Audit Report
2025-IT-B-011R
October 31, 2025

Board of Governors of the Federal Reserve System

2025 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, 2025-IT-B-011R, October 31, 2025

2025 Audit of the Board's Information Security Program

Findings

The Board's information security program has decreased from a level-4 maturity (*managed and measurable*) in fiscal year (FY) 2024 to a level-3 maturity *(consistently implemented)* in FY 2025. We further concluded, based on the results of our determinations of effectiveness in each domain and function, that the Board's overall information security program is not effective. We found that the Board has taken some steps to strengthen its information security program since our 2024 Federal Information Security Modernization Act of 2014 (FISMA) audit report. For instance, the Board has updated its cybersecurity risk register process and developed a new information security continuous monitoring strategy. However, challenges in cybersecurity governance resulting from the Board's information technology (IT) operating model and decentralized IT environment, coupled with opportunities to strengthen foundational cybersecurity elements, contributed to the decline in overall program maturity.

We found that the Board can strengthen its cybersecurity program by

- defining key elements of its current and target cybersecurity approach
- reassessing its policy for mobile device use and consistently enforcing mobile content and data protection controls
- reassessing the feasibility of developing and implementing an information classification for confidential supervisory information

Recommendations

This report includes three new recommendations and a matter for management consideration designed to strengthen the Board's information security program in the areas of cybersecurity governance, mobile device security, and confidential supervisory information protection. In its response to our draft report, the Board concurs with our recommendations and outlines actions to address each recommendation. We will follow up to ensure that the recommendations are fully addressed.

In addition, we are closing 4 previously issued recommendations, while keeping 18 recommendations made in our prior FISMA reports open. Notably, the Board has not yet addressed several significant recommendations related to insider threat management, data loss prevention, and cyber risk tolerance. We will continue to monitor the Board's progress in addressing these recommendations as part of future FISMA audits. Given the sensitivity of the information in our review, portions of the public version of this report have been redacted.

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 2025 Inspector General 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 FY 2025. OMB notes that level 4 *(managed and measurable)* represents an effective level of security.

A key addition in the *FY 2025 Inspector General FISMA Reporting Metrics* is the inclusion of a new *govern* function that focuses on the role governance plays in managing cybersecurity risks and incorporating cybersecurity into an organization's broader enterprise risk management strategy.

Recommendations, 2025-IT-B-011R, October 31, 2025

2025 Audit of the Board's Information Security Program

Finding 1: Developing Cybersecurity Profiles Can Help the Board Assess, Tailor, and Prioritize Its Cybersecurity Approach

Number	Recommendation	Responsible office
1	Develop and maintain cybersecurity profile(s) that define key elements of the Board's current and target cybersecurity program in alignment with the Board's organizational risk tolerance, mission objectives, and threat environment.	Division of Information Technology

Finding 2: Enhancing Mobile Device Security Could Better Protect Sensitive Data

Number	Recommendation	Responsible office
2	Evaluate the dual-use model for the Board's mobile devices, in accordance with the Board's security objectives and risk tolerance, and review and update the *Information Technology Resources Use* policy as appropriate.	Division of Information Technology
3	Strengthen mobile device security controls to enforce content and data protection policies.	Division of Information Technology

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, and other stakeholders collaborated to develop the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.[2]

The IG FISMA reporting metrics are grouped into 10 security domains, which align with the 6 function areas in the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework).[3] The 6 function areas are *govern*, *identify*, *protect*, *detect*, *respond*, and *recover*. 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 include a number of metrics that IGs are required to assess using a maturity model.[4] Table 1 highlights the relationships between the function areas, the 10 security domains, and metrics.

[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, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 2.0, April 3, 2025.

[3] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, February 26, 2024.

[4] As noted in the *FY 2025 IG FISMA Reporting Metrics*, IGs 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.

The total number of metrics IGs are required to assess declined from 37 for fiscal year 2024 to 25 for fiscal year 2025.

