Audit Report
2024-IT-B-020
October 31, 2024

Board of Governors of the Federal Reserve System

2024 Audit of the Board's Information Security Program

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Executive Summary, 2024-IT-B-020, October 31, 2024

2024 Audit of the Board's Information Security Program

Findings

The Board of Governors of the Federal Reserve System's information security program continues to operate effectively at a level-4 *(managed and measurable)* maturity. We found that the Board has taken steps to strengthen its information security program since our 2023 Federal Information Security Modernization Act of 2014 (FISMA) audit report. For instance, the Board has updated its personnel security processes to help ensure position risk designations are documented and used in personnel security processes. However, we identified several areas in which the Board's information security program decreased in maturity from prior years.

To ensure that its information security program remains effective, the Board should

- develop a supply chain risk management strategy
- define a review and escalation process for alerts generated by the Board's data loss prevention tool
- consistently document system interconnections and required documentation
- perform vulnerability scanning on mobile devices and applications
- annually test, review, and approve the incident notification and breach response plan to maintain organizational cyber resiliency
- provide role-based privacy training to help ensure that individuals are knowledgeable and aware of their privacy roles and responsibilities
- perform targeted phishing exercises to increase the cyber awareness of the Board's executives and those with significant security responsibilities
- ensure that contractual requirements for the Board's cloud service providers for the timely reporting of incidents are consistent with federal requirements

Finally, 14 recommendations that we made in our prior FISMA audit reports remain open. We will continue to monitor the Board's progress in addressing these recommendations as part of future FISMA audits. We believe that if sufficient progress is not made to address our prior open recommendations as well as the 9 new recommendations in this report, the Board's information security program maturity rating could decline in 2025.

Recommendations

This report includes nine new recommendations designed to strengthen the Board's information security program in the areas of risk management, supply chain risk management, data protection and privacy, and security training. In its response to a draft of our report, the Board concurs with our recommendations and plans to provide us with plans of action and milestones to address each recommendation. We will monitor the Board's progress in addressing these recommendations as part of future FISMA audits.

Purpose

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Board. Our specific audit objectives, based on the legislation's requirements, were to evaluate the effectiveness of the Board's (1) security controls and techniques for selected information systems and (2) information security policies, procedures, standards, and guidelines.

Background

FISMA requires each inspector general to conduct an annual independent evaluation of their agency's information security program, practices, and controls for selected systems. The Office of Management and Budget's (OMB) *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* directs inspectors general to evaluate the maturity level (from a low of 1 to a high of 5) of their agency's information security program for fiscal year 2024. OMB notes that level 4 (*managed and measurable*) represents an effective level of security.

Recommendations, 2024-IT-B-020, October 31, 2024

2024 Audit of the Board's Information Security Program

Finding 1: Establishing an SCRM Strategy Can Help Manage Supply Chain Risk

Number	Recommendation	Responsible office
1	Develop an SCRM strategy that includes a. a supply chain risk appetite and tolerance. b. an enterprise SCRM governance structure. c. supply chain risk assessment processes that include mitigation strategies or controls.	Office of the Chief Operating Officer

Finding 2: Improving the DLP Monitoring and Reporting Functions Can Provide Greater Assurance Against Unauthorized Data Transfer

Number	Recommendation	Responsible office
2	Document and implement a baseline review and escalation process for DLP alerts.	Division of Information Technology

Finding 3: Consistently Documenting System Interconnections Can Effectively Mitigate Risks Associated With Information and Resource Sharing

Number	Recommendation	Responsible office
3	Reinforce the requirements for identifying and documenting system interconnections as part of the Board's training on its cyber risk management application, and require all relevant individuals to take the training.	Division of Information Technology
4	Evaluate and implement options to enforce the agency's existing guidance related to identifying and documenting system interconnections.	Division of Information Technology

Finding 4: Mobile Application Vulnerability Scanning Can Help Maintain a Secure Mobile Device Platform

Number	Recommendation	Responsible office
5	Develop and implement a mobile application scanning program that includes a vulnerability scanning solution and process to identify and remediate vulnerabilities.	Division of Information Technology

Finding 5: Strengthening Review and Testing Processes Can Ensure an Effective Response to an Incident or Breach

Number	Recommendation	Responsible office
6	Ensure that the Board's *Incident Notification and Breach Response Plan* is reviewed, tested, and approved annually.	Division of Information Technology

Finding 6: Requiring Role-Based Privacy Training for Individuals With Significant Privacy Roles and Responsibilities Can Help Them to Effectively Perform Their Duties

Number	Recommendation	Responsible office
7	Develop and implement a role-based privacy training program.	Division of Information Technology

Finding 7: Performing Targeted Phishing Exercises Can Increase the Cyber Awareness of High-Ranking Staff and Those With Significant Security Responsibilities

Number	Recommendation	Responsible office
8	Incorporate targeted phishing exercises into the Board's security awareness and training program and processes.	Division of Information Technology

Finding 8: Ensuring That Cloud Computing Vendor Contracts Are Consistent With Federal Requirements Can Help Ensure Timely Response to Information Security Incidents

Number	Recommendation	Responsible office
9	Update the Board's standard language in CSP contracts to ensure that it is consistent with FedRAMP's *Incident Communications Procedures* incident reporting requirements.	Division of Information Technology

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

MEMORANDUM

DATE: October 31, 2024

TO: Jeffrey Riedel
Chief Information Officer
Board of Governors of the Federal Reserve System

Patrick J. McClanahan
Chief Operating Officer and Acting Chief Financial Officer
Board of Governors of the Federal Reserve System

FROM: Khalid Hasan
Assistant Inspector General for Information Technology

SUBJECT: OIG Report 2024-IT-B-020: *2024 Audit of the Board's Information Security Program*

We have completed our report on the subject audit. We performed this audit pursuant to requirements in the Federal Information Security Modernization Act of 2014 (FISMA). Specifically, FISMA requires each agency inspector general to conduct an annual independent evaluation of the effectiveness of their agency's information security program and practices. As part of our work, we also reviewed security controls for selected agency systems and performed other technical tests. We plan to transmit the detailed results of this testing in separate memorandums. In addition, we used the results of this audit to respond to specific questions in the Office of Management and Budget's *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

We provided you with a draft of our report for your review and comment. In your response, you concur with our recommendations and note that plans of action and milestones will be developed to detail the steps the Board will take to address them. We have included your response as appendix C to our report.

