October 31, 2023

Via Electronic Mail

Ms. Kemba Walden
National Cyber Director, Acting
Office of the National Cyber Director
Executive Office of the President
1600 Pennsylvania Avenue NW
Washington, DC 20500

Re: Request for Information on Cybersecurity Regulatory Harmonization

Dear Ms. Walden,

The Bank Policy Institute ("BPI") and American Bankers Association ("ABA") (collectively, the "Associations") welcome and appreciate the Office of the National Cyber Director's ("ONCD") Request for Information on Cybersecurity Regulatory Harmonization ("RFI"). This is an important opportunity to assess the effect of overlapping and duplicative regulation and develop a streamlined framework to improve security across critical infrastructure sectors.

The Associations support the National Cybersecurity Strategy's focus on improving baseline security practices across industry sectors. The strategy also recognizes that increased regulatory focus on cybersecurity, if not carefully calibrated and aligned across government and independent regulators, can have unintended adverse effects. As the Federal government contemplates harmonizing existing cyber regulations and where new regulatory regimes might be appropriate, we encourage a balanced approach that considers the effect on front-line cybersecurity personnel to ensure they are able to meet compliance requirements while maintaining critical day-to-day operational responsibilities.

Financial institutions have complied with myriad security, privacy, operational resilience and third-party risk management requirements for decades and have worked closely with prudential financial regulators—the Office of the Comptroller of the Currency ("OCC"), Federal Reserve Board ("FRB"), and the Federal Deposit Insurance Corporation ("FDIC")—to encourage coordination where possible. We offer the following recommendations based on these experiences:

- **Regulators should coordinate with each other to lessen the effect of overlapping requirements**—Most cybersecurity requirements for financial institutions are not directly duplicative due to slight variations in regulators' authorities. However, they

generally apply to the same sets of activities, policies, and procedures within firms. The collective effect of supervision and oversight can cause significant strain on firms' personnel, resources and ability to focus on innovation and keeping up with dynamic threats. Regulators should be cognizant that their requirements may overlap and should work with each other to coordinate and share information so the regulated entity can focus on risk management activities rather than compliance.

- **Regulators should have practical experience and subject matter expertise**—Effective oversight requires that agency staff be well-versed in the industries they regulate. This expertise helps promote realistic supervisory expectations and allows cyber professionals to spend more time on security operations.

- **Common standards and frameworks can support effective risk management and supervision**—By leveraging established frameworks, regulated entities can prioritize resources and make well-informed security investments. Common standards also allow regulators to tailor examinations and generate comparable responses across regulated entities.

- **Increased regulatory reciprocity will help cyber professionals keep pace with rapidly evolving threats—**A holistic reciprocity framework with streamlined oversight requirements would relieve regulated entities from demonstrating compliance with the same or substantially similar requirements to multiple regulators.

I. Financial Services Cyber Regulatory and Supervisory Landscape

Financial institutions are subject to complex cyber regulatory and supervisory requirements. These requirements are not confined to a single law or enforced exclusively by one regulator. Instead, several statutory regimes outline cybersecurity mandates for financial firms on a broad range of topics including cyber incident reporting, risk management, governance, third-party oversight, and operational resilience. The Gramm Leach Bliley Act ("GLBA") also established data privacy and security requirements implemented and enforced by several Federal regulators. In fact, the Cyber Incident Reporting Council's recent report identified eight distinct cyber incident reporting requirements applicable to the financial sector alone.[1]

As part of supervisory examinations, the prudential banking regulators examine whether firms operate in a safe and sound manner. Other regulators like the Consumer Financial Protection Bureau ("CFPB") and the Commodity Futures Trading Commission ("CFTC") also conduct similar examinations of financial institutions. These examinations evaluate compliance with relevant statutory requirements and whether banks implement appropriate security controls. The largest financial institutions have on-site examiners, who conduct several reviews related to cybersecurity each year. The length of those exams vary, but can last anywhere from three to

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

twelve weeks. Banks must then remediate any issues identified by examiners or be subject to fines or other business and operating restrictions.

A. Regulatory Authorities

The below section outlines the various regulatory requirements applicable to financial institutions. These include obligations for cyber incident reporting, incident disclosure, consumer breach notification, data security, and data privacy. These requirements are enforced by the prudential banking regulators, the U.S. Department of Treasury ("Treasury"), the Cybersecurity and Infrastructure Security Agency ("CISA"), CFTC, CFPB, the Federal Trade Commission ("FTC"), the Securities and Exchange Commission ("SEC"), and the New York Department of Financial Services ("NYDFS").