In 2024, NIST updated the Cybersecurity Framework to include a new *govern* function to underscore the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an organization's broader enterprise risk management strategy. This function consists of two domains: cybersecurity governance and cybersecurity supply chain risk management (SCRM).[5] *Govern* emphasizes organizational context; the establishment of cybersecurity strategy, roles, responsibilities, and authorities; cybersecurity supply chain risk oversight; and policy development. The *govern* function informs how an organization implements the other five functions and, as such, is a critical component for achieving and maintaining an effective information security program.

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

Security function	Security function objective	Associated IG FISMA reporting domain
Govern	Implement an understanding of organizational context; establish the cybersecurity strategy and cybersecurity SCRM; define roles, responsibilities, and authorities; develop policy; and oversee the execution of cybersecurity strategy.	Cybersecurity governance (for example, oversight), cybersecurity SCRM (for example, risk management strategy)
Identify	Develop an organizational understanding to manage cybersecurity risk to agency assets.	Risk and asset management (for example, risk assessment)
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 (for example, technology infrastructure resilience), identity and access management (for example, identity management, authentication, and access control), data protection and privacy (for example, data security), security training (for example, awareness and training)
Detect	Implement activities to identify the occurrence of cybersecurity events.	Information security continuous monitoring (for example, adverse event analysis)
Respond	Implement processes to take action regarding a detected cybersecurity event.	Incident response (for example, incident mitigation)
Recover	Implement plans for resilience to restore any capabilities impaired by a cybersecurity event.	Contingency planning (for example, incident recovery plan execution)

Source: Office of Management and Budget, *FY 2025 IG FISMA Reporting Metrics*.

[5] Office of Management and Budget, *FY 2025 IG FISMA Reporting Metrics*.

FISMA Maturity Model

Each function area, domain, and metric area is assessed using a five-level maturity model:

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 2025 IG FISMA Reporting Metrics*, in the context of the maturity model, OMB believes that achieving a level 4 (*managed and measurable*) or above represents an effective level of security.[6] Metric, domain, and function level maturity ratings factor into the overall determination of whether an agency's information security program is effective (figure 1). Further details on the scoring methodology for the maturity model are included in appendix A.

Figure 1. IG FISMA Maturity Model

Source: Office of Management and Budget, *FY 2025 IG FISMA Reporting Metrics*.

[6] 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 Audit Results of the Board's Information Security Program

The Board's information security program has decreased from a level-4 maturity (*managed and measurable*) in fiscal year (FY) 2024 to a level-3 maturity (*consistently implemented*) in FY 2025. We further concluded, based on the results of our determinations of effectiveness in each domain and function, that the Board's overall information security program is not effective.[7] We found that the Board has taken some steps to strengthen its information security program since our 2024 FISMA audit report. For instance, the Board has updated its cybersecurity risk register to ensure that all required attributes are consistently documented and that risks are prioritized. In addition, the Board updated its information security continuous monitoring (ISCM) standard to incorporate processes that, when implemented, can enable the Board to transition to ongoing system authorizations. However, challenges in cybersecurity governance resulting from the Board's IT operating model and decentralized IT environment, coupled with opportunities to strengthen foundational cybersecurity elements, including its cybersecurity profiles, mobile device security, and information classification for confidential supervisory information (CSI) contributed to the decline in overall program maturity.

The Board's IT and cybersecurity operating model includes both centralized and decentralized functions. In this operating model, the Board has not established an effective governance structure to ensure that cybersecurity strategy and priorities are aligned across all divisions. The chief information officer (CIO), who heads the Board's Division of Information Technology, has overall responsibility for implementing FISMA agencywide and offers information technology (IT) services Boardwide. However, 11 of 13 Board divisions have embedded IT groups, and the CIO has limited insight into the personnel and spending in those groups. In 2025, the Board budgeted about $30 million for its information protection program, representing about 10 percent of the total Boardwide IT budget. About half this amount is allocated outside the Division of IT. Further, of the Board's 88 full-time personnel performing cybersecurity functions, only 48 report to the CIO.

