June 9, 2025

Via Electronic Mail

The Honorable Scott Bessent
Secretary
U.S. Department of Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220

Dear Secretary Bessent,

In recent years, nation-state cyber adversaries have increasingly targeted and successfully compromised federal agencies, including the financial regulators. As the new administration evaluates its approach to cybersecurity and data protection, and assesses legacy challenges, we would like to highlight some perceived preparedness gaps and work in partnership with the U.S. government to protect our financial markets and ensure the health of the nation's economy.

We are deeply concerned about the cybersecurity risk management practices at federal regulatory agencies, and the need for critical reforms to ensure the supervisory process does not introduce unnecessary risk to firms through regulators' own security weaknesses. The recently disclosed cybersecurity incidents at the Office of the Comptroller of the Currency (OCC) and the Department of Treasury in December 2024 show that government agencies are increasingly the target of persistent and sophisticated nation state attacks that could disrupt financial markets and our economy. It is imperative that federal regulators recognize that they are equally a target of malicious actors and implement the same or substantially similar cybersecurity and incident response practices that they expect financial institutions to maintain.

To address similar challenges across all financial regulatory agencies, we encourage the Administration to implement the following recommendations:

(1) ensure agencies are held to the same or substantively similar security and data protection standards expected of financial institutions to include transparency and accountability for upholding these standards;

(2) enable firms to retain and house their own sensitive data needed for regulatory engagement;

(3) improve regulatory agencies' incident response processes to include notification and communication with regulated institutions; and

(4) consolidate and streamline examinations conducted by the financial regulatory agencies to reduce the amount of data being shared.

While this request is precipitated by the security breach of the OCC's email system,[1] inadequate security at regulatory agencies has been a long-standing issue. In the case of the OCC's incident, hackers likely had access to approximately 148,000 emails beginning in roughly May 2023.[2] The OCC did not learn of the breach until February 2025 when Microsoft notified the agency that it detected unusual activity on its email platform[3] and the OCC communicated in its first public notice on the incident that there was "no indication of any impact to the financial sector."[4]

During subsequent reviews, the OCC learned that the incident impacted sensitive information. On April 7th, the OCC determined that the breach qualified as a major incident triggering congressional notification requirements.[5] The next day, the OCC issued a press release on its notification to Congress and further clarified that the compromise included unauthorized access to "highly sensitive information relating to the financial condition of federally regulated financial institutions."[6]

Once informed of the incident, financial institutions activated their third-party risk management procedures to include disconnecting from the OCC and pausing the transfer of sensitive information to the agency. As firms work through the process for reconnecting to OCC systems, the agency has maintained communication with impacted institutions to provide updates. This continued dialogue will be critical for resolving any remaining concerns about the agency's data security practices, the security of its technology environment, and its incident management and notification procedures.

Strengthen Regulator Data Security Practices

With increasing frequency over the last few years, federal agencies have experienced significant cyber incidents. As firms are required to share non-public, highly sensitive information with regulators as part of the supervisory process, compromises at regulatory agencies could expose institutions' vulnerabilities and business information to malicious actors, putting them at a strategic disadvantage. After SolarWinds, the Financial Services Sector Coordinating Council formed a joint Data Protection Working Group with Treasury and the financial regulatory agencies. In 2022, this working group issued a report with recommendations for enhancing regulator data protection practices and incident notification.[7] Despite this work, the recent OCC breach and Consumer Financial Protection Bureau

[1] Letter from Rodney E. Hood, Acting Comptroller, Office of the Comptroller of the Currency, to Financial Institution CEOs (Apr. 14, 2025), https://www.occ.gov/news-issuances/news-releases/2025/nr-occ-2025-32a.pdf.
[2] Margi Murphy & Jake Bleiberger, *Hackers Spied on 100 US Bank Regulators' Emails for Over a Year*, BLOOMBERG (Apr. 8, 2025), https://www.bloomberg.com/news/articles/2025-04-08/hackers-spied-on-100-bank-regulators-emails-for-over-a-year?embedded-checkout=true.
[3] Letter from Rodney E. Hood, Acting Comptroller, Office of the Comptroller of the Currency, to Financial Institution CEOs (Apr. 14, 2025), https://www.occ.gov/news-issuances/news-releases/2025/nr-occ-2025-32a.pdf.
[4] Press Release, Office of the Comptroller of the Currency, OCC Reports Security Incident Involving Email System (Feb. 26, 2025), https://occ.gov/news-issuances/news-releases/2025/nr-occ-2025-13.html.
[5] Letter from Rodney E. Hood, Acting Comptroller, Office of the Comptroller of the Currency, to Financial Institution CEOs (Apr. 14, 2025), https://www.occ.gov/news-issuances/news-releases/2025/nr-occ-2025-32a.pdf.
[6] Press Release, Office of the Comptroller of the Currency, OCC Notifies Congress of Incident Involving Email System (Apr. 8, 2025), https://www.occ.gov/news-issuances/news-releases/2025/nr-occ-2025-30.html.
[7] FIN. & BANKING INFORMATION INFRASTRUCTURE COMMITTEE & FIN. SERVICES SECTOR COORDINATING COUNCIL, FBIIC-FSSCC JOINT DATA PROTECTION WORKING GROUP REPORT 11–12 (2022).