1. Cyber Incident Reporting, Disclosure, and Notification Requirements

a. Cyber Incident Reporting

While the RFI does not focus on harmonizing cyber incident reporting requirements specifically, it is worth noting that banks must comply with several reporting requirements with varying timelines, definitions, and thresholds. In general, financial institutions provide these reports to regulators on a confidential basis to enhance visibility of the cyber threats facing the sector.

One such requirement is the Computer-Security Incident Notification Rule issued jointly by the prudential banking regulators.[2] Under the rule, firms must notify regulators "as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred."[3] Banks can provide this notification via email, telephone, or other similar methods proscribed by Federal banking regulators.[4]

The prudential regulators previously issued separate guidance under GLBA "to address unauthorized access to, or use of customer information that could result in substantial harm or inconvenience to a customer."[5] Much like the notification rule above, this guidance was meant to "provide an early warning to allow an institution's regulator to assess the effectiveness of an institution's response plan, and, where appropriate, to direct that notice be given to customers."[6] The final guidance directs banks to notify "its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information."[7]

---

[2] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 (Nov. 23, 2021).
[3] *Id.* at 66442.
[4] *Id.*
[5] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15737 (Mar. 29, 2005).
[6] *Id.* at 15741.
[7] *Id.* at 15752.

Another requirement applicable to banks is the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA").[8] This law requires covered entities to report incidents to the CISA "not later than 72 hours after the covered entity reasonably believes that [a] covered cyber incident has occurred."[9] Moreover, covered entities must report all ransom payments within 24 hours.[10] Additional requirements may emerge as CISA conducts its ongoing rulemaking process to implement CIRCIA.

The CFTC's System Safeguards Rule also has incident reporting requirements for specified financial institutions including derivatives clearing organizations and swap data repositories.[11] Under that rule, those institutions are required to "promptly" notify the CFTC of cyber incidents and other system malfunctions.[12]

At the state level, NYDFS requires firms to report cyber incidents "as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred."[13] The NYDFS rule provides two thresholds for providing notice to NYDFS. First, banks must report to NYDFS any cyber event that triggers notice "to any government body, self-regulatory agency or any other supervisory body."[14] Second, financial institutions must also report "cybersecurity events that have a reasonable likelihood of materially harming any material part of [its] normal operations."[15]

Last, while broader in scope, the Bank Secrecy Act requires banks to file Suspicious Activity Reports (SARs) with Treasury's Financial Crimes Enforcement Network when they identify certain types of suspicious activity—including cyber incidents.[16] From a timing standpoint, banks must file SARs "no later than 30 calendar days after the date of initial detection by the bank."[17]

b. Cyber Incident Disclosure

Beyond confidential incident reporting, firms have public cyber incident disclosure requirements. In July 2023, the SEC approved the primary disclosure requirement applicable to most financial institutions known as the Public Company Disclosure Rule.[18]

---

[8] Cyber Incident Reporting for Critical Infrastructure Act, 6 U.S.C § 681 (2023).
[9] *Id.* at § 681(b).
[10] *Id.*
[11] System Safeguards Testing Requirements for Derivatives Clearing Organizations, 81 Fed. Reg. 64322 (Sept. 19, 2016); Swap Data Repositories: Registration Standards, Duties, and Core Principles, 76 Fed. Reg. 54538, 54585 (Sept. 1, 2011).
[12] *Id.*
[13] 23 NYCRR § 500, 500.17 (2021).
[14] *Id.*
[15] *Id.*
[16] Reports By Banks of Suspicious Transactions, 31 C.F.R. § 1020.320 (2023); U.S. DEP'T OF TREASURY, ADVISORY TO FINANCIAL INSTITUTIONS ON CYBER-EVENTS AND CYBER-ENABLED CRIME (Oct. 2016), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005.
[17] Reports By Banks of Suspicious Transactions, 31 C.F.R. § 1020.320 (2023).
[18] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896, 51944 (Aug. 4, 2023).

