Audit Report
2023-IT-B-015
September 29, 2023

Board of Governors of the Federal Reserve System

2023 Audit of the Board's Information Security Program

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

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

Executive Summary, 2023-IT-B-015, September 29, 2023

2023 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. Since our review last year, we found that the Board has taken steps to strengthen its information security program. For instance, the Board has expanded the coverage of its vulnerability disclosure program to include all internet-accessible systems. In addition, the Board has strengthened its supply chain risk management program through improved documentation of its processes.

We identified five new findings to strengthen the Board’s information security program in the *identify* and *protect* function areas. Specifically, we found that the Board has not defined the organization’s cybersecurity risk tolerance and that the agency’s cybersecurity risk register is missing required information. In addition, the Board has not defined its process for consistently inventorying and documenting necessary attributes for its web applications or third-party systems. Further, the Board can strengthen mobile device security by ensuring that mobile device operating systems are updated timely and by denying access to enterprise services when they are not. Lastly, we found that the majority of the Board’s privacy impact assessments are not updated and reviewed in accordance with the agency’s policy.

Finally, seven recommendations we made in our previous Federal Information Security Modernization Act of 2014 (FISMA) audit reports remain open. These recommendations relate to risk management, identity and access management, data protection and privacy, security training, and information security continuous monitoring.

Recommendations

This report includes seven new recommendations designed to strengthen the Board’s information security program in the *identify* and *protect* function areas. In its response to a draft of our report, the Board concurs with our recommendations and outlines actions 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 select 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 2023. OMB notes that level 4 (*managed and measurable*) represents an effective level of security.

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

Recommendations, 2023-IT-B-015, September 29, 2023

2023 Audit of the Board's Information Security Program

Number	Recommendation	Responsible office
1	Prioritize the definition and incorporation of a cybersecurity risk tolerance into the agency's cybersecurity policies, procedures, and processes, as appropriate.	Division of Information Technology
2	Ensure all required attributes are consistently documented within the agency's cybersecurity risk register.	Division of Information Technology
3	Document and implement a process to consistently inventory the Board's web applications, including its public-facing websites.	Division of Information Technology
4	Document and implement a process to consistently inventory and prioritize the Board's third-party systems, including the identification of subcontractors.	Division of Information Technology
5	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.	Division of Information Technology
6	Develop, document, and implement a process to review and update the Board's PIAs.	Division of Information Technology
7	Ensure that the process to update PIAs is adequately resourced for effective implementation.	Division of Information Technology

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

MEMORANDUM

DATE: September 29, 2023

TO: Distribution List

FROM: Khalid Hasan Khalid Hasan
Assistant Inspector General for Information Technology

SUBJECT: OIG Report 2023-IT-B-015: *2023 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 state that you concur with our recommendations and outline actions that have been or will be taken to address our recommendations. 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: Andrew Krug
Charles Young
Annie Martin
Craig Delaney
Donna Butler
Cheryl Patterson

Distribution:
Patrick J. McClanahan, Chief Operating Officer
Ricardo A. Aguilera, Chief Financial Officer
Kofi Sapong, Acting Chief Information Officer
Winona H. Varnon, Director, Division of Management

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*, which represents a continuation of the work started in fiscal year (FY) 2022 when the IG FISMA metrics reporting process was transitioned to a multiyear cycle.[2]

As part of this transition, OMB implemented a new framework regarding the timing and focus of annual IG FISMA assessments, with the goal of providing a more flexible and continued focus on annual assessments for the federal community. This effort yielded two distinct groups of metrics for IGs to assess in their annual FISMA reviews: core metrics and supplemental metrics.

- **Core metrics:** These metrics are assessed annually and represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness.
- **Supplemental metrics:** These metrics are assessed at least once every 2 years. They represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

The *FY 2023–2024 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

[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] Office of Management and Budget, Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, December 2, 2022.

identify, *protect*, *detect*, *respond*, and *recover* (table 1).[3] 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.

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 and 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, and 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 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.1, May 12, 2021.

FISMA Maturity Model

OMB's *FY 2023–2024 IG FISMA Reporting Metrics* notes that IGs are required to assess the effectiveness of their agencies' information security programs by assessing the core and supplemental metrics against a maturity model spectrum.[4] The five levels of the maturity model are

