Statement for the Record from the Bank Policy Institute

Before the U.S. Senate Committee on Homeland Security & Governmental Affairs

"Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization"

June 5, 2024

The Bank Policy Institute welcomes the opportunity to provide input on today's Senate Homeland Security and Governmental Affairs Committee hearing on "Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization." Today's hearing examines an important topic many critical infrastructure entities are grappling with given the proliferation of cybersecurity regulatory requirements in recent years. As such, we commend both the Committee and the Office of the National Cyber Director for emphasizing the need for increased harmonization.

Harmonization is particularly relevant for financial institutions that operate in a complex regulatory environment with multiple regulators and overlapping requirements. For example, resident examiners from the prudential financial regulatory agencies—the Office of the Comptroller of the Currency, the Federal Reserve Board and the Federal Deposit Insurance Corporation—regularly evaluate financial institutions to ensure they operate in a safe and sound manner and comply with relevant regulations. These examinations cover topics including information security, cyber risk management and incident reporting, governance, third-party oversight and operational resilience. Other agencies like the Consumer Financial Protection Bureau and the Commodity Futures Trading Commission also conduct similar oversight. Beyond examinations, banks are subject to additional cybersecurity-related regulatory requirements enforced by the Federal Trade Commission, the Securities and Exchange Commission and forthcoming requirements by the Cybersecurity and Infrastructure Security Agency, not to mention various state and international regulatory authorities.

Without appropriate harmonization, the collective effect of supervisory and regulatory obligations causes significant operational strain on financial institution staff and resources, diverting attention from efforts to keep pace with rapidly evolving cyber threats. During an exam, it is not unusual for firms to produce hundreds and sometimes thousands of pages of documents within 24-to-48-hour deadlines. In fact, according to a recent survey of large financial institutions, several firms reported their cyber teams now spend more than 70 percent of their time on regulatory compliance activities. Those same financial institutions also reported their Chief Information Security Officers or comparable senior cyber leaders spend between 30 to 50 percent of their time on the same regulatory compliance matters. Diverting finite cyber resources in this way leaves less time for risk mitigation efforts and more strategic security initiatives to fortify firm defenses over the long term. It leaves firms less well-positioned to confront existing critical threats and emerging risks associated with artificial intelligence and quantum computing, contributes to burnout and attrition among critical cyber personnel and unduly exposes firms to risk.

Based on our experiences within the multifaceted financial regulatory landscape, below are several proposed regulatory principles for the Committee to consider when developing a path to broader harmonization.[1] These principles include better coordination among regulatory agencies, regulatory reciprocity and leveraging common frameworks.

Regulator Coordination

Financial institutions work closely with the prudential financial regulators who coordinate among themselves through the Federal Financial Institutions Examination Council to help promote uniform supervision. There is significant benefit to the collaborative opportunities the FFIEC provides for regulatory agencies to develop joint standards and limit duplication where possible. Even with that coordination, differences in agency mission and exam scope continue to lead to overlap. This is particularly true as technology and cybersecurity play a more pivotal role within financial institutions and regulatory scrutiny of those areas increases.

As a general matter, it is imperative that all regulators consider existing requirements and do not duplicate or create variations of what already exists. Over the last few years, we have seen this does not always occur, especially with independent regulatory agencies. A prime example of this is the SEC's Public Company Disclosure Rule[2] which threatens to directly undermine the central purpose of confidential reporting requirements like the Cyber Incident Reporting for Critical Infrastructure Act.[3]

Relatedly, better coordination is especially necessary for requirements governing cyber incident reporting. Last year, the Cyber Incident Reporting Council identified 45 in-effect reporting requirements across the Federal government, all with varying standards and thresholds.[4] Just a few weeks ago, the Federal Housing Administration issued a new duplicative reporting requirement effective *immediately* requiring incident reporting within 12 hours of detection—all without the opportunity for public notice and comment.[5] The FHA's requirement is not aligned with any existing requirement such as the prudential banking regulators' 36-hour notification rule[6] or CIRCIA. The FHA is not alone in its efforts, as earlier this year we also saw the CFTC propose a separate incident reporting requirement as part of a proposed rule on operational resilience.[7]

As cybersecurity- and resilience-related regulatory requirements continue to expand in number and scope across critical infrastructure sectors, it is imperative that regulatory agencies consider the impact of these requirements on the ability of firms to focus on critical security tasks and preserve the ability to innovate to keep up with the dynamic threat environment. We are encouraged that the Committee is considering legislative approaches to address this need.[8]

Regulatory Reciprocity

---

[1] *See* Bank Policy Institute & American Bankers Association, Comment Letter on Request for Information on Cybersecurity Regulatory Harmonization (Oct. 31, 2023), https://bpi.com/wp-content/uploads/2023/10/2023.10.31-BPI-ABA-ONCD-RFI-Response-2023.10.31.pdf.
[2] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896, 51944 (Aug. 4, 2023).
[3] *Surveying CIRCIA: Hearing on Sector Perspectives on the Notice of Proposed Rulemaking Before the Subcomm. on Cybersecurity and Infrastructure Protection of the H. Comm. on Homeland Security*, 118th Cong. 3 (2024) (statement of Heather Hogsett, Senior Vice President, BITS/Bank Policy Institute), https://bpi.com/wp-content/uploads/2024/04/Statement-for-the-Record-from-the-Bank-Policy-Institute-H.-Homeland-CIRCIA-Hearing.pdf.
[4] Dep't of Homeland Sec., Harmonization of Cyber Incident Reporting to the Federal Government 4 (2023).
[5] Fed. Housing Admin, Significant Cybersecurity Incident (Cyber Incident) Reporting Requirements (May 23, 2024), https://www.hud.gov/sites/dfiles/OCHCO/documents/2024-10hsgml.pdf.
[6] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 (Nov. 23, 2021).
[7] Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants, 89 Fed. Reg. 4,709, 4758–59 (Jan. 24, 2024).
[8] Suzanne Smalley, *Senate chairman wants new White House-led panel to streamline federal cyber rules*, THE RECORD (May 30, 2024), https://therecord.media/gary-peters-legislation-new-committee-oncd-harmonize-cyber-regulations.

While enhanced harmonization would likely have to occur first, exploring a regulatory reciprocity model is a worthwhile endeavor to promote regulatory coherence. This reciprocity would involve regulators better leveraging each other's documentation, testing, evaluations and findings. Developing such a model would provide regulators with the information they need to fulfill their oversight responsibilities while preventing organizations from having to demonstrate compliance with the same or similar requirements multiple times and to multiple regulators. This would be a much more effective and efficient approach and would reserve more time for core security activities.

Common Frameworks

Last, utilizing existing standards—like the National Institute for Standards and Technology's Cybersecurity Framework—can be valuable for companies as they navigate complex regulatory obligations. Within the financial sector, the Cyber Risk Institute developed the Financial Sector Profile[9]—based on the NIST CSF—which integrates regulatory requirements unique to financial institutions. The Profile provides financial institutions with a single scalable resource for managing cyber risk and compliance requirements. Regulators can similarly use common frameworks to more efficiently tailor oversight activities and determine an organization's baseline security posture.

BPI recognizes the important role regulatory agencies play in promoting sound cybersecurity practices. As noted above, however, it is equally important to strike a balance between regulatory obligations and critical security activities to protect an organization. We look forward to engaging further with the Committee to find that appropriate balance.

[9] *The Profile,* CYBER RISK INSTITUTE, https://cyberriskinstitute.org/the-profile/.