We appreciate the cooperation that we received from Board personnel during our review. Please contact me if you would like to discuss this report or any related issues.

cc: Charles Young
Tannaz Haddadi
Annie Martin
Stephen J. Bernard
Craig Delaney

Contents

Introduction

Objectives

In accordance with the requirements of the Federal Information Security Modernization Act of 2014 (FISMA), our audit objectives were to evaluate the effectiveness of the Board of Governors of the Federal Reserve System's (1) security controls and techniques for selected information systems and (2) information security policies, procedures, standards, and guidelines. Our scope and methodology are detailed in appendix A.

Background

FISMA requires agencies to develop, document, and implement an agencywide security program for the information and the information systems that support the operations and assets of the agency, including those provided by another agency, a contractor, or another source.[1] FISMA also requires that each inspector general (IG) perform an annual independent evaluation to determine the effectiveness of the information security program and practices of their respective agency, including testing the effectiveness of information security policies, procedures, and practices for selected systems. To support independent evaluation requirements, the Office of Management and Budget (OMB), the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other stakeholders collaborated to develop the *FY 2023–2024 Inspector General Federal Information Security Modernization Act (FISMA) Reporting Metrics*.

The IG FISMA reporting metrics are grouped into nine security domains, which align with the five function areas in the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework). These five function areas are *identify*, *protect*, *detect*, *respond*, and *recover* (table 1).[2] The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks. Each of these function areas and domains includes a number of metrics that IGs are required to assess using a maturity model.[3]

[1] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014) (codified at 44 U.S.C. §§ 3551–3558).

[2] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018.

[3] As noted in the *FY 2023–2024 IG FISMA Reporting Metrics*, IGs should use the U.S. Department of Homeland Security's CyberScope application to submit the results of their metrics evaluation, including maturity level ratings. As such, we reported our detailed responses and assessment of the Board's progress in implementing these metrics in CyberScope. Because of the sensitive nature of our responses, they are restricted and not included in this report.

Table 1. NIST Cybersecurity Framework Security Functions, Objectives, and Associated IG FISMA Reporting Domains

Security function	Security function objective	Associated IG FISMA reporting domain
Identify	Develop an organizational understanding to manage cybersecurity risk to agency assets.	Risk management, supply chain risk management
Protect	Implement safeguards to ensure delivery of critical infrastructure services as well as to prevent, limit, or contain the impact of a cybersecurity event.	Configuration management, identity and access management, data protection and privacy, security training
Detect	Implement activities to identify the occurrence of cybersecurity events.	Information security continuous monitoring
Respond	Implement processes to take action regarding a detected cybersecurity event.	Incident response
Recover	Implement plans for resilience to restore any capabilities impaired by a cybersecurity event.	Contingency planning

Source: U.S. Department of Homeland Security, *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.1, February 10, 2023.

FISMA Maturity Model

The five levels of the maturity model are

1. *ad hoc*
2. *defined*
3. *consistently implemented*
4. *managed and measurable*
5. *optimized*

The foundational levels (1–3) of the model are geared toward the development and implementation of policies and procedures, and the advanced levels (4–5) capture the extent to which agencies institutionalize those policies and procedures. As noted in the *FY 2023–2024 IG FISMA Reporting Metrics*, within the context of the maturity model, OMB believes that achieving a level 4 (*managed and measurable*) or above represents an effective level of security.[4] Further details on the scoring methodology for the maturity model are included in appendix A.

[4] NIST defines *security and privacy control effectiveness* as the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the designated security and privacy requirements. National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5, updated December 10, 2020.

Summary of the Board's Information Security Program

The Board's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity.[5] We found that the Board has taken steps to strengthen its information security program since our 2023 FISMA audit report. For instance, the Board has updated its personnel security processes to help ensure position risk designations are documented and used in personnel security practices. However, the maturity of the Board's information security program has declined in several areas. This report includes 9 new recommendations designed to strengthen the Board's information security program in the areas of risk management, supply chain risk management (SCRM), data protection and privacy, and security training. In addition, all 14 of the recommendations made in prior years' FISMA audit reports that were open at the start of this audit remain open. We believe that if sufficient progress is not made to address our old and new open recommendations, the Board's information security program maturity rating could decline in 2025.

We identified the following areas in which the Board can mature its information security program:

- SCRM strategy. We found that while the Board has processes for risk management of third-party providers, the agency has not developed an SCRM strategy that defines an enterprise governance structure and supply chain risk assessment processes, mitigation strategies, or controls. As the Board increasingly adopts cloud-based systems, an SCRM strategy will help ensure that the agency's data are effectively secured by cloud service providers (CSPs).