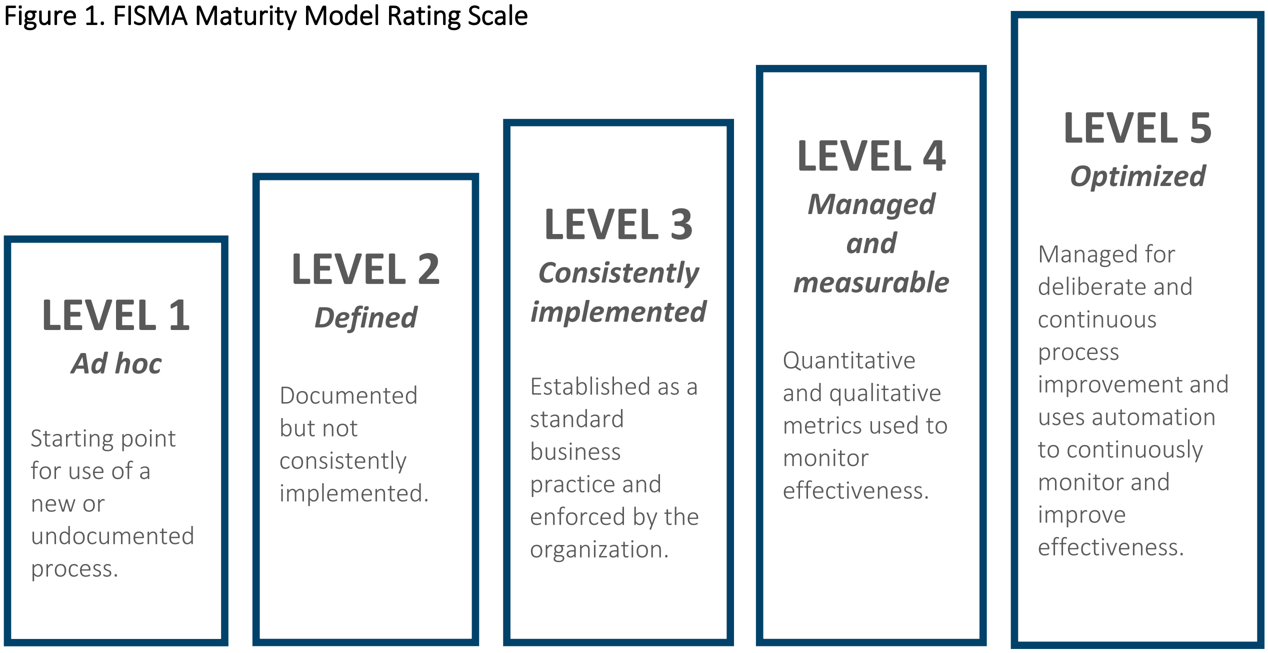
1. *ad hoc*
2. *defined*
3. *consistently implemented*
4. *managed and measurable*
5. *optimized*

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

[4] As noted in the *FY 2023–2024 IG FISMA Reporting Metrics*, IGs should use the Cyberscope application to submit the results of their core metrics evaluation. As such, our detailed responses and assessment of the Board's progress in implementing the core metrics were provided to the U.S. Department of Homeland Security in the Cyberscope application. Because of the sensitive nature of our responses, they are restricted and not included in this report.

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 (figure 1). 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.[5] Further details on the scoring methodology for the maturity model are included in appendix A.

Figure 1. FISMA Maturity Model Rating Scale



LEVEL 1
Ad hoc
Starting point for use of a new or undocumented process.

LEVEL 2
Defined
Documented but not consistently implemented.

LEVEL 3
Consistently implemented
Established as a standard business practice and enforced by the organization.

LEVEL 4
Managed and measurable
Quantitative and qualitative metrics used to monitor effectiveness.

LEVEL 5
Optimized
Managed for deliberate and continuous process improvement and uses automation to continuously monitor and improve effectiveness.

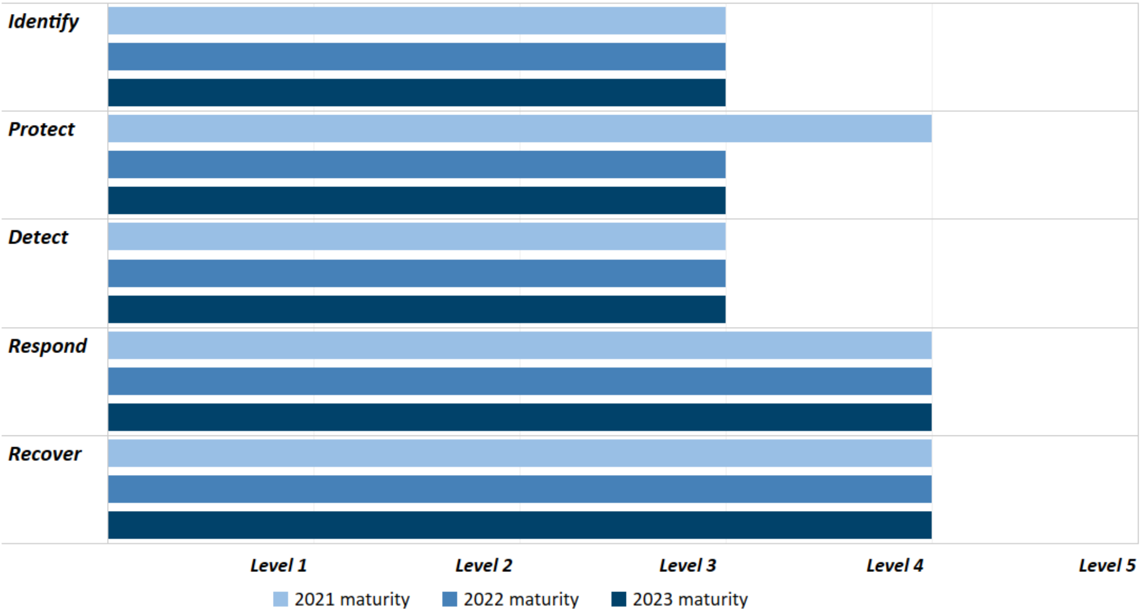
Source: OIG analysis of OMB's *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, February 10, 2023.

[5] 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, Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, updated December 10, 2020.

Analysis of the Board's Progress in Implementing FISMA Information Security Program Requirements

The Board's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity.[6] This year, we found that the Board maintained a level-3 (*consistently implemented*) maturity for the *identify*, *protect*, and *detect* functions and an effective level-4 (*managed and measurable*) maturity for the *respond* and *recover* functions (figure 2). Since our review last year, we found that the Board has taken several steps to strengthen its information security program. For instance, the Board has expanded the coverage of its vulnerability disclosure policy to include all internet-accessible systems. In addition, the Board has strengthened its supply chain risk management program through improved documentation of its processes.