According to the SEC, its public disclosure requirements are necessary because "investors need more timely and consistent cybersecurity disclosure to make informed investment decisions."[19] Although the SEC views its rule through that lens, it directly conflicts with most cyber incident reporting requirements documented above in both scope and purpose. In fact, the Cyber Incident Reporting Council recently identified the SEC's rule as an example of a duplicative cross-sector reporting requirement.[20] The rule itself requires public companies to disclose material cybersecurity incidents within four business days on Form 8-K.[21] This includes disclosing ongoing and unremediated incidents which can introduce additional risk to victim companies, third parties, or similarly situated entities in that sector.[22]

Requiring disclosure in those circumstances stands in stark contrast to the confidential and measured approach taken by the prudential financial regulators and Congress through CIRCIA to enhance cyber threat information sharing and reduce risk. The rule also requires firms to disclose its cyber risk management practices on Form 10-K.[23] These disclosures must be made with sufficient detail to allow investors "to ascertain a registrant's cybersecurity practices, such as whether they have a risk assessment program in place."[24] Overall, the Associations believe the SEC's rule requires public disclosure of considerably too much, too sensitive, highly subjective information, at premature points in time, without requisite deference to prudential regulators or relevant cybersecurity specialist agencies.

c. Consumer Breach Notification

In some circumstances, banks must provide consumers with individualized notice of a cyber incident. Financial institutions have these obligations at both the Federal and state level. The timing for providing notification to consumers and the information those notices must contain varies from requirement to requirement.

For banks, the first set of consumer breach notification obligations comes from implementing guidance issued by the prudential banking regulators under GLBA.[25] Under that guidance, when a financial institution becomes aware of unauthorized access to sensitive customer information, it must conduct a reasonable investigation to determine if that information has been or will be misused.[26] If, after reasonable investigation, a bank determines sensitive customer information has or is reasonably likely to be misused, it must notify affected customers "as soon as possible."[27]

---

[19] *Id.* at 51899.
[20] DEP'T OF HOMELAND SEC., HARMONIZATION OF CYBER INCIDENT REPORTING TO THE FEDERAL GOVERNMENT 12 (2023).
[21] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51896, 51904 (Aug. 4, 2023).
[22] *Id.* at 51904–05.
[23] *Id.* at 51912.
[24] *Id.*
[25] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15737, 15752 (Mar. 29, 2005).
[26] *Id.*
[27] *Id.*

At the state level, firms are subject to consumer breach notification laws enacted in each of the 50 states.[28] These laws generally mandate notice to consumers when a cyber incident involves unauthorized access to sensitive personal information.[29] The patchwork of varying requirements and nuances around whether notification is required, what data must be provided, to whom, and how can take considerable time and subject matter expertise.

For example, the timing for notifying consumers ranges from "without unreasonable delay" to no later than 60 days after a breach is discovered.[30] In some states, financial institutions must notify impacted customers of a breach at one of their vendors, while in others the requirement only applies to a breach at the financial institution. Further, states have different requirements for informing the state Attorney General, law enforcement agencies, and/or state administrative agencies. New Jersey's breach notification law, for instance, requires notification to State Police *prior* to notifying consumers.[31] Virginia, on the other hand, mandates simultaneous notification to the state Attorney General and consumers.[32] The fundamental differences around notification timelines, the lack of consistent definitions for key terms, notification triggers, and methods for providing notification to consumers diverts attention toward compliance obligations rather than important remediation and security work.

2. Data Privacy and Data Security

Title V of GLBA imposes data privacy and security requirements on financial institutions.[33] While GLBA establishes these general frameworks, several key regulations implement those requirements.

The first is the Privacy Rule, often called Regulation P, enforced by the CFPB for banks. Regulation P describes the various notices banks must provide to consumers and establishes the conditions under which nonpublic personal information can be disclosed to nonaffiliated third parties.[34] Second, under GLBA, the FTC, the prudential banking regulators, the National Credit Union Administration, and the SEC were tasked with establishing appropriate "administrative, technical, and physical safeguards" for financial institutions.[35] The prudential regulators issued a joint rule establishing standards for safeguarding customer information and requirements for developing and implementing an information security program.[36] The FTC's Safeguards Rule, has similar requirements including elements for implementing and maintaining a comprehensive information security program, designating a qualified individual to oversee the information

[28] *Cyber Incident Reporting Requirements & Notification Timelines for Financial Institutions*, BANK POLICY INSTITUTE (Apr. 30, 2022), https://bpi.com/cyber-incident-reporting-requirements-notification-timelines-for-financial-institutions/.
[29] *Id.*
[30] *Id.*
[31] N.J. STAT. § 56:8–163 (2019).
[32] VA. CODE § 18.2–186.6 (2019).
[33] Gramm Leach Bliley Act, 15 U.S.C. § 6801–02 (2023).
[34] Privacy of Consumer Financial Information (Regulation P), 76 Fed. Reg. 79025, 79028 (Dec. 21, 2011).
[35] Gramm Leach Bliley Act, 15 U.S.C. § 6801, 6805 (2023).
[36] Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Recission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8616 (Feb. 1, 2001).