(CFPB) Inspector General report[8] demonstrate regulators have not implemented these recommendations.

In the CFPB instance, the Inspector General found that the CFPB lacks controls to limit access to confidential supervisory information (CSI). The IG conducted this review following a 2023 breach and recommended the CFPB update its guidance to reduce the risk of unauthorized data access. The report flagged that the CFPB lacks guidance for managing CSI breaches and "determining, enforcing, and documenting consequences for responsible employees."[9] Furthermore, the CFPB lacks a defined process for notifying financial institutions of breaches affecting their sensitive information.

Given the threat environment, regulators should strengthen their internal cyber policies and practices across the full set of cybersecurity control domains to require controls commensurate with those demanded of financial institutions as outlined in the 2022 Data Protection Working Group report. This includes consistent application of baseline cyber hygiene practices like multi-factor authentication, data minimization and least privilege access. Regulators should also review the design of enterprise platforms and any shared services, how those systems are kept secure, and whether they employ modern resilience techniques.

In addition, we recommend that the most experienced examiners who conduct rigorous cyber reviews of regulated entities also review internal agency systems. This would complement the agency audits conducted under the *Federal Information Security Modernization Act*, and more closely mirror the various methods financial institutions employ—including internal and external audit functions—to provide appropriate oversight. To ensure accountability and rebuild trust, regulators should be more transparent with industry about how they safeguard the sensitive information provided by firms during exams and ongoing supervision. The interagency guidance on third-party risk management reiterates that "it is important for a banking organization to identify, assess, monitor, and control risks related to third party relationships."[10] Without adequate transparency, financial institutions will be unable to assess similar risks facing the regulatory agencies, who are a critical third party.

Enable Firms to Retain Sensitive Data Within their Own Secure Systems

Cyber risk management—including oversight of third-party relationships—is a paramount concern for financial institutions as cybercriminals increasingly target supply chain weaknesses. This concern, in part, is generated by the inherent risk presented by sensitive firm data residing outside the firm's networks and the corresponding inability to ensure the security of that information. Federal agency systems are attractive targets for threat actors because they are concentrated repositories of sensitive information on multiple regulated entities.

---

[8] OFFICE OF INSPECTOR GEN., CONSUMER FIN. PROTECTION BUREAU, 2025-SR-C-005, THE CFPB CAN IMPROVE ITS SAFEGUARDS FOR PROTECTING CONFIDENTIAL SUPERVISORY INFORMATION 2 (2025), https://oig.federalreserve.gov/reports/cfpb-confidential-supervisory-information-may2025.pdf. The OIG report found CFPB's guidance does not properly limit access to confidential supervisory information in its system of record for supervisory activities. In addition, the OIG found CFPB's guidance for managing CSI breaches did not include expectations for assessing the severity of an incident, determining consequences for responsible employees, or a defined process for notifying affected supervised institutions of a CSI breach.

[9] OFFICE OF INSPECTOR GEN., CONSUMER FIN. PROTECTION BUREAU, 2025-SR-C-005, THE CFPB CAN IMPROVE ITS SAFEGUARDS FOR PROTECTING CONFIDENTIAL SUPERVISORY INFORMATION 2 (2025), https://oig.federalreserve.gov/reports/cfpb-confidential-supervisory-information-may2025.pdf.

[10] Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37920, 37927 (Jun. 9, 2023).

To better defend against these threats, regulators should stop requiring firms to submit sensitive data through online portals or via email and otherwise purge highly sensitive information in their possession. This includes but is not limited to sensitive technology and cybersecurity data such as penetration testing results, specific control weaknesses and third-party reports, as well as other confidential business information such as acquisition plans or new initiatives, succession plan documents and earnings previews.

Instead, firms should have the option to retain such data on their own secure systems, allowing regulators access via on-site review or on firm computers with security controls in place to limit downloading, copying or printing the information. Allowing firms to institute additional data access, redaction, and minimization methods for protecting sensitive information like vendor names, open vulnerabilities, names of individuals, and details on control weaknesses would further mitigate potential risks to systems maintained by both the government and financial institutions. While the OCC provided independent attestations for certain systems, requiring financial institutions to fully reconnect before they have met their own internal guidelines and thresholds for reconnection could put firms in the position of violating their own third-party risk management policies. Regulators compelling reconnection under such circumstances could introduce additional risk.