Figure 2. Maturity of the Board's Information Security Program, by Security Function, 2021–2023



Source: OIG analysis.

We identified five new findings to help mature the Board's information security program in the *identify* and *protect* function areas. In addition, we highlight ongoing opportunities to improve the Board's information security program in the *detect*, *respond*, and *recover* functions.

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

Identify

The objective of the *identify* function in NIST's Cybersecurity Framework is to develop an organizational understanding of how to manage cybersecurity risks to agency systems, assets, data, and capabilities. The Cybersecurity Framework highlights risk management processes that organizations can implement to inform and prioritize decisions. Examples of the areas in this security function, as outlined in OMB's *FY 2023–2024 IG FISMA Reporting Metrics*, that we assessed include the Board's cybersecurity risk management processes; asset management, including mobile device management; the use of plans of action and milestones to manage the remediation of security weaknesses; and the agency's understanding and control of the cybersecurity supply chain risks of the products and services that it uses.

We found that the Board's *identify* function area continues to operate at a level-3 (*consistently implemented*) maturity. We identified several opportunities to mature the Board's risk management processes related to the agency's cybersecurity risk tolerance, cybersecurity risk register process, public website and vendor inventories, and mobile device management processes. Specifically, we found that

- The Board has not defined the organization's cybersecurity risk tolerance or the priorities and tradeoffs to be used when managing cyberrisk.
- The agency's cybersecurity risk register process is inconsistently implemented, with information missing in required fields.
- The Board has not defined its process for consistently inventorying and documenting necessary attributes for its web applications or third-party systems.
- The Board is not enforcing operating system updates for its mobile devices nor denying mobile access to enterprise services when the operating system is outdated.

In addition, two recommendations from previous FISMA reports in the *identify* area remain open. These recommendations relate to the Board's insider threat program for its sensitive but unclassified information, as well as the prioritization and categorization of the risk items maintained on the agency's cybersecurity risk register. Further details on these recommendations can be found in appendix B.

Defining a Cybersecurity Risk Tolerance Could Strengthen the Board's Risk Management Program

Risk tolerance is the degree of risk or uncertainty that is acceptable to an organization. The risk tolerance is a key component of a risk management strategy, which defines how security and privacy risks are framed, assessed, responded to, and monitored. Further, an organization's risk management strategy makes explicit the assumptions, constraints, priorities, tradeoffs, and risk tolerance used for making operational decisions. Although the Board has defined and implemented its *Risk Management Program and Risk Assessment Standard*, the agency has not defined its cybersecurity risk tolerance or the priorities and tradeoffs to be used when managing risk.

NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, notes that, in addition to being an important part of a risk management strategy, risk tolerance affects all components of the risk management process, having a direct effect on the risk management decisions made by senior leaders and executives throughout the organization and providing important constraints on those decisions.[7] For example, risk tolerance affects the nature and extent of risk management oversight implemented in organizations, the extent and rigor of risk assessments performed, and the content of organizational strategies for responding to risk.

Division of Information Technology officials informed us that plans to define the organization's cybersecurity risk tolerance have been delayed because of competing priorities. Further, these same officials noted that the Division of IT is involved in the organization's ongoing implementation of enterprise risk management (ERM).[8] We believe that defining the agency's cybersecurity risk tolerance could help ensure a consistent approach to risk assessment and response at the division and enterprise levels.

Recommendation

We recommend that the chief information officer (CIO)

1. Prioritize the definition and incorporation of a cybersecurity risk tolerance into the agency's cybersecurity policies, procedures, and processes, as appropriate.

Management Response

The CIO concurs with our recommendation and states that the Board plans to work with agency stakeholders to develop and document a cybersecurity risk tolerance consistent with the Board's ERM objectives.

OIG Comment

We believe that the actions described by the CIO are responsive to our recommendation. We plan to follow up on the Board's actions to address our recommendation as part of future FISMA reviews.

The Board Can Enhance Its Cyberrisk Register Process

NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* (NISTIR 8286), highlights the importance of, and the relationships between, cybersecurity risk management and ERM.[9] Specifically, NISTIR 8286 notes that one way to ensure that cybersecurity risk information is able to be aggregated, normalized, and prioritized at the enterprise level is through the use of a cybersecurity

[7] National Institute of Standards and Technology, Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2021.

[8] As we have previously reported, the Board continues to take steps to implement an ERM program. Office of Inspector General, *The Board's Implementation of Enterprise Risk Management Continues to Evolve and Can Be Enhanced*, OIG Report 2021-IT-B-011, September 15, 2021.

[9] NISTIR 8286 defines *cybersecurity risk* as an effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality; integrity; or availability of information, data, or information (or control) systems and reflect the potential adverse effects to enterprise operations (meaning, mission, functions, image, or reputation) and to assets, individuals, other organizations, and the nation. NISTIR 8286 defines *ERM* as an effective agencywide approach to addressing the full spectrum of the organization's significant risks by understanding the combined effect of risks as an interrelated portfolio, rather than addressing risks only within silos. National Institute of Standards and Technology, Internal Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, October 2020.

risk register.[10] The Division of IT uses a cybersecurity risk register to capture risks from across the enterprise by contacting representatives from each Board division on a quarterly basis to gather information on new and existing cybersecurity risks and ensuring that this information is documented in the agency's FISMA compliance tool. Our 2022 Board FISMA report includes a recommendation to ensure that risks are appropriately categorized and prioritized on the Board's cybersecurity risk register; this recommendation remains open.[11]

This year, we found that the agency's existing cybersecurity risk register process is not consistently implemented. Specifically, the Board's cybersecurity risk register includes approximately 50 risks. We noted that the majority of these risk items had information missing in one or more required fields, such as finding year, risk decision, likelihood, impact, remediation start date, residual risk assessment, and risk acceptance justification.