security program, establishing a written incident response plan, encrypting all customer information, and implementing multi-factor authentication.[37]

3. Other Relevant Regulations

a. NYDFS Cybersecurity Requirements for Financial Services Companies

NYDFS's Part 500 regulation is noted above, however, the rule's requirements extend beyond cyber incident reporting. For example, Part 500 requires financial institutions to implement multi-factor authentication, encrypt nonpublic information, and conduct periodic vulnerability assessments.[38] It also requires banks to develop written policies for managing third-party risk and establish an incident response plan.[39]

b. CFTC System Safeguards Testing Requirements

In addition to incident reporting, the CFTC's System Safeguards Rule also outlines several testing requirements.[40] Among other things, the rule requires certain financial institutions to conduct "vulnerability testing, penetration testing, controls testing, security incident response plan testing, and enterprise technology risk assessment."[41]

B. Supervisory Authorities

When overseeing financial institutions, prudential banking regulators conduct thorough examinations to ensure banks operate in a safe and sound manner and comply with relevant regulations. The prudential banking regulators conduct these examinations in accordance with several authorities including the Federal Deposit Insurance Act, GLBA, and the Bank Service Company Act. To help promote uniform supervision, Congress created the Federal Financial Institutions Examination Council ("FFIEC") to "prescribe uniform principles and standards for the Federal examination of financial institutions."[42]

In general, financial institutions have a primary Federal regulator dictated by its charter. For example, the OCC is the primary regulator for all nationally chartered banks.[43] The FDIC is the primary regulator for state chartered banks who are not Federal Reserve members.[44] The FRB is the primary regulator for state chartered banks who are Federal Reserve members and all

---

[37] Standards for Safeguarding Customer Information, 86 Fed. Reg. 70272, 70307 (Dec. 9, 2021).
[38] 23 NYCRR § 500.5, 500.12, 500.15 (2021).
[39] *Id.* at § 500.11, 500.16.
[40] System Safeguards Testing Requirements, 81 Fed. Reg. 64272 (Sept. 19, 2016).
[41] *Id.*
[42] Financial Institutions Regulatory and Interest Rate Control Act, 12 U.S.C. § 3301 (2023); FFIEC members include the OCC, FRB, FDIC, CFPB, the National Credit Union Administration, and a State Regulator Liaison Committee. *About the FFIEC,* FFIEC, https://www.ffiec.gov/about.htm.
[43] *Laws & Regulations*, OFF. OF COMPTROLLER OF THE CURRENCY, https://www.occ.treas.gov/topics/laws-and-regulations/index-laws-and-regulations.html.
[44] *Examination Processes And Procedures*, FED. DEPOSIT INS. CORP., https://www.fdic.gov/resources/bankers/exam-processes-and-procedures/.

bank holding companies.[45] Nevertheless, multiple regulatory agencies often have overlapping authority over the largest financial institutions with multiple lines of business.

As noted above, banking regulators examine a firm's compliance with several statutes and regulations involving cybersecurity. For instance, while GLBA gives FTC and CFPB rulemaking authority, the statute gives prudential banking regulators supervisory authority to ensure banks comply with GLBA implementing regulations like the Privacy Rule and Safeguards Rule.[46] Regulators also conduct safety and soundness examinations to determine whether firms implement and maintain adequate information security controls. Finally, the Bank Service Company Act permits regulators to examine third-party service providers "to the same extent as if such services were being performed by the depository institution itself on its own premises."[47] Several months ago, the prudential regulators finalized additional joint guidance on third-party risk management with considerations for information security.[48]

II. Principles for Effective Regulation

As the prior section describes, financial institutions face a multifaceted and evolving cyber regulatory regime, with state, Federal and international requirements. The following section proposes several principles for achieving more effective and harmonized regulatory outcomes based on these experiences. The Associations recognize each critical infrastructure sector has unique cyber risks and resilience levels to account for, however, we believe the principles discussed below are generally applicable across industry sectors and would help advance regulatory coherence. As such, the key principles discussed below are: (1) coordination among regulatory agencies; (2) regulator expertise; (3) use of frameworks; and (4) regulatory reciprocity.