This year, we identified three areas in which the Board can strengthen its information security program:

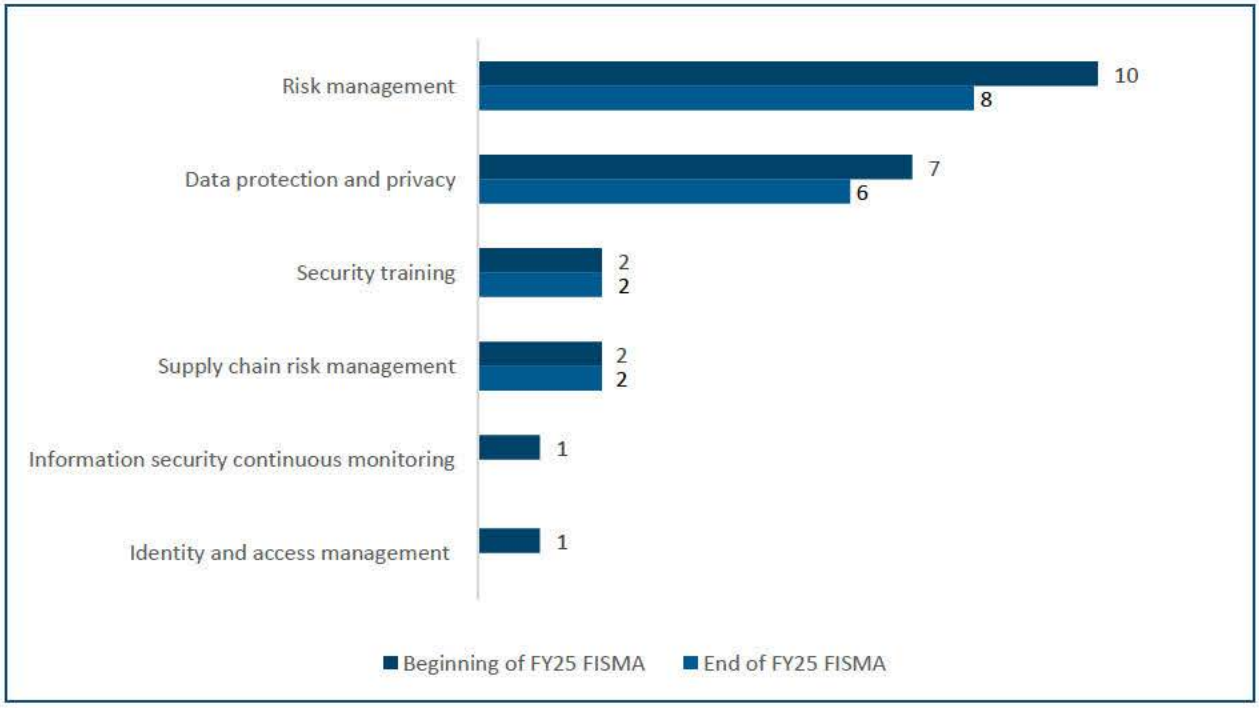
- Cybersecurity profiles. The Board has not developed cybersecurity profiles or used an alternative method to establish and communicate its cybersecurity objectives.
- Mobile device security. The Board inconsistently enforces content and data protection policies across laptops and Board-issued mobile devices.
- Information classification for CSI. Although the Board has developed an information classification standard for sensitive information, the agency does not have a security designation specific to CSI.

[7] Appendix A explains the scoring methodology outlined in the *FY 2025 IG FISMA Reporting Metrics*, which we used to determine the maturity of the Board's information security program.

Our report includes three new recommendations and one matter for management's consideration in these areas.

Further, 18 of the 23 recommendations made in prior years' FISMA audit reports that were open at the beginning of audit fieldwork remain open.[8] Based on corrective actions taken by the Board, we are closing 5 recommendations related to risk management, data protection and privacy, ISCM, and identity and access management (figure 2). The remaining 18 recommendations, which are related to risk management, data protection and privacy, security training, and SCRM, remain open. We will update the status of these recommendations in our fall 2025 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.

Figure 2. Status of Open Recommendations at the Start and the End of Our 2025 FISMA Audit, by Domain



Source: OIG analysis.

[8] Appendix B provides the status of all open recommendations.