We believe required fields were blank because of the manual nature of the agency's cybersecurity risk register process in 2023. Specifically, Board officials informed us that the cybersecurity risk register is currently being maintained outside the agency's FISMA compliance tool while the tool is being configured to customize risk register elements. These same officials noted that migration of the risk register back to the FISMA compliance tool is expected to be completed by the second quarter of 2024. We believe that completing all required fields before this migration would allow the agency to prioritize risks and estimate risk remediation more accurately.

Recommendation

We recommend that the CIO

2. Ensure all required attributes are consistently documented within the agency's cybersecurity risk register.

Management Response

The CIO concurs with our recommendation and states that the Board will develop a process for reviewing and completing all required attributes within the agency's cybersecurity risk register.

OIG Comment

We believe that the actions described by the CIO are responsive to our recommendation. We plan to follow up on the Board's actions to address our recommendation as part of future FISMA reviews.

[10] NISTIR 8286 defines a *risk register* as a repository of risk information, including the data understood about risks over time.

[11] Office of Inspector General, *2022 Audit of the Board's Information Security Program*, OIG Report 2022-IT-B-013, September 30, 2022.

The Board Should Document and Consistently Implement Its Inventory Processes for Web Applications and Third-Party Systems

We found that the Board has processes in place to maintain an inventory of its information systems. However, we identified several opportunities to improve processes related to the inventories of web applications and third-party systems. Specifically, the Board does not have a defined process for consistently inventorying and documenting necessary attributes for its public-facing websites or third-party systems. For instance, we found that several fields within the Board's web application and third-party inventories are often blank or inconsistent, such as *destination URL* for public-facing websites and *interconnections* for third-party systems. We also noted that the agency's third-party inventory neither prioritizes vendors by their risk nor clearly identifies the use of subcontractors.

OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, notes that a necessary foundation for any enterprise zero trust architecture is a complete understanding of the devices, users, and systems interacting within an organization. In addition, NIST Special Publication 800-53, Revision 5, S*ecurity and Privacy Controls for Information Systems and Organizations*, requires agencies to develop and document an inventory of information system components that (1) accurately reflects the current information system, (2) includes all components within the authorization boundary of the information system, and (3) includes the granularity deemed necessary for tracking and reporting.[12] OMB Circular A-130, *Managing Information as a Strategic Resource*, further highlights an agency's responsibilities related to third-party systems, mandating that information systems used or operated by contractors or other entities on behalf of a federal agency be included in its inventory of information systems.[13] Accordingly, a comprehensive and accurate inventory of an agency's web applications and third-party systems is crucial to ensuring that appropriate controls are in place to protect an organization's systems data.

We attributed these issues to two key causes. First, the Board is in the process of transitioning to a new FISMA compliance tool, which has changed the methods and attributes by which the agency inventories these types of systems. Second, Board officials informed us that they are using internal working processes, as opposed to its documented inventory processes, to track these types of systems. We believe that a documented process to consistently inventory all web applications and third-party systems will help ensure that the Board's system inventory is complete and provides the necessary foundation for the agency's zero trust architecture.

[12] National Institute of Standards and Technology, Special Publication 800-53, S*ecurity and Privacy Controls for Information Systems and Organizations*, Revision 5, updated December 10, 2020.

[13] Office of Management and Budget, *Managing Information as a Strategic Resource*, OMB Circular A-130, July 28, 2016.

Recommendations

We recommend that the CIO

3. Document and implement a process to consistently inventory the Board's web applications, including its public-facing websites.

4. Document and implement a process to consistently inventory and prioritize the Board's third-party systems, including the identification of subcontractors.

Management Response

The CIO concurs with our recommendations and states that the Board plans to develop a process to ensure it maintains an inventory of all Board web applications and plans to establish a protocol to ensure the inventory is reviewed regularly for completeness and accuracy. Further, the Board will work with stakeholders to enhance its current vendor risk management procedures to better identify and inventory systems maintained by third parties as well as subcontractors of trusted business partners.

OIG Comment

We believe that the actions described by the CIO are responsive to our recommendations. We plan to follow up on the Board's actions to address our recommendations as part of future FISMA reviews.

The Board Should Deny Agency Services to Mobile Devices With Outdated Operating System Software

The Board has implemented a mobile device management tool to manage the configurations of the agency's mobile devices. However, we found that at the time of our testing, over half of the approximately 3,000 mobile devices on the Board's network were not using the currently approved version of the mobile device's operating system. Specifically, 54 percent of these noncompliant devices were one or more minor versions behind the currently approved operating system, and 4 percent were a major version behind. Further, the Board does not deny agency services to mobile devices when the operating system is not updated within a given period of time.

NIST Special Publication 800-124, Revision 2, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, emphasizes the importance of timely updates to mobile device software, noting that if users do not make appropriate updates, administrators could enforce compliance actions, including blocking or restricting access to enterprise information or the complete removal of enterprise information on the mobile device.[14] In addition, the Board's *iOS Update and Device Inactivity Policy* defines the agency's process for reminding users via daily emails that they have a noncompliant operating system installed on their mobile device; the policy also details steps for enforcing compliance, including

[14] National Institute of Standards and Technology, Special Publication 800-124, Revision 2, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, May 17, 2023.

removing the device’s virtual private network (VPN) agent until the user installs the compliant operating system.[15] However, we found that this policy was not being enforced.