A. Coordination Among Regulators

ONCD's RFI references the FFIEC as a potential model that might be replicated across industry sectors. Within financial services, there is significant benefit to bringing together the regulatory agencies who comprise the FFIEC. For example, the FFIEC has issued several joint publications including a cybersecurity resource guide for financial institutions and perhaps most notably its IT Examination Handbook—which the FFIEC regularly updates.[49] Beyond those publications, the FFIEC also conducts training for examiners and coordinates with the Conference of State Bank Supervisors to encourage uniform examination principles.[50]

---

[45] FED. RESERVE, THE FED EXPLAINED: WHAT THE CENTRAL BANK DOES 64 (2021).
[46] Gramm Leach Bliley Act, 15 U.S.C. § 6805 (2023).
[47] Bank Service Company Act, 12 U.S.C. § 1867 (2023).
[48] Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37920 (Jun. 9, 2023).
[49] FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, CYBERSECURITY RESOURCE GUIDE FOR FINANCIAL INSTITUTIONS (2022); *IT Examination Handbook*, FED. FIN. INSTITUTIONS EXAMINATION COUNCIL (2023), https://ithandbook.ffiec.gov/.
[50] The Conference of State Bank Supervisors ("CSBS") supports state regulator efforts to develop supervisory principles that ensure safety and soundness, protect consumers, and foster innovation. *Policy*, CSBS, https://www.csbs.org/policy. The CSBS is a representative on the FFIEC State Liaison Committee. *FFIEC State Liaison Committee (SLC)*, FFIEC, https://www.ffiec.gov/slc.htm; *Examiner Education Office,* FFIEC, https://www.ffiec.gov/exam/default.htm.

Regardless of industry sector, bodies like the FFIEC could help regulators develop uniform standards and better communicate consistent expectations to regulated entities.

Outside of the FFIEC, the prudential banking regulators have coordinated several joint regulations and guidance documents. One such example is the Computer-Security Incident Notification Rule issued following months of dialog and consultation with firms.[51] Two additional examples include the recent interagency guidance on third-party risk management and the interagency paper on Sound Practices to Strengthen Operational Resilience issued in 2020.[52] Each of these efforts, which incorporated significant feedback from industry, led to workable standards and guidelines that also satisfy regulator needs.

While joint guidance and rules alleviate some compliance burden, examiners sometimes interpret and apply those requirements differently. Regulatory expectations are most complicated for large financial institutions supervised by several agencies with distinct mandates. Without thoughtful coordination, overlapping regulatory inquiries can strain resources and complicate efforts to enhance security.

With technology and cybersecurity playing a more pivotal role in most financial institutions, examinations on these topics have increased in both frequency and depth. Some firms reported that cyber-related exams increased by as much as 50 percent over the last several years. Firms can receive more than 100 requests for information leading up to an exam followed by anywhere from 75 to 100 supplemental requests during the exam. Collectively, financial institutions often produce hundreds, and sometimes thousands, of pages of documents when responding to these inquiries. These documents often contain highly sensitive information and underscores the importance of the joint Financial and Banking Information Infrastructure Committee ("FBIIC")-Financial Services Sector Coordinating Council ("FSSCC") effort to enhance data security protections for sensitive information submitted to regulatory agencies.[53]

Increased regulatory scrutiny for cyber has led to situations where several agencies conduct overlapping or consecutive exams on the same or similar topics. Some banks experienced a similar but distinct challenge where one regulator requested the same information across exams on different topics. Several other financial institutions reported that 25 percent of the information requests received during regulatory exams were duplicative or similar in scope.

Regulators are right to prioritize cybersecurity given the risk cyber threats present for financial institutions. Nonetheless, when examinations are not well coordinated in scope and timing, banks experience several significant challenges and the risk of potential operational disruption increases. Perhaps the most significant challenge is the resource and staff strain accompanying regulatory exams. On an annual basis, responding to exam requests often consumes thousands of staff hours and some firms dedicate upwards of a dozen employees to

---

[51] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 12 C.F.R. § 53 (2021).

[52] Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37920 (Jun. 9, 2023); U.S. FEDERAL RESERVE BD. OF GOVERNORS, INTERAGENCY PAPER ON SOUND PRACTICES TO STRENGTHEN OPERATIONAL RESILIENCE (2020).