- Data loss prevention (DLP) monitoring and reporting. We continue to identify weaknesses in coverage and configurations of the Board's DLP tool. In addition, the Board has not defined a review and escalation process to ensure that alerts generated by the DLP solution are reviewed timely. As we reported in 2016, the Board has not developed an insider threat program for its sensitive but unclassified information. While the Board has other tools and processes to support DLP, the Board's DLP solution is a key tool to mitigate insider threat risk.

- System interconnections. We found that information on the Board's system interconnections is not consistently documented in the agency's cyber risk management application. While this information can be stored outside the cyber risk management application, the lack of centralized system interconnection information affects the Board's ability to quickly identify systems that share data and contain the impact of a security incident in an interconnected system.

- Vulnerability scanning of mobile devices and applications. We found that mobile devices and applications are not included in the Board's vulnerability scanning program. As the agency looks to maintain and expand its mobile device offerings and application development efforts, a vulnerability scanning program can assist in identifying and mitigating security weaknesses.

[5] Appendix A explains the scoring methodology outlined in the *FY 2023–2024 IG FISMA Reporting Metrics*, which we used to determine the maturity of the Board's information security program.

- Testing and reviewing the data breach response plan. We found that the Board has not conducted an annual test of its *Incident Notification and Breach Response Plan* or ensured that the plan is reviewed and approved annually. Testing and reviewing the plan can help ensure organizational resiliency in a changing cybersecurity threat environment.

- Role-based privacy training. We found that the Board offers security and privacy awareness training to its workforce and also provides security updates to address risk areas. However, we found that the agency has not developed a role-based privacy training for individuals with specific privacy responsibilities. Developing and implementing a role-based privacy training program can help ensure that these individuals can effectively perform their duties.

- Targeted phishing exercises. We found that while the Board performs periodic phishing exercises for its workforce, it does not conduct targeted phishing exercises for executives or individuals with specialized security and privacy responsibilities. Performing these exercises based on roles could assist the Board in increasing the cyber awareness of its workforce.

- Contractual requirements for CSPs. We found that while the Board has developed standard cybersecurity language to include in contracts with its third-party providers, clauses for timely incident reporting do not align with federal requirements. With the Board's increasing adoption of cloud-based technologies, timely incident reporting can help ensure an effective response.

Finding 1: Establishing an SCRM Strategy Can Help Manage Supply Chain Risk

Recent security incidents that exploited vulnerabilities in federal agency supply chains highlight the importance of SCRM. We found that the Board does not have an SCRM strategy. In addition, we found that the Board's security control baseline currently requires a supply chain control regarding maintaining configuration control over organization-defined system components awaiting service and repair. However, we found that the Board does not have policies or procedures for implementing this control in its environment.

According to NIST Special Publication 800-161, Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, *SCRM* is a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. By identifying potential risks and developing plans, organizations can prepare for and respond to unexpected events and ensure supply chain security across their operations. Special Publication 800-161 states that SCRM is an enterprise activity that should be directed as such from a governance perspective, regardless of the specific enterprise structure. In addition, NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, requires that organizations develop and implement an enterprise SCRM strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. Special Publication 800-53 further states that the SCRM strategy should include, among other things, an unambiguous expression of the supply chain risk appetite and tolerance for the organization as well as acceptable supply chain risk mitigation strategies or controls.

Board officials informed us that they have been relying on the existing *Vendor Risk Management Standard* to cover their SCRM program. However, the *Vendor Risk Management Standard* does not contain all required components of an SCRM strategy, such as an SCRM governance structure. We believe that defining an SCRM strategy that includes a defined SCRM risk appetite and tolerance will help the Board determine the controls needed to effectively manage SCRM risks and develop associated policies and procedures to guide implementation.

Recommendation

We recommend that the chief operating officer (COO)

1. Develop an SCRM strategy that includes
    a. a supply chain risk appetite and tolerance.
    b. an enterprise SCRM governance structure.
    c. supply chain risk assessment processes that include mitigation strategies or controls.

Management Response

Management concurs with our recommendation and intends to develop a plan of action and milestones (POA&M) to address the recommendation. The Board's response also notes that the agency will work with us to confirm that the planned actions fully address the issues identified in our report.

OIG Comment

We look forward to reviewing the Board's POA&M to address this recommendation, and we will follow up on the Board's corrective actions as part of future FISMA reviews.

Finding 2: Improving the DLP Monitoring and Reporting Functions Can Provide Greater Assurance Against Unauthorized Data Transfer

DLP refers to a set of tools and processes used to ensure that sensitive data are not lost, misused, or accessed by unauthorized users. The Board leverages a commercially available DLP solution managed by the Federal Reserve System to reinforce existing information handling practices and policies to reduce the risk of disclosing sensitive information to unauthorized individuals.

The Board's DLP tool performs three overall functions (figure 1). First, the DLP tool monitors outbound data transmissions. Second, it detects whether confidential data are being transmitted to an uncontrolled destination and provides a warning to help the user to make an informed decision about proceeding with the transmission. Finally, confirmed transmissions of data to uncontrolled destinations are reported and subject to review. We found issues with the monitoring and reporting functions.

Figure 1. Three Basic Functions of the Board's DLP System

Source: Board of Governors of the Federal Reserve System, Division of Information Technology, *DLP Quick Reference Guide*.

In terms of monitoring, we found that the DLP tool was not effective in ensuring that sensitive agency data were protected from inadvertent or malicious exfiltration.[6] This ineffectiveness is caused by the tool's rulesets not functioning consistently across Board technologies and not being tailored to account

[6] Because of the sensitive nature of these issues, the details will be transmitted in a separate, restricted communication.

for the data exfiltration avenues we identified. As a result, the risk of undetected exfiltration of sensitive Board information is heightened.