Board officials acknowledged that the Board’s *iOS Update and Device Inactivity Policy* needs to be updated to reflect the agency’s current process, as they do not deny agency services to mobile devices that are not in compliance. We believe that vulnerability scanning, as noted in U.S. Department of Homeland Security, Binding Operational Directive 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*, could be a compensating control to identify security weaknesses for mobile devices that are out of compliance.[16] However, Board officials informed us that their current suite of vulnerability scanning tools does not have the capability to scan mobile devices for potential vulnerabilities. As such, we believe that enforced compliance with an approved mobile device operating system will help mitigate the risk of security vulnerabilities affecting the agency’s environment.

Recommendation

We recommend that the CIO

5. 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.

Management Response

The CIO concurs with our recommendation and states that the Board will explore enforcement measures with agency stakeholders to uphold the Board’s mobile device policies, which will ensure that services are restricted for mobile devices found to be noncompliant with required patches and updates.

OIG Comment

We believe that the actions described by the CIO are responsive to our recommendation. We plan to follow up on the Board’s actions to address our recommendation as part of future FISMA reviews.

Protect

The objective of the *protect* function in NIST’s Cybersecurity Framework is to develop and implement safeguards to secure information systems. This function supports the ability to limit or contain the effect of a cybersecurity event through applicable configuration management, identity and access management, data protection and privacy, and security training processes. Examples of the areas in this security function, as outlined in OMB’s *FY 2023–2024 IG FISMA Reporting Metrics*, that we assessed include processes for managing the agency’s baseline configurations, performing vulnerability scanning, utilizing multifactor authentication, maintaining privacy-related documentation for the Board’s systems, and assessing the knowledge and skills of the agency’s cybersecurity workforce.

[15] Loss of the VPN agent will block the user from accessing email, browsers, and video conferencing services on their mobile device.

[16] The directive states that agencies must perform the same type of vulnerability enumeration on mobile devices as they would for on-premises devices, as feasible.

We found that the Board's *protect* function continues to operate at a level-3 (*consistently implemented*) maturity, and we identified an opportunity for the Board to strengthen its processes around privacy impact assessments (PIAs). In addition, four recommendations in the *protect* area from previous FISMA reports remain open. These recommendations relate to the Board's continuous monitoring of the agency's network devices; its data loss prevention processes; and the organization's assessment of the knowledge, skills, and abilities of its cybersecurity personnel. Further details on these recommendations can be found in appendix B.

The Board Should Regularly Review and Update Its PIAs

A PIA is an analysis of how information in identifiable form is collected, stored, protected, shared, and managed. PIAs are an important tool that the Board uses to fulfill its legal and regulatory responsibilities for safeguarding personally identifiable information[17] maintained in information technology systems and to mitigate potential privacy risks. In accordance with the E-Government Act of 2002, the Board publishes its PIAs on its public website.[18] However, we found that 26 of the Board's 44 PIAs have not been reviewed and updated within the past 3 years.

The Board's privacy program requires that system owners complete a privacy threshold analysis to determine whether a PIA is needed.[19] The purpose of a PIA is to demonstrate that system owners and developers have incorporated privacy protections throughout the entire life cycle of a system. The Board's *Privacy Policy* notes that PIAs are scheduled to be reviewed (1) whenever a system undergoes a significant change or (2) every 3 years in alignment with the system's authority to operate.

Division of IT officials informed us that while the Board has developed its processes for drafting PIAs, the agency has not defined or implemented a formalized process for the regular review and update of its PIAs. Division of IT officials also noted that a key agency privacy expert departed during 2023, which affected the team's workload. These officials further stated that a replacement for this individual has recently been hired and the agency hopes to add additional privacy expertise in 2024. Establishing a formal process to review and update PIAs and devoting adequate resources to execute that process should help ensure that the privacy information maintained for the Board's systems is accurate and complete.

Recommendations

We recommend that the CIO

6. Develop, document, and implement a process to review and update the Board's PIAs.
7. Ensure that the process to update PIAs is adequately resourced for effective implementation.

[17] *Personally identifiable information* generally includes any information that identifies or describes an individual including, but not limited to, an individual's name combined with other personal information such as the individual's Social Security number, driver's license number, birthday, place of birth, account numbers for financial accounts, passwords, or security codes.

[18] E-Government Act of 2002, Public Law No. 107-347, December 17, 2002.

[19] A *privacy threshold analysis* is the process the Board uses to determine whether a system contains personally identifiable information and the privacy requirements that apply to the system, including whether a PIA is required.

Management Response

The CIO concurs with our recommendations and states that the Board plans to improve its current procedures for regularly reviewing, updating, and documenting Board PIAs to ensure ongoing compliance with privacy regulations and standards. Further, the Board will work to prioritize the allocation of resources, including personnel, to ensure that the process for updating PIAs is effectively implemented and sustained.

OIG Comment

We believe that the actions described by the CIO are responsive to our recommendations. We plan to follow up on the Board's actions to address our recommendations as part of future FISMA reviews.

Detect

The objective of the *detect* function in the NIST Cybersecurity Framework is to implement activities to discover and identify the occurrence of cybersecurity events in a timely manner. The Cybersecurity Framework notes that continuous monitoring processes are used to detect anomalies and changes in the organization's environment of operation, maintain knowledge of threats, and ensure security control effectiveness. Examples of the areas in this security function, as outlined in OMB's *FY 2023–2024 IG FISMA Reporting Metrics*, that we assessed include the Board's progress in developing and implementing an information security continuous monitoring (ISCM) strategy, the performance of ISCM-related roles and responsibilities, and the execution of the agency's system authorization process.