Finding 1: Developing Cybersecurity Profiles Can Help the Board Assess, Tailor, and Prioritize Its Cybersecurity Approach

Cybersecurity profiles can be used by organizations to define the current state or target state of elements of their cybersecurity programs. Cybersecurity profiles can be used to define objectives, consider relevant context and resources, and assign responsibility for achieving the objectives. Organizations may use several cybersecurity profiles, which can be at different levels of the organization and for different types of information (see sidebar). For example, Board divisions may develop their own cybersecurity profiles to address differences in data sensitivity, such as the handling of Federal Open Market Committee (FOMC) data.

The Board has developed security models/programs for the overall organization, for the FOMC, and for Federal Reserve Bank systems supporting Board-delegated functions. However, the Board does not use cybersecurity profiles or an alternative method to establish and communicate its cybersecurity objectives and approach to achieving its objectives. Additionally, the Board has not defined its cyber risk tolerance, a key step to developing cybersecurity profiles.[9] A Board official informed us that the agency planned to develop cybersecurity profiles but had not prioritized the effort. As a result, the Board cannot ensure

CYBERSECURITY PROFILES

The NIST Cybersecurity Framework outlines a five-step approach that may be used to build a cybersecurity profile. The five steps, which can be repeated as needed, cover determining the scope and number of profiles, the inputs that can be considered, the information to include in the profile, gap analysis, and continuous improvement (figure 3).

Figure 3. Steps for Creating and Using a Cybersecurity Framework Organizational Profile

Source: National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*.

An organization may wish to use several profiles, for example, for different types of systems, each with a distinct scope.

[9] We recommended that the Board establish an organizational cyber risk tolerance in our 2023 FISMA audit report. *Cyber risk tolerance* refers to the level of cyber risk or the degree of uncertainty that is acceptable to an organization. Office of Inspector General, *2023 Audit of the Board's Information Security Program*, OIG Report 2023-IT-B-015, September 29, 2023.

that cybersecurity priorities are consistently aligned with mission objectives, current threats, and available resources.

Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, issued in May 2017, requires agencies to follow the NIST Cybersecurity Framework to manage cybersecurity risk. In 2017, the Board determined that the agency would voluntarily comply with the Cybersecurity Framework as a best practice consistent with its information security responsibilities under FISMA. According to the Cybersecurity Framework, organizations should develop and maintain a current cybersecurity profile that reflects mission objectives, threat landscape, and resources to guide implementation of cybersecurity activities. Further, organizations should develop a target profile that specifies the desired outcomes that an organization has selected and prioritized for achieving its cybersecurity risk management decisions. This in turn enables an organization to analyze gaps and create an action plan.

Recommendation

We recommend that the CIO

1. Develop and maintain cybersecurity profile(s) that define key elements of the Board's current and target cybersecurity program in alignment with the Board's organizational risk tolerance, mission objectives, and threat environment.

Management Response

In response to our draft report, the CIO concurs with our recommendation. Regarding recommendation 1, the response states that the Board will develop and maintain a NIST Cybersecurity Framework 2.0 current and target profile that balances the Board's cyber risk appetite, agency mission objectives, and the current threat environment. The Board estimates it will complete these efforts by the third quarter of 2026.

OIG Comment

The planned actions described by the Board appear responsive to our recommendation. We will follow up to ensure that the recommendation is fully addressed.

Finding 2: Enhancing Mobile Device Security Could Better Protect Sensitive Data

The Board provides its employees with devices such as mobile phones and laptops to conduct their work and serve the Board's mission. The Board allows employees to use Board-issued mobile devices for both personal and official purposes. On Board-issued mobile phones, [redacted] as long as they comply with the Board's *Information Technology Resources Use* policy.

SECURITY RISKS POSED BY THE INTEGRATION OF GENERATIVE ARTIFICIAL INTELLIGENCE INTO MOBILE PHONES

As highlighted in the Verizon *2025 Data Breach Investigations Report*, the integration of generative artificial intelligence (GenAI) into the operating system of mobile phones presents unique security risks. For example, GenAI is being integrated into the camera and messaging functionality of mobile phones by default. A mobile device management system, however, can be configured to help mitigate these risks.