The *FY24 CIO FISMA Metrics* highlights the importance of using technology, such as a DLP solution, to detect potential unauthorized exfiltration of information.[7] In addition, NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, notes that organizations can employ automated tools, such as DLP technologies, to monitor PII internally or at network boundaries for unusual or suspicious transfers or events. Our 2019 FISMA report includes a recommendation that the Board's chief information officer (CIO) work with the System to ensure that the DLP replacement solution both functions consistently across the Board's technology platforms and supports rulesets that limit the exfiltration weaknesses we identified, to the extent practicable.[8] When we made this recommendation, the Board was planning to replace its DLP solution. This year, we tested the DLP replacement solution, and we found similar issues. As such, our 2019 recommendation remains open.

For the reporting function, we found that the Board has not defined a review and escalation process to ensure that alerts generated by the DLP tool are reviewed timely. While the Board's DLP website contains guidance that the System uses for DLP alert review and escalation, the Board does not use or enforce this guidance.

NIST Special Publication 800-53, Revision 5, notes that audit record review, analysis, and reporting covers information security and privacy-related logging performed by organizations. Specifically, NIST Special Publication 800-53, Revision 5, requires agencies to review and analyze system audit records at an organization-defined frequency for indications of organization-defined inappropriate or malicious unusual activity and the potential impact of the inappropriate or unusual activity.

Board officials also informed us that they allow each division to determine its own DLP review procedures. We believe that a defined review and escalation process would provide a baseline from which the Board divisions could determine their own DLP review procedures based on risk.

Recommendation

We recommend that the CIO

2. Document and implement a baseline review and escalation process for DLP alerts.

Management Response

Management concurs with our recommendation and intends to develop a POA&M to address the recommendation. The Board's response also notes that the agency will work with us to confirm that the planned actions fully address the issues identified in our report.

[7] To support independent evaluation requirements, OMB, CIGIE, and other stakeholders collaborated to develop the *FY24 CIO FISMA Metrics*.

[8] Office of Inspector General, *2019 Audit of the Board's Information Security Program*, OIG Report 2019-IT-B-016, October 31, 2019.

OIG Comment

We look forward to reviewing the Board's POA&M to address this recommendation, and we will follow up on the Board's corrective actions as part of future FISMA reviews.

Finding 3: Consistently Documenting System Interconnections Can Effectively Mitigate Risks Associated With Information and Resource Sharing

A *system interconnection* is the direct connection of two or more information systems for the purpose of sharing data and other information resources. A system interconnection has three basic components: two information technology systems and the mechanism by which they are joined through which data are made available, exchanged, or passed one way. We found that information about the Board's system interconnections is not consistently included in the agency's cyber risk management application.[9] Specifically, of the 55 active business applications and cloud systems we analyzed, we determined that 40 have system interconnections. Of those 40, 11 (27.5 percent) either did not list system interconnections in the *Information Exchange* section of the cyber risk management application or did not attach the accompanying Interconnection Security Agreement, Memorandum of Understanding/Agreement, or Information Exchange Agreement in *the Information Exchange Documents* section.

NIST Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, requires that for each system interconnection, specific identifying information is documented in the system security plan, such as the name of the system, the type of interconnection, and the authorization for the interconnection. In addition, the Board's cyber risk management application desk manual stipulates that system interconnections should be documented in the *Information Exchange* section and supporting documentation should be added to the *Information Exchange Documents* section of the Board's cyber risk management application.

The system interconnection information in the agency's cyber risk management application is incomplete for two reasons. First, system owners are not consistently entering interconnections information in the Board's cyber risk management application. Second, Board officials informed us that they rely on the Board's cyber risk management application desk manual for guidance on storing system interconnections. However, the requirements in the manual are not enforced. The Board has trainings for its cyber risk management application; however, we found these trainings were high level and focused more on the process of using the tool than the specific information required in the tool.

Not having this information centralized in its cyber risk management application inhibits the Board's ability to quickly ascertain whether a system has interconnections. Further, the Board's ability to ensure that a security incident in an interconnected system does not compromise connected systems and the data they store, process, or transmit is impaired. As such, we believe that consistently documenting and

[9] The Board's cyber risk management application is used to inventory, review, and maintain the security posture of information systems.

storing system interconnection documentation will allow Board staff to effectively manage the risk associated with sharing information.

Recommendations

We recommend that the CIO

3. Reinforce the requirements for identifying and documenting system interconnections as part of the Board's training on its cyber risk management application, and require all relevant individuals to take the training.
4. Evaluate and implement options to enforce the agency's existing guidance related to identifying and documenting system interconnections.

Management Response

Management concurs with our recommendations and intends to develop POA&Ms to address the recommendations. The Board's response also notes that the agency will work with us to confirm that the planned actions fully address the issues identified in our report.

OIG Comment

We look forward to reviewing the Board's POA&Ms to address these recommendations, and we will follow up on the Board's corrective actions as part of future FISMA reviews.

Finding 4: Mobile Application Vulnerability Scanning Can Help Maintain a Secure Mobile Device Platform

As noted in NIST Special Publication 800-124, Revision 2, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, modern mobile devices are essentially general-purpose computing platforms capable of performing tasks far beyond the voice and text capabilities of legacy mobile devices. Mobile devices present a vector for phishing, social engineering, and malware distribution, which is why organizations should safeguard them with the same diligence as they would traditional computer devices, such as desktops and laptops. The Board uses modern mobile devices extensively; however, we found that although the Board has a tool capable of performing vulnerability scanning on mobile devices and applications, it does not intend to use the tool for that purpose.