We found that the Board continues to operate at a level-3 (*consistently implemented*) maturity within the *detect* function. While we did not identify any new opportunities for improvement in this area, our 2017 FISMA audit report contains a recommendation related to the development and implementation of an ISCM strategy that remains open (appendix B).

Respond

The objective of the *respond* function in NIST's Cybersecurity Framework is to implement processes to contain the impact of detected cybersecurity events. Examples of the areas in this security function, as outlined in OMB's *FY 2023–2024 IG FISMA Reporting Metrics*, that we assessed include the Board's incident detection, analysis, and handling processes as well as its use of technology to support its incident response program.

We found that the Board continues to operate at a level-4 (*managed and measurable*) maturity within the *respond* function. While we did not identify any new opportunities for improvement in this area, the Board continues to work toward full implementation of the U.S. Department of Homeland Security's Continuous Diagnostic and Mitigation (CDM) program, particularly in the areas of configuration and vulnerability management. These CDM capabilities could provide greater visibility into the security configurations and posture of agency systems, thus enabling the Board to strengthen its incident response processes. We will continue to monitor the Board's progress in implementing the tools offered through the CDM program as part of future FISMA audits.

Recover

The objective of the *recover* function in NIST's Cybersecurity Framework is to ensure that organizations maintain resilience by implementing appropriate activities to restore capabilities or infrastructure services that were impaired by a cybersecurity event. The Cybersecurity Framework outlines contingency planning processes that support timely recovery to normal operations and reduce the effect of a cybersecurity event. Examples of the assessment areas in this security function, as outlined in OMB's *FY 2023–2024 IG FISMA Reporting Metrics*, that we assessed include the performance of contingency planning–related roles and responsibilities, the processes for conducting an enterprise business impact analysis, and the testing of system-level contingency plans.

We found that the Board continues to operate at a level-4 (*managed and measurable*) maturity within the *recover* function. We did not identify any new opportunities for improvement in this area. As reported in our previous FISMA reviews, the agency has an opportunity to further mature its contingency planning program by ensuring that it is fully integrated with the Board's ERM processes. This integration should help ensure that risks associated with the agency's contingency processes are consistently prioritized for the Board's most critical processes and systems.

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 OMB's *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*, *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 FY 2023 metrics identified in OMB's *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 level as well as for three sampled Board systems[20]

To rate the maturity of the Board's information security program and functional areas, we used the scoring methodology defined in OMB's *FY 2023–2024 IG FISMA Reporting Metrics*. In previous years, IGs were directed to use a mode-based scoring approach to assess agency maturity levels, where the most frequent level (meaning, the mode) across the metrics served as the domain rating. This same mode-based approach applied to ratings at the function and overall information security program levels. However, in FY 2023, OMB and CIGIE determined that a calculated average would provide a more accurate assessment of agency maturity. As such, core metrics and supplemental metrics are averaged independently to determine a domain's maturity calculation. These averages in a particular domain provide data points to be used by IGs to determine the effectiveness of the individual function areas (*identify*, *protect*, *detect*, *respond*, and *recover*) as well as the overall information security program.

To provide IGs with additional flexibility and to encourage evaluations that are based on an agency's risk tolerance and threat models, calculated averages are not automatically rounded to a particular maturity level. In determining maturity levels and the overall effectiveness of an agency's information security program, OMB strongly encourages IGs to focus on the results of the core metrics, as these tie directly to administration priorities and other high-risk areas. IGs should use the calculated averages of the supplemental metrics as a data point to support their risk-based determination of overall program- and function-level effectiveness.

[20] We selected these three 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. The results of our testing for these three systems did not indicate any new program-level findings that are presented in this report. We plan to transmit the detailed results of our testing of these systems in separate, restricted memorandums because of the sensitive nature of the information.

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. We conducted this work from March 2023 to July 2023.

Appendix B: Status of Prior FISMA Recommendations

As part of our 2023 FISMA audit, we reviewed the actions taken by the Board to address the outstanding recommendations from prior FISMA audit reports. Based on our review, we determined that the seven recommendations that were open at the start of our 2023 FISMA audit, which are related to risk management, identity and access management, data protection and privacy, security training, and ISCM, will remain open (table B-1). We will update the status of these recommendations in our fall 2023 semiannual report to Congress, and we will continue to monitor the Board's progress in addressing our open recommendations as a part of our future FISMA audits.