We found inconsistent implementation of the Board's security controls for enforcing content and data protection restrictions for mobile applications. While the Board prohibits access to certain websites for conducting agency business on Board-issued laptops, the Board does not consistently enforce these restrictions for mobile devices. [redacted] We also noted that the Board allows users to access [redacted], which increases the risk of unauthorized data exfiltration. This risk is heightened as the Board does [redacted]

We also found that Board-issued mobile devices provide employees with [redacted] As such, these services could also be used to bypass controls that the Board has implemented [redacted]

[redacted]

[redacted] Insufficient security configurations and inconsistent enforcement of security controls on mobile devices increase the risk of exposure and exfiltration of sensitive Board data and exposure to cyber threats.

These issues primarily exist because the Board made a business decision to allow employees to use Board-issued mobile devices for both personal and official purposes. However, the agency has not implemented the technical controls and configurations needed to provide effective security in this model. For example, [redacted][11] [redacted] and are not sufficiently restrictive to enforce least privilege. A Board official notified us that the agency made this business decision to ensure mobile device usability.

The Board's *Information Technology Resources Use* policy notes [redacted] In addition, the policy states that users may not use [redacted] for conducting the Board's business. Further, NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, and NIST Special Publication 800-124, Revision 2, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, note that organizations should restrict mobile application permissions and [redacted] NIST Special Publication 800-53 also requires organizations to monitor and control communications and prevent data exfiltration.

Recommendations

We recommend that the CIO

2. Evaluate the dual-use model for the Board's mobile devices, in accordance with the Board's security objectives and risk tolerance, and review and update the *Information Technology Resources Use* policy as appropriate.
3. Strengthen mobile device security controls to enforce content and data protection policies.

Management Response

In response to our draft report, the CIO concurs with our recommendations. Regarding recommendations 2 and 3, the response states that the Board will evaluate the dual-use model for Board mobile devices against the Board's cyber risk appetite, mission objectives, and current threat environment and update policies, standards, and configurations as required to ensure appropriate levels

[11] The Board uses MDM software to manage mobile device security and enforce restrictions on managed applications.

[redacted]

of least privilege and data protection restrictions that align with the Board's risk appetite. The Board estimates it will complete these efforts by the third quarter of 2026.

OIG Comment

The planned actions described by the Board appear responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Matter for Management Consideration: Developing a Confidential Supervisory Information Classification Can Strengthen Safeguards for Financial Institution Information

The Board plays a significant role in supervising and regulating banking organizations, including bank holding companies and state member banks. The Board seeks to ensure that the banking organizations under its supervisory authority have safe and sound business practices and comply with all applicable federal laws and regulations. In the Federal Reserve System, the Board delegates to each Reserve Bank the authority to supervise financial institutions located within the Reserve Bank's District. As a result, both the Board and the Reserve Banks collect CSI. Unauthorized disclosure of CSI may harm financial regulators, banks, consumers, and the financial system.

In a June 2025 letter to the secretary of the U.S. Department of the Treasury, major financial trade associations cited recent cybersecurity incidents and expressed concern about regulators' safeguards for CSI (see sidebar). They urged that agencies be held to security standards comparable to those for financial institutions and that regulator incident response processes include timely notification and communication with affected institutions. Board and Reserve Bank staff currently use the information sensitivity classifications in the Board's *Information Classification and Handling Standard* for labeling CSI.

The Board's information classification standard provides a framework for designating and labeling sensitive information, including FOMC information. However, the Board does not have a designation specific to CSI. Board officials said that the Board has considered developing a CSI sensitivity label but had not because the effort would require defining and communicating multiple tiers of CSI and making extensive efforts to train staff, and that these efforts would be costly. However, we believe that technological advancements may reduce the cost and complexity of implementing a CSI sensitivity classification.

CSI BREACHES AT FEDERAL FINANCIAL REGULATORS

- In 2023, a financial regulatory agency experienced a major incident when an employee forwarded CSI to a personal email account without authorization. An office of inspector general report identified weaknesses in CSI handling and breach notification practices at the agency.
- In 2025, a financial regulatory agency reported that compromised administrative accounts were used to access its email environment and caused a major breach of CSI. The agency initiated internal and third-party reviews to strengthen security controls.