[53] FIN. AND BANKING INFORMATION INFRASTRUCTURE COMMITTEE & FIN. SERVICES SECTOR COORDINATING COUNCIL, FBIIC-FSSCC JOINT DATA PROTECTION WORKING GROUP REPORT 3 (2022).

identify exam questions, collect pertinent materials, and organize responses to examiners. Moreover, many banks spend hundreds of millions of dollars on cyber-related internal and external costs—including significant percentages of their cyber budgets on regulatory compliance. One reason exams are resource intensive is because only a very small percentage of exam responses are reusable across different regulators. This is primarily due to discrete differences in exam scope and timing. Exams also consume significant resources because additional regulator focus on cyber creates a cascading effect within a financial institution's risk management program. For example, as regulators devote more attention to second line governance and third line audit teams, there is a simultaneous increase in demand on first line compliance staff. To help manage the workload, many firms hired additional staff or engaged consultants. It should be noted, however, that the deep operational subject matter expertise required for regulatory engagements cannot be easily supplemented by additional administrative staff.

Even with increased staff, several banks paused or extended timeframes for completing strategic initiatives to enhance security, like implementing zero trust initiatives or preparing for threats from artificial intelligence or quantum computing, until they resolve the findings from exams. Other firms did not modify timing for similar strategic initiatives, but reported staff working exceptionally long hours to maintain day-to-day security operations while undergoing an exam. In many cases, this led to employee burnout and decreased morale. As regulatory exams increase in depth and frequency, financial institutions are compelled to divert critical resources from security to compliance. Without a reassessment of current exam procedures, firms could face additional risk because fewer staff are available to focus on identifying and remediating material threats.

There will always be differences between each regulator's approach to supervisory and oversight responsibilities. This notwithstanding, a clear focus on establishing common cyber requirements and enhanced regulator coordination—regardless of sector—can help regulated entities balance the demands of defending their organizations from sophisticated cyber threats while also responding to regulatory inquiries in a timely fashion.

B. Regulator Expertise

Effective regulatory oversight requires that agency staff have sufficient functional area expertise and understand the complexities of the industry they oversee. For cybersecurity, this need is even more acute because unfocused or unclear compliance demands can consume time normally spent on network and enterprise security operations.

To avoid this, any new regulatory frameworks should adopt a risk-based, non-prescriptive approach to cybersecurity oversight. This would allow regulated entities to focus on the most significant threats facing their enterprises, but also provide regulators with a more accurate representation of an entity's security posture. While important, overemphasis on compliance or administrative processes diverts resources away from the critical task of identifying and remediating material risks. It can also lead to increased investment in cyber capabilities not aligned with an entity's risk profile and compensating controls.

Beyond adopting a risk-based approach, regulators should clearly articulate the scope and expectations prior to an exam and maintain that standard as an exam progresses. Any subjective changes to those expectations forces entities to make frequent revisions to exam responses—again diverting valuable time from front line security activities.

While financial regulator examination and supervisory authorities are unique, the importance of expertise is not. To effectively oversee an organization, regulators must understand its business model, overall structure and technology. Investing the time to do so will help familiarize regulators with an organization's internal processes—including the role of the Board and senior managers as it relates to cyber risk management. This familiarity will also help reduce regulatory findings based on unrealistic expectations or issues beyond an organization's control—like issues at third or fourth parties that exceed contractual obligations.

Nevertheless, to some degree experience is an element of expertise made difficult by the regular transition of examiners as they rotate to new assignments every two to three years. Learning an organization's processes and procedures is no trivial task—particularly for financial institutions with complex cyber environments. Doing so requires significant training from regulatory agencies as well as background and other informational materials from the entities they supervise. That training helps provide important context and facilitate a productive regulatory environment where findings—and their relation to specific regulations—are clearly articulated and aligned to the entity's business model and operations. Extending examiner assignments or having new examiners overlap with the outgoing team for a period of time would allow those individuals—and the firms they oversee—to fully benefit from the training and experience an examiner receives on assignment.

C. Use of Frameworks

Existing standards and frameworks are valuable tools for navigating complex regulatory environments. Financial institutions, like many other sectors, have long leveraged the National Institute of Standards and Technology's ("NIST") Cybersecurity Framework ("CSF") to inform and prioritize cyber risk management.

