BANK POLICY INSTITUTE

Testimony of Pat Warren

Bank Policy Institute Vice President for Regulatory Technology, BITS

Before the U.S. House Oversight Subcommittee on Cybersecurity, Information Technology, and Government Innovation

Enhancing Cybersecurity by Eliminating Inconsistent Regulations

July 25, 2024

Chairwoman Mace, Ranking Member Connolly and Honorable Members of the Subcommittee, thank you for inviting me to testify. My name is Pat Warren, Vice President for Regulatory Technology 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, critical infrastructure protection, fraud reduction, regulation and innovation.

As illustrated by CrowdStrike's software update last week that caused a global IT outage, the security and resilience of the networks, systems and software that we rely on as a nation are vitally important. Cybersecurity regulations can play a key role in fostering the necessary programs and policies to protect our critical infrastructure, and they have certainly played a role in protecting banks. As new cybersecurity regulations continue to proliferate, we must be mindful that, if not properly harmonized and aligned, such requirements can place unnecessary strain on the critical cybersecurity resources we rely on to prepare for emerging threats and address incidents when they occur.

On behalf of BPI member companies, I appreciate the opportunity to provide input on the need to harmonize cybersecurity regulations and streamline existing requirements. This is a challenge for many critical infrastructure entities—financial institutions especially—as they are grappling with a significant increase in new regulations.

Like the Committee, the Office of the National Cyber Director identified cyber regulatory harmonization as a key consideration in the National Cybersecurity Strategy and issued a

request for information last year to better understand how duplicative and overlapping cyber requirements affect regulated entities. BPI, along with the American Bankers Association, submitted a response discussing the current financial sector regulatory landscape and encouraging a balanced approach that considers the effect on front-line cyber personnel to ensure they can meet compliance requirements while maintaining critical day-to-day operational obligations.[1]

Congressional action is needed to ensure new and existing cybersecurity requirements accomplish the goals of better security and resilience while balancing the collective impact of these requirements on regulated entities. As Congress considers ways to better align cyber regulatory requirements, we offer the following recommendations:

1) Regulatory harmonization efforts should be led by an entity at the national level, such as the ONCD, that can compel action and possesses government-wide visibility into the cyber regulatory requirements issued by federal agencies and independent regulators.
2) That same national-level entity should conduct an assessment of the cyber regulations currently in effect to identify inconsistent, overlapping or contradictory requirements and develop recommendations to achieve increased harmonization.
3) Agencies considering new cybersecurity regulations should be required to consult with the national-level entity leading harmonization efforts to limit duplication and encourage consideration for how the proposed regulation may affect other policy directives.

Financial Services Regulatory Landscape

Financial institutions are subject to numerous regulations and rigorous supervision and examinations from the prudential banking regulators—the Office of the Comptroller of the Currency, the Federal Reserve Board and the Federal Deposit Insurance Corporation—to ensure they operate in a safe and sound manner. This includes resident examiners evaluating compliance with statutory requirements and whether financial institutions implement appropriate security controls in areas including third-party risk management, operational resilience and appropriate board oversight.

Beyond the prudential banking regulators, financial institutions also comply with cyber incident reporting, incident disclosure, consumer breach notification, data security and data privacy requirements enforced by the Commodity Futures Trading Commission, the Consumer Financial

[1] 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.

Protection Bureau, the Federal Trade Commission, the Securities and Exchange Commission, the New York Department of Financial Services and forthcoming rules from the Cybersecurity and Infrastructure Security Agency.

For cyber incident reporting alone, and as noted by the Cyber Incident Reporting Council in 2023, there are eight distinct cyber incident reporting requirements applicable to financial institutions.[2] That number also doesn't account for new requirements recently issued by the Federal Housing Administration and Ginnie Mae.[3]

This multifaceted environment was further complicated by the SEC's recent public company disclosure rule.[4] That rule conflicts with the primary purpose of the confidential reporting requirements noted earlier because it requires companies to publicly disclose material cybersecurity incidents—even if those incidents are still ongoing. Requiring public disclosure in those circumstances exposes victim companies to additional risk while shortening the timeframe other agencies have to leverage confidential reports and warn potential downstream victims. Moreover, since the SEC rule went into effect last December, we have seen threat actors weaponize the rule as an additional ransom payment extortion method against victim companies.

Principles for Effective Regulation

Based on our experience navigating the complexities of these requirements, we offer the following regulatory principles for the Committee to consider as part of its efforts to enhance harmonization. These principles include better coordination among regulatory agencies, regulatory reciprocity and leveraging common frameworks.