Without a designation for CSI, Board and Reserve Bank staff may misclassify CSI, under- or over-assessing the risk from its exposure. Additionally, the Board may be unable to efficiently identify breaches of CSI, which could delay notification to financial institutions and consumers, if needed. Given the changing threat and technology environment, we believe that management should consider reassessing the feasibility of developing and implementing a standardized sensitivity classification requirement for documents containing CSI.

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 six function areas outlined in the *FY 2025 IG FISMA Reporting Metrics*.

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

- focused our detailed testing activities on the annual core metrics and supplemental FY 2025 metrics identified in the *FY 2025 IG FISMA Reporting Metrics*[13]
- 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 for three sampled Board systems[14]
- 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 2025 IG FISMA Reporting Metrics*. Specifically, the metrics note that IGs have the discretion to determine whether an agency is effective in each of the Cybersecurity Framework functions and whether the agency's overall information security program is effective based on the results of the determinations of effectiveness in each domain, function, and overall program assessment. The metrics also direct IGs to place greater emphasis on the core metric ratings and use the supplemental metrics scores as part of their risk-based determinations of effectiveness.

In accordance with this 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 conclusions. We entered our specific maturity ratings at the function and domain levels in the CyberScope FISMA reporting application.

We conducted this work from March 2025 to October 2025. 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

[13] Core 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 are not considered a core metric but represent important activities conducted by security programs and contribute to the overall determination of security program effectiveness.

[14] To select these three systems, we used a risk-based methodology that included consideration of system risk levels, data types, technologies, users, and our previously completed work. We plan to communicate the results for these systems to the Board separately.

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.

Appendix B: Status of Prior FISMA Recommendations

Table B-1. Status of FISMA Recommendations That Were Open as of the Start of Our 2025 FISMA Audit, 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.	Pending verification	The Board submitted a closure request for this recommendation, which we are evaluating.
2022	1	We recommend that the CIO ensure that risks are appropriately categorized and prioritized on the Board's cybersecurity risk register.	Closed	The Board updated its processes and is categorizing and prioritizing risks on its cybersecurity risk register.
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 they plan to establish a standalone cybersecurity risk tolerance by the second quarter of 2026.
2023	2	We recommend that the CIO ensure all required attributes are consistently documented within the agency's cybersecurity risk register.	Closed	The Board incorporated the required attributes into its cybersecurity risk register.

Year	Recommendation		Status	Explanation
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. The Board plans to validate and update the results by the end of the fourth quarter of 2025.
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 they made updates to the agency's vendor risk management procedures, and they are working on populating historical vendor information in a consistent manner. The agency plans to finalize these efforts by the fourth quarter of 2025.
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 the agency is rolling out a new MDM tool. Once fully implemented, the tool will allow enforcement of updates. The agencywide implementation is currently planned for the fourth quarter of 2025.
2024	3	We recommend that the CIO 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.	Pending verification	The Board submitted a closure request for this recommendation, which we are evaluating.
2024	4	We recommend that the CIO evaluate and implement options to enforce the agency's existing guidance related to identifying and documenting system interconnections.	Open	Board officials informed us that they provided users with training for documenting system interconnections. The agency plans to validate users' input by the end of the third quarter of 2025.
2024	5	We recommend that the CIO develop and implement a mobile application scanning program that includes a vulnerability scanning solution and process to identify and remediate vulnerabilities.	Pending verification	The Board submitted a closure request for this recommendation, which we are evaluating.