Vulnerability detection on mobile devices can be achieved through a variety of means, including active scanning.[10] The U.S. Department of Homeland Security's Binding Operational Directive 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*, stipulates that as of April 3, 2023, where the capability is available, agencies must perform the same type of vulnerability enumeration on mobile devices and other devices that reside outside agency on-premises networks. In addition, the Board has developed a smartphone device infrastructure and mobile application development strategy that is designed to operationalize secure, cost-effective standards for the management of the mobile application life cycle. The strategy notes that the Board will use secure application standards, guidelines, and best practices in the development and use of mobile applications, as applicable, including vulnerability scanning.

Board officials did not provide a reason as to why they do not intend to use the vulnerability scanning tool for Board mobile devices. They informed us that they are evaluating other mobile scanning solutions.

Board officials also noted that the agency relies on the current mobile device management tool, which allows the Board to control the configuration of Board mobile phones and prevents information from being exchanged between Board-managed and unmanaged mobile applications.[11] Although a mobile device management tool can be used to quickly mitigate some security issues, it does not contain all the capabilities of a dedicated mobile scanning solution, such as identifying and eradicating a vulnerability on an application that already exists on a mobile device.

[10] Vulnerability scanners look for known vulnerabilities, particularly in software dependencies, and detect easily missed loopholes in application code, checking against a record of common vulnerabilities and their characteristics.

[11] A *managed application* is a mobile application installed on Board smartphones that requires access to internal Board resources listed in the *Approved Software Catalog*, including third-party applications. An *unmanaged application* does not require Board internal resources and is not listed in the *Approved Software Catalog*, but it may be installed from the app store using a personal account.

Because the majority of managed mobile applications that the Board uses are third-party applications, we believe that implementing a mobile scanning solution will complement the agency's mobile device management solution by providing insight into application- and code-level vulnerabilities.

Recommendation

We recommend that the CIO

5. Develop and implement a mobile application scanning program that includes a vulnerability scanning solution and process to identify and remediate vulnerabilities.

Management Response

Management concurs with our recommendation and intends to develop a POA&M to address the recommendation. The Board's response also notes that the agency will work with us to confirm that the planned actions fully address the issues identified in our report.

OIG Comment

We look forward to reviewing the Board's POA&M to address this recommendation, and we will follow up on the Board's corrective actions as part of future FISMA reviews.

Finding 5: Strengthening Review and Testing Processes Can Ensure an Effective Response to an Incident or Breach

In accordance with OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, the Board has developed an *Incident Notification and Breach Response Plan.* The plan sets forth the notification procedures to be used in the event of a security incident involving Board data, including an incident involving sensitive personally identifiable information or other confidential information, such as confidential supervisory information. The plan establishes a Core Response Group (CRG) that is responsible for responding effectively and efficiently to security incidents and privacy breaches. We found that the Board has not conducted an annual test of its incident notification and breach plan and has not ensured that it is reviewed and approved annually.

OMB Memorandum M-17-12 requires that agencies conduct an annual tabletop exercise of their breach response plan. The memorandum also requires that an agency's senior agency official for privacy (SAOP) review and approve the plan annually. Both requirements are also referenced in the Board's *Incident Notification and Breach Response Plan.* The plan specifically requires the CRG to conduct an annual tabletop exercise to test the plan to ensure that members of the CRG are familiar with the plan and understand their specific roles. The plan also states that the SAOP shall review it annually to confirm that it is current, accurate, and reflects any changes in law, guidance, standards, agency policy, procedures, staffing, or technology.

The Board was unable to complete the annual tabletop exercise and annual review of the plan because of competing priorities. Specifically, the Board's information security officer (ISO), who is designated by the CIO to carry out all aspects of the day-to-day operation and maintenance of the Board's information security program and the program's compliance with FISMA requirements, is also serving as the agency's SAOP. These roles have historically been performed by different individuals at the Board, in accordance with federal best practices;[12] additionally, these roles are defined as being separate and distinct in the Board's *Incident Notification and Breach Response Plan*. The responsibility on a single individual to cover both positions necessarily causes some tasks to be deprioritized.[13]

We believe that by conducting tabletop exercises and reviewing and approving the data breach response plan annually, the Board can ensure that team members understand and are prepared to defend against and respond to data breaches.

[12] OMB M-16-24, *Role and Designation of Senior Agency Officials for Privacy*, notes that privacy and security are independent and separate disciplines. Further, while privacy and security require coordination, they often raise distinct concerns and require different expertise and different approaches.

[13] While we are not making a recommendation in this area, we plan to initiate a review of information technology governance at the Board. This review may include the roles and responsibilities of the ISO and SAOP.

Recommendation

We recommend that the CIO

6. Ensure that the Board's *Incident Notification and Breach Response Plan* is reviewed, tested, and approved annually.

Management Response

Management concurs with our recommendation and intends to develop a POA&M to address the recommendation. The Board's response also notes that the agency will work with us to confirm that the planned actions fully address the issues identified in our report.

OIG Comment

We look forward to reviewing the Board's POA&M to address this recommendation, and we will follow up on the Board's corrective actions as part of future FISMA reviews.

Finding 6: Requiring Role-Based Privacy Training for Individuals With Significant Privacy Roles and Responsibilities Can Help Them to Effectively Perform Their Duties

The Board provides annual security and privacy awareness training but has not developed a role-based privacy training program for employees with specialized privacy roles and responsibilities. The *Fiscal Year 2024 Senior Agency Official of Privacy (SAOP) FISMA Reporting Metrics* highlights the importance of role-based privacy training for federal employees with privacy roles and responsibilities, including managers, before authorizing their access to federal information or information systems.[14] Specialized or role-based privacy training is also required by NIST Special Publication 800-53, Revision 5, which notes that roles that may require such training include senior leaders or management officials, system owners, authorizing officials, system security officers, and network and database administrators.