In fact, several years ago, the FSSCC mapped cyber regulatory expectations to the CSF and found the majority "aligned with the cyber risk management outcomes expressed in the CSF's functions, categories, and subcategories."[54] Following that determination, the FSSCC launched an initiative to develop a financial sector specific framework that industry and regulators could use to inform compliance processes.[55] This extensive consultation between firms and regulators led to the creation of the Cyber Risk Institute's ("CRI") Financial Sector Profile ("Profile").

The Profile uses the CSF's five functions as its foundation, but adds two additional functions of significant interest to regulators—governance and supply chain management. Moreover, the Profile integrates regulatory requirements unique to the financial sector. This

[54] CYBER RISK INST., THE CYBER RISK INSTITUTE PROFILE: A FINANCIAL SECTOR USE CASE OF THE NIST CYBERSECURITY FRAMEWORK 2 (2023).
[55] *Id.* at 3.

includes references to international standards for firms with a global presence. As such, the Profile provides financial institutions with a concentrated and scalable resource to manage cyber risk and compliance practices. For example, banks can leverage the Profile's tiering questionnaire to determine the security controls they should implement based on their respective risk posture.

Using the Profile, firms can mitigate perennial challenges like resource prioritization to make more informed and deliberate security investments. The common terminologies set out in the Profile also present opportunities for enhanced collaboration with similarly situated institutions and peers.

Common frameworks, like the Profile, also offer significant benefits for regulators. Recognizing this, the OCC included the Profile in its Cybersecurity Supervision Work Program which outlines high-level examination objectives and procedures.[56] Moreover, other entities including the CFTC, FDIC, FFIEC, FRB, NIST, NYDFS, and Treasury all reference the Profile as an established industry standard and encourage its use.[57] Among other things, regulators can use the Profile to tailor examination priorities and efficiently determine an organization's baseline security posture. Perhaps most important, the Profile's common terms and controls provide regulators with comparable regulatory responses from financial institutions to get a better sense of the systemic risks facing the sector. While the Profile was developed for the financial sector, it serves as a model other sectors can use to develop their own tools for managing, streamlining, and prioritizing their cybersecurity programs.

The Financial Stability Board's ("FSB") recent work on a common framework for global cyber incident reporting serves as another good example of alignment and harmonization across regulatory jurisdictions that benefits both firms and regulatory authorities.[58] The FSB's recent report on this topic identified several practical issues regulators and financial institutions encounter when collecting and using cyber incident information.[59] These issues include operational challenges, varying reporting thresholds, and inconsistent definitions.[60] To address those challenges, the FSB recommended that regulators adopt common data requirements and reporting formats.[61] In particular, the FSB recommended that financial regulators "may also consider accepting the format and content of a cyber incident report that [financial institutions] must submit to their main supervisory or oversight authority."[62]

---

[56] U.S. DEP'T OF TREASURY, OCC BULLETIN 2023-22, CYBERSECURITY: CYBERSECURITY SUPERVISION WORK PROGRAM (2023).
[57] CYBER RISK INST., THE INDUSTRY'S STANDARD: GLOBAL SUPPORT FOR THE PROFILE 3–6 (2023).
[58] The FSB is an international coordination body that brings together national financial authorities and international standard-setting bodies to promote the stability of international financial markets. *About the FSB,* FIN. STABILITY BD., https://www.fsb.org/about/; FIN. STABILITY BD., RECOMMENDATIONS TO ACHIEVE GREATER CONVERGENCE IN CYBER INCIDENT REPORTING 1 (2023).
[59] FIN. STABILITY BD., RECOMMENDATIONS TO ACHIEVE GREATER CONVERGENCE IN CYBER INCIDENT REPORTING 7 (2023).
[60] *Id.*
[61] *Id.*
[62] *Id.* at 13.

As part of that same effort, FSB developed a common format for incident reporting exchange ("FIRE") to help reduce operational challenges for financial institutions and enhance cyber threat information sharing among regulators.[63] The FIRE concept would benefit banks because it proposes "a single, but flexible, set of data fields that could satisfy the reporting needs of multiple [regulatory] stakeholders."[64] For regulators, "the structured elements of a common reporting format facilitate the ability to compare and contrast incident occurrences on a historical, cross-border or cross-sectoral basis."[65]

D. Regulatory Reciprocity

As described above, the financial sector has many cyber requirements—including several that are not well-harmonized. This complicates the development and implementation of a regulatory reciprocity model for financial firms, but regulatory reciprocity remains an end goal worth pursuing. Successfully integrating a reciprocity model would provide regulators with the information they need to conduct rigorous oversight, but also streamline compliance burden so regulated entities can devote more time to day-to-day security activities and strategic resiliency improvements.