Regulator Coordination

Within the financial sector, the prudential banking regulators coordinate through the Federal Financial Institutions Examination Council to help promote uniform supervision across those agencies. That forum provides valuable collaborative opportunities for regulatory agencies to develop joint standards and minimize duplication. One example is the Interagency Computer-Security Incident Notification Rule issued following months of dialogue and consultation with

[2] Dep't of Homeland Sec., Harmonization of Cyber Incident Reporting to the Federal Government 9 (2023).
[3] U.S. Dep't of Housing & Urban Development, Fed. Housing Admin., Mortgagee Letter 2024-10, Significant Cybersecurity Incident (Cyber Incident) Reporting Requirements (2024); U.S. Dep't of Housing & Urban Development, Ginnie Mae, APM 24-02, Cybersecurity Incident Notification Requirement (2024).
[4] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896, 51944 (Aug. 4, 2023).

financial institutions.[5] Additional examples include the interagency guidance on third-party risk management[6] and the interagency paper on operational resilience.[7] Each of these efforts, which incorporated significant feedback from industry, led to workable standards and guidelines that also satisfy the needs of regulators.

While joint guidance and rules help provide much-needed clarity and consistency for firms and support the efficient use of resources, the collective effect of supervision and oversight can cause significant strain on personnel and the resources necessary to implement security solutions that keep pace with evolving threats. Although most cybersecurity requirements for financial institutions are not directly duplicative due to slight variations in regulators' authorities, they generally apply to the same activities, policies and procedures within firms. As a result, the same cyber and technology personnel are often responsible for responding to regulatory requests across agencies.

While regulators' focus on cybersecurity reflects the current threat environment and the increasing role technology plays in financial institution operations, the intensity, depth and frequency of regulatory requirements create their own operational challenges. When regulations and oversight activities are not well-coordinated, including coordination on exam scope and scheduling, firms must prioritize compliance activities over other security program priorities and risk mitigation efforts.

As an example, 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 firms reported their Chief Information Security Officers or comparable senior cyber leaders spend between 30 to 50 percent of their time on those same regulatory compliance matters. During examinations, financial institutions often produce hundreds, and sometimes thousands, of pages of documents responding to regulatory requests.

Diverting finite cyber resources in this way leaves less time for risk mitigation activities and strategic security initiatives to fortify firm defenses moving forward. For example, several banks reported pausing or extending timeframes for implementing new initiatives or preparing for threats from artificial intelligence or quantum computing until they resolve findings from exams. Other firms did not modify timing for similar strategic initiatives, but reported staff working exceptionally long hours to maintain routine security operations while undergoing an exam. In many cases, this led to staff burnout and attrition among critical cyber personnel.

---

[5] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 12 C.F.R. § 53 (2021).
[6] Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37920 (Jun. 9, 2023).
[7] U.S. Fed. Reserve Bd. of Governors, Interagency Paper on Sound Practices to Strengthen Operational Resilience (2020).

Differences in how regulators approach their supervisory and oversight responsibilities is inevitable. As a general matter, though, it is imperative that all regulators consider existing requirements and do not duplicate or create variations of what already exists. We have seen this does not always occur—particularly with independent regulatory agencies like the SEC. A clear focus on establishing common cyber requirements and enhanced regulator coordination would help entities better defend against sophisticated cyber threats while also responding to regulatory inquiries in a timely fashion.

Regulatory Reciprocity

Regulatory reciprocity refers to one regulator accepting the results of oversight activities performed by another regulator on the same or similar topic. Implementing a reciprocity model would be particularly valuable for sectors with multiple regulators and would alleviate the need for entities to demonstrate compliance with the same requirements multiple times.

Based on our survey, financial institutions reported that only 30 percent of exam documentation can be reused due to slight differences in exam scope and cadence between different regulators. Similarly, firms also said that 25 percent of the information requests received during exams were duplicative or similar in scope. Repackaging exam responses to account for modest variations in exam scope consumes significant staff resources and leaves less time for core security activities.

By better leveraging each other's documentation, testing, evaluations and findings, regulators would receive the information they need to conduct rigorous oversight while preserving the ability of cybersecurity teams to adjust to rapid technological change. Without that bandwidth, regulated entities could be ill-prepared to defend against future threats.

Common Frameworks

Last, existing standards and frameworks can be helpful tools for navigating complex regulatory requirements. Like many other critical infrastructure sectors, financial institutions use NIST's Cybersecurity Framework to inform and prioritize cyber risk management.

In fact, the Cyber Risk Institute developed the Financial Sector Profile—which is based on NIST's Cybersecurity Framework—but additionally integrates regulatory requirements unique to the financial sector.[8] This provides financial institutions with a single, scalable resource for managing cyber risk and compliance requirements.

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

Regulators can similarly leverage common frameworks to tailor oversight priorities and more efficiently determine a company's baseline security posture. The common terms and controls in frameworks like the Financial Sector Profile also provide regulators with comparable results across a given sector to help identify potential systemic risks.

Conclusion

Over the last several years the patchwork of state, federal and international cyber regulatory requirements has expanded significantly, contributing to overlap, duplication and even conflict among requirements. The current approach imposes significant costs and unintended effects that are not always commensurate with a corresponding reduction in risk.

We welcome the Committee's focus on this important issue and support congressional action to help solve these significant challenges. A thoughtful, harmonized approach to streamline existing requirements will provide cyber professionals with the time they need to protect their organizations while providing government agencies with access to the information they need to fulfill their oversight responsibilities. To that end, we are committed to working with the Committee as it explores potential legislative solutions for achieving broader harmonization.