The Board has not prioritized the development of a role-based privacy training program; however, Board officials noted that the agency is working with the System to develop such training. We believe that a role-based privacy training program will ensure that individuals with significant privacy responsibilities can effectively perform their duties and help protect sensitive Board information.

Recommendation

We recommend that the CIO

7. Develop and implement a role-based privacy training program.

Management Response

Management concurs with our recommendation and intends to develop a POA&M to address the recommendation. The Board's response also notes that the agency will work with us to confirm that the planned actions fully address the issues identified in our report.

OIG Comment

We look forward to reviewing the Board's POA&M to address this recommendation, and we will follow up on the Board's corrective actions as part of future FISMA reviews.

[14] To support independent evaluation requirements, OMB, CIGIE, and other stakeholders collaborated to develop the *Fiscal Year 2024 SAOP FISMA Metrics*.

Finding 7: Performing Targeted Phishing Exercises Can Increase the Cyber Awareness of High-Ranking Staff and Those With Significant Security Responsibilities

Phishing is a type of cyberattack that uses social engineering techniques. In a phishing attack, a threat actor poses as a trustworthy acquaintance or a reputable organization to lure a victim into providing sensitive information or network access. These attacks can take different forms, often targeting specific group of individuals (*spear phishing*), or high-ranking members of organizations (*whaling*). While the Board conducts phishing exercises for the general staff population, it does not perform phishing simulations that are targeted to specific groups or individuals, such as high-ranking officials and individuals with significant security and privacy responsibilities.

NIST Special Publication 800-53, Revision 5, control AT-3, *Role-Based Training*, emphasizes that training should be specific to the roles and responsibilities of individuals with significant security duties. Additionally, the *FY 2023–2024 IG FISMA Reporting Metrics* highlights the importance of measuring the effectiveness of the agency's specialized security training program by, for example, conducting targeted phishing exercises and following up with additional training, as appropriate. In its *Cybersecurity Advisory: Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs*, the Cybersecurity and Infrastructure Security Agency also urges critical infrastructure owners to implement a user training program and conduct simulated spear-phishing attacks to discourage users from visiting malicious websites or opening malicious attachments and to reenforce the appropriate user responses to spear-phishing emails.[15]

Board officials informed us that they have not performed targeted phishing exercises because they have prioritized higher-risk issues. These same officials indicated that they plan to perform targeted phishing exercises as the program matures. We believe that conducting targeted phishing exercises will help the Board ensure that those who are most likely to be targeted or who have significant security responsibilities are not vulnerable to spear-phishing or whaling attempts.

[15] Cybersecurity and Infrastructure Security Agency, *Cybersecurity Advisory: Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs*, Alert Code AA21-148A, May 29, 2021.

Recommendation

We recommend that the CIO

8. Incorporate targeted phishing exercises into the Board's security awareness and training program and processes.

Management Response

Management concurs with our recommendation and intends to develop a POA&M to address the recommendation. The Board's response also notes that the agency will work with us to confirm that the planned actions fully address the issues identified in our report.

OIG Comment

We look forward to reviewing the Board's POA&M to address this recommendation, and we will follow up on the Board's corrective actions as part of future FISMA reviews.

Finding 8: Ensuring That Cloud Computing Vendor Contracts Are Consistent With Federal Requirements Can Help Ensure Timely Response to Information Security Incidents

The Board's cloud strategy requires integrating cloud computing into the agency's technology environment to take advantage of the advanced data integration, analytics, and external collaboration capabilities the cloud provides. Specifically, the Board has adopted a "cloud first" strategy that notes that cloud solutions should be the first or default option when seeking new technology solutions. As such, the Board has been increasingly migrating to cloud-based systems, and CSPs play an increasingly important role in the Board's information, communications, and technology supply chain. However, the Board's contracts with CSPs do not align with federal requirements for timely notification of information security incidents.

The Federal Risk and Authorization Management Program (FedRAMP) was established by OMB to safely accelerate the adoption of cloud computing services by federal agencies. FedRAMP's *FedRAMP Incident Communications Procedures* outlines requirements for CSPs with FedRAMP authorization to use when reporting information concerning information security incidents. CSPs must meet these requirements to retain their FedRAMP certification independent of any contract terms. These procedures require CSPs to report suspected and confirmed information security incidents to the following parties within 1 hour of being identified by the CSP's top-level Computer Security Incident Response Team, Security Operations Center, or information technology department:

- customers who are affected or who are suspected of being affected
- the Cybersecurity and Infrastructure Security Agency, if the CSP has confirmed, has yet to confirm, or suspects the incident is the result of a reportable attack vector
- FedRAMP points of contact
- agency points of contact

If a CSP fails to report an incident or a suspected incident, FedRAMP may issue a corrective action plan. A series of violations may result in the suspension of the CSP's FedRAMP authorization.

The Board information security contract clause for incident reporting by CSPs requires CSPs to notify the agency within 24 hours instead of 1 hour if there is a suspected or confirmed breach that has occurred that threatens the security of System information systems or the confidentiality of agency personally identifiable information contained therein. Board officials informed us that they recognize the potential conflict between the 1-hour reporting that applies to FedRAMP-authorized CSPs and the Board's standard contract language requiring notice within 24 hours. These same officials noted that they plan to modify

the Board's standard contract language to make it clear that the 24-hour reporting period does not override other reporting obligations.