Improve Incident Management and Notification Processes

Financial institutions are expected to have incident response playbooks that include incident identification and internal escalation procedures, the use of outside counsel and forensics firms, and internal and external communications plans to establish clear channels for the accurate and appropriate flow of information. Based on the OCC's response to the latest incident, it appears that the agency lacked similar robust plans. This delayed initial communications and the sharing of critical details to financial institutions while forensic and discovery efforts took place. Moreover, the OCC's slow response to the incident far exceeded the 36-hour notification requirement that the OCC, Federal Deposit Insurance Corporation (FDIC) and Federal Reserve Board (FRB) impose on financial institutions to report computer security incidents.[11]

There were also inconsistencies between OCC headquarters and the guidance provided to firms by their local exam teams. For instance, while headquarters was managing the breach investigation and many firms had disconnected from OCC systems, some examiners were still expecting firms to continue submitting sensitive data to the OCC via existing channels. The OCC subsequently secured additional support, developed a communication plan, and deployed a legal discovery tool to expeditiously assess exposed information that was highly confidential. It would be worthwhile for all financial regulatory agencies to closely review their incident management processes and playbooks and ensure they adhere to best practices that are widely used across industry. Moreover, when a breach occurs, regulator requests for information should be suspended.

Within the U.S., financial institutions are subject to no fewer than ten distinct incident reporting requirements—all with different timelines, thresholds, and information requirements for reporting.[12]

---

[11] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 (Nov. 23, 2021).

[12] U.S. DEP'T OF HOMELAND SEC., HARMONIZATION OF CYBER INCIDENT REPORTING TO THE FEDERAL GOVERNMENT 9 (2023); U.S. DEP'T OF HOUSING & URBAN DEVELOPMENT, FED. HOUSING ADMIN., MORTGAGEE LETTER 2024-10, SIGNIFICANT CYBERSECURITY

Federal regulators, however, are not subject to the same time constraints when notifying private sector entities impacted by a government breach and must only do so "as expeditiously as practicable and without unreasonable delay."[13] Unauthorized access to personally identifiable, confidential, or proprietary business information carries substantial implications for financial institutions and the customers they serve. To best position firms to respond and mitigate any incident impacts, federal agencies should notify regulated entities whose information was compromised within 72 hours as recommended by the Data Protection Working Group report and as private entities will soon be required to do under the *Cyber Incident Reporting for Critical Infrastructure Act*.[14]

Consolidate Supervisory Exams

Financial institutions are subject to rigorous supervision and examinations from the OCC, the Federal Reserve Board, and the Federal Deposit Insurance Corporation, among others. During these reviews, resident examiners issue broad requests for information with frequent overlap and duplication between the various agencies. While there have been efforts to consolidate exams for the largest financial institutions as part of interagency coordinated cybersecurity reviews, progress has been limited because regulatory agencies continue to conduct additional cyber exams on top of the coordinated review. This duplication is compounded by examiners often requesting information far beyond what is necessary for determining whether a financial institution operates in a safe and sound manner. To limit supervisory overreach, requests for data as part of an exam should be subject to consistent review by senior supervisory officials to provide greater consistency across exam teams and minimize the collection and retention of unnecessary sensitive data.

In addition to the massive amounts of data firms must produce for exams, the frequency, depth and duration of exams has increasingly diverted firms' attention away from vital security work. Staff reported an average of 100 requests for information leading up to a supervisory examination followed by 75 to 100 supplemental requests during the exam—25 percent of which were duplicative of requests from other agencies. As part of the effort to protect sensitive data, it is critical that exam consolidation and reform be included. This approach would help refocus exams on outcomes rather than data gathering and help cyber defenders focus on security rather than responding to data requests.

Conclusion

As a nation, we will continue to face well-resourced and sophisticated cyber adversaries—including nation states and affiliated criminal organizations. Amidst this threat landscape, we must ensure that regulators adhere to modern best practices for cybersecurity and incident response and implement reforms to further reduce the risk they present to financial institutions. Doing so will enable better cybersecurity for the Federal government, and most importantly, the American people.

The financial services industry stands ready to partner with the administration and the regulators to ensure our financial markets are well guarded against our adversaries and protect the

---

INCIDENT (CYBER INCIDENT) REPORTING REQUIREMENTS (2024); U.S. DEP'T OF HOUSING & URBAN DEVELOPMENT, GINNIE MAE, APM 24-02, CYBERSECURITY INCIDENT NOTIFICATION REQUIREMENT (2024).

[13] 44 U.S.C § 3553 note.

[14] FIN. & BANKING INFORMATION INFRASTRUCTURE COMMITTEE & FIN. SERVICES SECTOR COORDINATING COUNCIL, FBIIC-FSSCC JOINT DATA PROTECTION WORKING GROUP REPORT 12 (2022); 6 U.S.C. § 681b(a)(1)(A).

vitality of the U.S. economy. We look forward to working collaboratively with you to develop an implementation plan that ensures our regulatory system does not introduce more risk than it mitigates.

Sincerely,

American Bankers Association
Bank Policy Institute
Managed Funds Association
Securities Industry and Financial Markets Association

cc: The Honorable Kristi Noem
Secretary
U.S. Department of Homeland Security
Washington, DC 20528

The Honorable Michael Faulkender
Deputy Secretary
U.S. Department of Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220