The RFI proposes a potential regulatory reciprocity model whereby a "primary" or "principal" regulator enforces baseline cybersecurity requirements. For sectors with only a few regulators, identifying which agency would fill that "primary" role is straightforward. Within financial services or other more complex sectors, that calculation is more challenging given the unique authorities and mandates of each Federal regulator.

Despite that challenge, all sectors would benefit from an increased reliance on a clearly defined primary regulator. Designating a primary regulator for each sector would not foreclose other agencies with overlapping authorities from executing their own oversight responsibilities. It would simply require those secondary regulators to accept the results of oversight activities performed by the primary—including any findings. On this point, a critical element of any reciprocity model is that secondary regulators be prohibited from tacking on additional findings and remediation requirements beyond those already identified by the primary regulator.

A reciprocity model constructed in this way would be more efficient and alleviate the need for regulated entities to demonstrate compliance with the same requirements to multiple government agencies. At the same time, there would still need to be some mechanism for involving secondary regulators who previously conducted their own independent reviews. To help steer a middle ground, regulators could form joint oversight teams, led by the primary, allowing each agency to participate in the compliance process simultaneously. This happens on occasion in the financial sector, when one agency sits in on another agency's supervisory exam. When this occurs, banks do not have to present the same material multiple times and regulators do not expend valuable resources unnecessarily. This streamlining would allow regulated entities to devote more time to other security initiatives and regulators to leverage one another's expertise to achieve better regulatory outcomes.

---

[63] FIN. STABILITY BD., FORMAT FOR INCIDENT REPORTING EXCHANGE (FIRE): A POSSIBLE WAY FORWARD 5–6 (2023).
[64] *Id.* at 6.
[65] *Id.* at 7.

For financial institutions with multiple overlapping regulatory requirements or service providers with customers in multiple sectors, a regulatory reciprocity model with uniform and streamlined standards for cybersecurity oversight is increasingly necessary to keep pace with dynamic cyber threats. Such an approach would promote more effective resource allocation–both for firms and regulatory agencies–while encouraging ongoing security improvements without overburdening cyber professionals and diverting attention from broader enterprise-wide risk management.

While financial institutions collaborate with regulators on an ongoing basis through coordinative organizations like the FSSCC and the FBIIC, the day-to-day realities of cyber examinations often stretch cybersecurity teams thin. Through a recent survey of large financial institutions, several firms reported their security teams spend more than 70 percent of their time on regulatory compliance activities. Despite coordination on cyber exams at the policy level, many firms reported overlap and duplication through the exam process and the inability to reuse materials. Firms reported that only 30 percent of exam documentation can be reused due to slight differences in exam scope and cadence between different regulators.

The sheer volume of regulatory exam requests, post first-day preparations, with tight 24 to 48 hour turnarounds, along with shifting or unrealistic examiner expectations risks compromising firms' ability to implement their cyber, resilience, and technology modernization programs. This risk also underscores why regulators should not retread previous exam findings or impose subjective preferences on the firms they examine. Overall, regulators should adopt a holistic approach that considers existing requirements and how any additional obligations might affect regulated entities already challenged to balance compliance with day-to-day security operations.

As regulations continue to expand in number and scope, reciprocity among regulators will preserve the ability of cybersecurity teams to adjust to rapid technological change—particularly as hostile actors move to weaponize emerging technologies like artificial intelligence and quantum computing. Without that bandwidth, regulated entities could be ill-prepared to defend against these strategic threats.

To facilitate that flexibility, we encourage the ONCD and other policymakers to carefully consider ways to streamline existing requirements as well as develop more effective models for critical infrastructure sectors currently lacking regulation.

III. Conclusion

We welcome ONCD's focus on cyber regulatory harmonization. The current regulatory landscape for financial institutions—with significant overlap among multiple regulators—imposes significant costs with limited risk reduction benefits. Efforts to streamline and deconflict existing requirements will help cyber professionals spend more time addressing the critical threats facing their organizations. If you have any questions or would like to discuss these comments further, please contact Heather Hogsett at heather.hogsett@bpi.com or John Carlson at jcarlson@aba.com.

Sincerely,

/s/ Heather Hogsett
Heather Hogsett
SVP, Technology & Risk Strategy, BITS
Bank Policy Institute

/s/ John Carlson
John Carlson
VP, Cybersecurity Regulation & Resilience
American Bankers Association