We believe that there are several benefits to ensuring that the Board's cloud computing contract language aligns with FedRAMP requirements for incident reporting. As noted in the Board's cloud computing strategy, because not all technology products seek FedRAMP authorization, the Board is determining where FedRAMP exceptions should be made. By aligning its contractual requirements for incident reporting with FedRAMP requirements, the Board can ensure that all CSPs it contracts with have a clear understanding of incident reporting requirements, which should enable the Board and its CSPs to take timely action to prevent additional leaks and notify affected individuals.

Recommendation

We recommend that the CIO

9. Update the Board's standard language in CSP contracts to ensure that it is consistent with FedRAMP's *Incident Communications Procedures* incident reporting requirements.

Management Response

Management concurs with our recommendation and intends to develop a POA&M to address the recommendation. The Board's response also notes that the agency will work with us to confirm that the planned actions fully address the issues identified in our report.

OIG Comment

We look forward to reviewing the Board's POA&M to address this recommendation, and we will follow up on the Board's corrective actions as part of future FISMA reviews.

Appendix A: Scope and Methodology

Our specific audit objectives, based on FISMA requirements, were to evaluate the effectiveness of the Board's (1) security controls and techniques for selected information systems and (2) information security policies, procedures, standards, and guidelines. To accomplish our objectives, we reviewed the effectiveness of the Board's information security program across the five function areas outlined in the *FY 2023–2024 IG FISMA Reporting Metrics*. These five function areas are *identify*, *protect*, *detect*, *respond*, and *recover*. The five function areas consist of nine security domains: *risk management*, *supply chain risk management*, *configuration management*, *identity and access management*, *data protection and privacy*, *security training*, *information security continuous monitoring (ISCM)*, *incident response*, and *contingency planning*.

To assess the effectiveness of the Board's information security program, we

- used a risk-based approach and focused our detailed testing activities on the annual core metrics and supplemental fiscal year 2024 metrics identified in the *FY 2023–2024 IG FISMA Reporting Metrics*
- analyzed security policies, procedures, and documentation
- interviewed Board management and staff
- observed and tested specific security processes and controls at the program and information system level[16]
- performed data analytics using commercially available tools to support our testing in multiple security domains

To determine whether the Board's information security program is effective, we used the scoring methodology defined in the *FY 2023–2024 IG FISMA Reporting Metrics*. In accordance with the methodology, we determined maturity ratings at the cybersecurity function and domain levels and factored in our knowledge of the Board's risk environment to come to our conclusion. We entered our specific maturity ratings at the function and domain levels in the CyberScope FISMA reporting application.

We conducted this work from March 2024 to July 2024. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[16] We sampled systems using a risk-based approach that includes various factors, such as the system's purpose, the information maintained within the system, and the function of the system.

Appendix B: Status of Prior FISMA Recommendations

As part of our 2024 FISMA audit, we reviewed the actions taken by the Board to address the outstanding recommendations from prior FISMA audit reports. Below is a summary of the status of the 14 recommendations that were open at the start of our 2024 FISMA audit (table B-1). Based on our review, we determined that the 14 recommendations, which are related to risk management, identity and access management, data protection and privacy, security training, and ISCM, will remain open. We will update the status of these recommendations in our fall 2024 semiannual report to Congress, and we will continue to monitor the Board's progress in addressing our open recommendations as a part of future FISMA audits.

Table B-1. Status of 2016–2023 FISMA Recommendations That Were Open as of the Start of Our Fieldwork, by Security Domain

Year		Recommendation	Status	Explanation
Risk management				
2016	1	We recommend that the CIO work with the COO to perform a risk assessment to determine which aspects of an insider threat program are applicable to other types of sensitive Board information and develop and implement an agencywide insider threat strategy for sensitive but unclassified Board information, as appropriate.	Open	Board officials informed us that they have components of an insider threat program in place, such as a DLP solution and user activity monitoring. However, there remains no insider threat strategy in place to govern the various divisions and groups involved in insider threat activities. Further, no assessment has been done to determine which aspects of an insider threat program are applicable to other types of sensitive Board information.
2022	1	We recommend that the CIO ensure that risks are appropriately categorized and prioritized on the Board's cybersecurity risk register.	Open	The Board is planning to implement custom risk register fields within its FISMA compliance tool to require the categorization and prioritization of risks. This update to the tool is currently planned for the third quarter of 2024.
2023	1	We recommend that the CIO prioritize the definition and incorporation of a cybersecurity risk tolerance into the agency's cybersecurity policies, procedures, and processes, as appropriate.	Open	Board officials informed us that initial discussions have occurred for defining a cybersecurity risk tolerance and incorporating it into agency processes, as appropriate.

Year		Recommendation	Status	Explanation
2023	2	We recommend that the CIO ensure all required attributes are consistently documented within the agency's cybersecurity risk register.	Open	Board officials informed us they are working to enhance their reporting capabilities to show which required fields are not being completed so that appropriate action can be taken. After the end of our fieldwork, Board officials provided additional information and requested closure of this recommendation. We plan to follow up as part of future audits.
2023	3	We recommend that the CIO document and implement a process to consistently inventory the Board's web applications, including its public-facing websites.	Open	Board officials informed us that new fields were implemented in the Board's FISMA compliance tool to identify new domains and public-facing websites and applications. However, the Board needs to validate the update results before submitting this recommendation for closure.
2023	4	We recommend that the CIO document and implement a process to consistently inventory and prioritize the Board's third-party systems, including the identification of subcontractors.	Open	Board officials informed us that work to address this recommendation is ongoing.
2023	5	We recommend that the CIO enforce the agency's *iOS Update and Device Inactivity Policy* to ensure that agency services are denied to mobile devices that are out of compliance.	Open	Board officials informed us that a pop-up notification had been implemented to remind users to update to the current iOS version. However, we found that the number of devices with out-of-date iOS versions had not declined.
Identity and access management				
2020	3	We recommend that the CIO ensure that the Board's continuous monitoring processes include the security control requirements for applicable network devices.	Open	The Board's continuous monitoring processes now include vulnerability scanning for applicable network devices. Further, the agency has developed a process to check the security of administrator credentials for network devices. However, our testing continues to find issues with the administrator credentials of certain network devices.