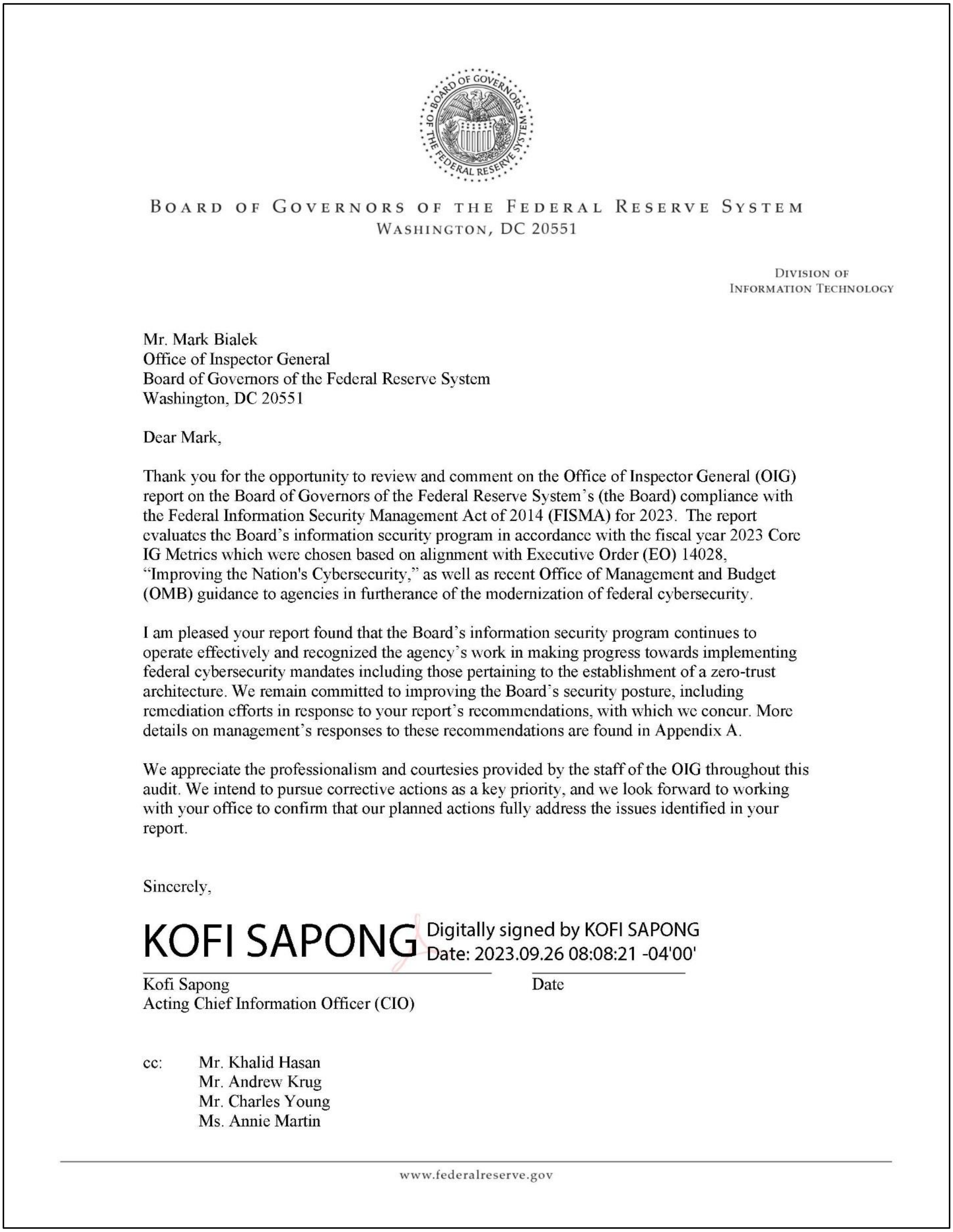
Table B-1. Status of 2016–2022 FISMA Recommendations That Were Open as of the Start of Our Fieldwork, by Security Domain

Year	Recommendation		Status	Explanation
Risk management				
2016	1	We recommend that the CIO work with the chief operating officer 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 are still working with other stakeholders on an approach to implement an agencywide insider threat strategy for sensitive but unclassified 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 second quarter of 2024.
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 found opportunities to improve in this area.

Year	Recommendation		Status	Explanation
Data protection and privacy				
2019	5	We recommend that the CIO work with the Federal Reserve System to ensure that the data loss protection (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 continue to work with the System to test the agency's replacement DLP solution. These same officials informed us that the current plan is for the System to implement the replacement solution in the fourth quarter of 2023, with the Board's implementation following in the first quarter of 2024.
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 exfiltration 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.
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 they are still in the preliminary stages of information gathering for this process. The agency plans to map the applicable work roles to the Board's cybersecurity-related positions and use this mapping to identify skill gaps.
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 in the development and implementation of 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 2023. The report evaluates the Board's information security program in accordance with the fiscal year 2023 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. We remain committed to improving the Board's security posture, including remediation efforts in response to your report's recommendations, with which we concur. More details on management's responses to these recommendations are found in Appendix A.

