity Information Sharing Act of 2015

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

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

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

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

Conclusion

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

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