Year		Recommendation	Status	Explanation
Data protection and privacy				
2019	5	We recommend that the CIO work with the System to ensure that the DLP replacement solution (a) functions consistently across the Board's technology platforms and (b) supports rulesets that limit the exfiltration weaknesses we identified, to the extent practicable.	Open	Board officials informed us that they successfully transferred to the agency's replacement DLP solution. However, testing revealed that the new solution does not function consistently across the Board's technology platforms and does not support the rulesets of previously identified exfiltration weaknesses.
2019	6	We recommend that the CIO develop and implement a Boardwide process to incorporate the review of DLP logs into employee and contractor offboarding processes to identify any potential unauthorized data exfiltrations or access.	Open	Board officials informed us that they are still working to incorporate data from their DLP processes into the agency's reporting tools to assist in the offboarding process.
2023	6	We recommend that the CIO develop, document, and implement a process to review and update the Board's privacy impact assessments (PIAs)	Open	Board officials informed us that while there is a new key privacy expert, there have not yet been updates to define and implement a formalized process to review and update the Board's PIAs. After the end of our fieldwork, Board officials provided additional information and requested closure of this recommendation. We plan to follow up as part of future audits.
2023	7	We recommend that the CIO ensure that the process to update PIAs is adequately resourced for effective implementation.	Open	Board officials noted that while additional resources would be welcome, the only additional resource it has received for its PIA processes was the addition of a new key privacy expert. After the end of our fieldwork, Board officials provided additional information and requested closure of this recommendation. We plan to follow up as part of future audits.
Security training				
2018	6	We recommend that the CIO develop and implement a process to assess the knowledge, skills, and abilities of Board staff with significant security responsibilities and establish plans to close identified gaps.	Open	Board officials informed us that the work to address this recommendation is ongoing. The agency is still in the preliminary stages of mapping the applicable work roles to the Board's cybersecurity-related positions and plans to use this mapping to identify skill gaps.

Year		Recommendation	Status	Explanation
ISCM				
2017	8	We recommend that the CIO develop, implement, and regularly update an ISCM strategy that includes performance measures to gauge the effectiveness of related processes and provides agencywide security status.	Open	The Board continues to make progress to develop and implement an ISCM strategy. However, agency officials informed us that the strategy is being revised to ensure it is fully comprehensive with respect to the Board's needs and provides the necessary flexibility for the agency's constantly changing technology.

Source: OIG analysis.

Appendix C: Management Response

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, DC 20551

DIVISION OF
INFORMATION TECHNOLOGY

Mr. Mark Bialek
Office of Inspector General
Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Mark,

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG) report on the Board of Governors of the Federal Reserve System's (the Board) compliance with the Federal Information Security Management Act of 2014 (FISMA) for 2024. The report evaluates the Board's information security program in accordance with the fiscal year 2024 Core IG Metrics which were chosen based on alignment with Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," as well as recent Office of Management and Budget (OMB) guidance to agencies in furtherance of the modernization of federal cybersecurity.

I am pleased your report found that the Board's information security program continues to operate effectively and recognized the agency's work in making progress towards implementing federal cybersecurity mandates including those pertaining to the establishment of a zero-trust architecture and supply chain risk management (SCRM). We remain committed to improving the Board's security posture, including remediation efforts in response to your report's recommendations, with which we concur. We will develop POA&Ms that will detail the steps the Board will take to address the recommendations.

We appreciate the professionalism and courtesies provided by the staff of the OIG throughout this audit. We intend to pursue corrective actions as a key priority, and we look forward to working with your office to confirm that our planned actions fully address the issues identified in your report.

Sincerely,

JEFFREY RIEDEL
Digitally signed by JEFFREY RIEDEL
Date: 2024.10.29 09:22:24 -04'00'

Jeff Riedel
Director, Chief Information Officer (CIO)

cc: Mr. Khalid Hasan
Mr. Charles Young
Ms. Tannaz Haddadi
Ms. Annie Martin

www.federalreserve.gov

Abbreviations

CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	chief information officer
COO	chief operating officer
CRG	Core Response Group
CSP	cloud service provider
Cybersecurity Framework	*Framework for Improving Critical Infrastructure Cybersecurity*
DLP	data loss prevention
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
IG	inspector general
ISCM	information security continuous monitoring
ISO	information security officer
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	privacy impact assessment
POA&M	plan of action and milestones
SAOP	senior agency official for privacy
SCRM	supply chain risk management

Report Contributors

Paul Vaclavik, Senior OIG Manager for Information Technology Audits
Chelsea Nguyen, OIG Manager, Information Technology Audits
Ken Dyke, Senior IT Auditor
Aaliyah Clark, IT Auditor
Alyssa O'Brien, IT Auditor
Ula Piotrowska, IT Auditor
Khalid Hasan, Assistant Inspector General for Information Technology

Contact Information

General

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

Phone: 202-973-5000
Fax: 202-973-5044

Media and Congressional

OIG.Media@frb.gov

Hotline

Report fraud, waste, and abuse.

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, web form, phone, or fax.

OIG Hotline
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

Phone: 800-827-3340
Fax: 202-973-5044