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,

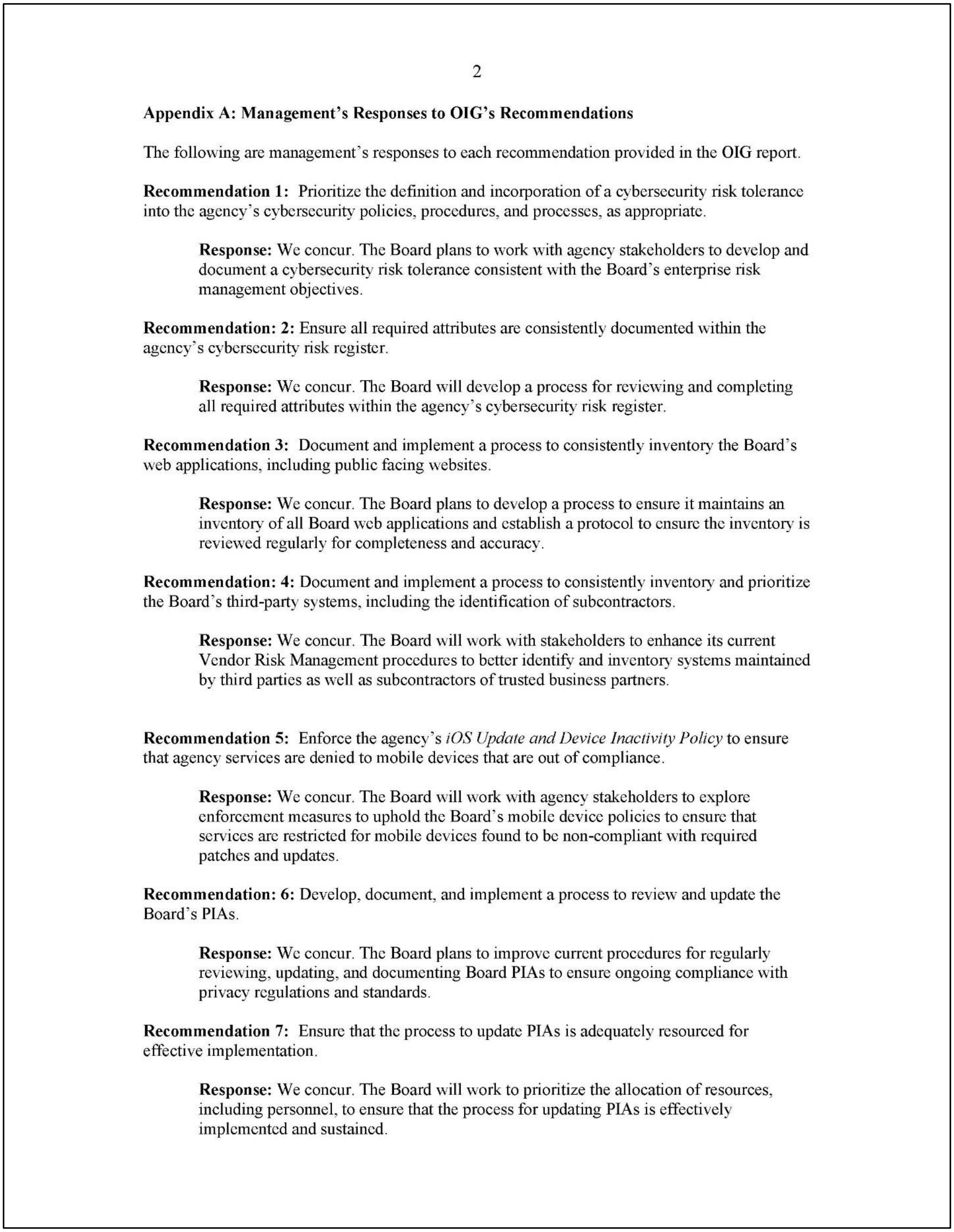
KOFI SAPONG Digitally signed by KOFI SAPONG
Date: 2023.09.26 08:08:21 -04'00'

Kofi Sapong
Acting Chief Information Officer (CIO)

Date

cc: Mr. Khalid Hasan
Mr. Andrew Krug
Mr. Charles Young
Ms. Annie Martin

www.federalreserve.gov



Appendix A: Management's Responses to OIG's Recommendations

The following are management's responses to each recommendation provided in the OIG report.

Recommendation 1: Prioritize the definition and incorporation of a cybersecurity risk tolerance into the agency's cybersecurity policies, procedures, and processes, as appropriate.

> **Response:** We concur. The Board plans to work with agency stakeholders to develop and document a cybersecurity risk tolerance consistent with the Board's enterprise risk management objectives.

Recommendation: 2: Ensure all required attributes are consistently documented within the agency's cybersecurity risk register.

> **Response:** We concur. The Board will develop a process for reviewing and completing all required attributes within the agency's cybersecurity risk register.

Recommendation 3: Document and implement a process to consistently inventory the Board's web applications, including public facing websites.

> **Response:** We concur. The Board plans to develop a process to ensure it maintains an inventory of all Board web applications and establish a protocol to ensure the inventory is reviewed regularly for completeness and accuracy.

Recommendation: 4: Document and implement a process to consistently inventory and prioritize the Board's third-party systems, including the identification of subcontractors.

> **Response:** We concur. The Board will work with stakeholders to enhance its current Vendor Risk Management procedures to better identify and inventory systems maintained by third parties as well as subcontractors of trusted business partners.

Recommendation 5: 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.

> **Response:** We concur. The Board will work with agency stakeholders to explore enforcement measures to uphold the Board's mobile device policies to ensure that services are restricted for mobile devices found to be non-compliant with required patches and updates.

Recommendation: 6: Develop, document, and implement a process to review and update the Board's PIAs.

> **Response:** We concur. The Board plans to improve current procedures for regularly reviewing, updating, and documenting Board PIAs to ensure ongoing compliance with privacy regulations and standards.

Recommendation 7: Ensure that the process to update PIAs is adequately resourced for effective implementation.

> **Response:** We concur. The Board will work to prioritize the allocation of resources, including personnel, to ensure that the process for updating PIAs is effectively implemented and sustained.

Abbreviations

CDM	Continuous Diagnostic and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	chief information officer
Cybersecurity Framework	*Framework for Improving Critical Infrastructure Cybersecurity*
DLP	data loss protection
ERM	enterprise risk management
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
IG	inspector general
ISCM	information security continuous monitoring
NIST	National Institute of Standards and Technology
NISTIR 8286	National Institute of Standards and Technology, Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*
OMB	Office of Management and Budget
PIA	privacy impact assessment
VPN	virtual private network

Report Contributors

Joshua Dieckert, OIG Manager, Information Technology Audits
Paul Vaclavik, OIG Manager, Information Technology Audits
Ken Dyke, Senior IT Auditor
Chelsea Nguyen, Senior IT Auditor
Nilesh Patel, Senior IT Auditor
Justin Byun, IT Auditor
Aaliyah Clark, IT Auditor
Deyanara Gonzalez, IT Auditor
Alyssa O’Brien, IT Auditor
Alexander Karst, Senior Information Technology Management Specialist
Fay Tang, Senior Information Technology Management Specialist
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

OIG

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