Year		Recommendation	Status	Explanation
Supply chain risk management				
2024	1	We recommend that the chief operating officer develop an SCRM strategy that includes (a) a supply chain risk appetite and tolerance, (b) an enterprise SCRM governance structure, and (c) supply chain risk assessment processes that include mitigation strategies or controls.	Open	Board officials informed us that they established the SCRM plan and are working on developing a policy. The agency plans to complete the policy by the third quarter of 2026.
2024	9	We recommend that CIO update the Board's standard language in cloud service provider contracts to ensure that it is consistent with the Federal Risk and Authorization Management Program's *Incident Communications Procedures* incident reporting requirements.	Pending verification	The Board submitted a closure request for this recommendation, which we are evaluating.
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.	Closed	The Board developed a software tool to check for devices with default login credentials and has a process in place to address any identified instances of such devices.
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 the organization plans to address this recommendation as part of its ongoing efforts to strengthen its insider risk management program.

Year	Recommendation		Status	Explanation
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 the organization plans to address this recommendation as part of its ongoing efforts to strengthen its insider risk management program.
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	The Board is updating its PIAs, and Board officials estimate that the agency will finalize these efforts by the fourth quarter of 2025.
2023	7	We recommend that the CIO ensure that the process to update PIAs is adequately resourced for effective implementation.	Closed	The Board allocated sufficient resources to ensure effective implementation.
2024	2	We recommend that the CIO document and implement a baseline review and escalation process for DLP alerts.	Open	Board officials informed us that the organization plans to address this recommendation as part of its ongoing efforts to strengthen its insider risk management program.
2024	6	We recommend that the CIO ensure that the Board's *Incident Notification and Breach Response Plan* is reviewed, tested, and approved annually.	Open	Board officials informed us that the new incident response notification policies are nearly finalized. The agency plans to update its incident response plan in accordance with the new policy by the first quarter of 2026.
2024	8	We recommend that the CIO incorporate targeted phishing exercises into the Board's security awareness and training program and processes.	Pending verification	The Board submitted a closure request for this recommendation, which we are evaluating.
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 work roles and required training have been identified and the agency plans to update the security and privacy standard to reflect the required training in the third quarter of 2025.
2024	7	We recommend that the CIO develop and implement a role-based privacy training program.	Pending verification	The Board submitted a closure request for this recommendation, which we are evaluating.

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.	Closed	The Board issued a new *Continuous Monitoring Standard* in 2025. The *Continuous Monitoring Standard* and *Risk Management Standard* collectively serve as the ISCM strategy.

Appendix C: Management Response

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

DIVISION OF
INFORMATION TECHNOLOGY

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

Dear Michael,
Thank you for the opportunity to review and comment on the Office of the Inspector General (OIG) report on the Board of Governors of the Federal Reserve System's (the Board) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) for 2025. The report evaluates the Board's information security program in accordance with the fiscal year 2025 Core IG Metrics which were chosen in alignment with Office of Management and Budget (OMB) M-25-04, "Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements" and Executive Order (EO) 14028, " Improving the Nation's Cybersecurity," as well as OMB guidance to agencies in furtherance of the modernization of federal cybersecurity.

While your report found that the Board's information security program continues to make progress towards implementing federal cybersecurity mandates including those related to the establishment of a zero-trust architecture and continuing to maintain strong response and recovery capabilities, you found that the program was not operating effectively due to a low maturity level in governance, a new domain. The Board recognized this opportunity for improvement in governance in 2024 and has recently implemented a new enterprise information security operating model that will assist us in maturing in this domain while maintaining and enhancing our strengths in other domains. We remain committed to improving the Board's security posture, including remediation efforts in response to your report's recommendations, with which we concur. To address Recommendation 1, the Board will develop and maintain a NIST Cybersecurity Framework 2.0 current and target profile that balances the Board's cyber risk appetite, agency mission objectives, and the current threat environment. The Board will target Q32026 to complete this work. To address Recommendations 2 and 3, the Board will evaluate the dual use model for Board mobile devices against the Board's cyber risk appetite, mission objectives, and current threat environment and update policies, standards, and configurations as required to ensure appropriate levels of least privilege and data protection restrictions that are in alignment with the Board's risk appetite. The Board will target 3Q2026 to complete this work.

www.federalreserve.gov

We appreciate the professionalism and courtesy provided by the staff of the OIG throughout the 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: 2025.10.29 10:48:41 -04'00'

Jeff Riedel
Director, Chief Information Officer (CIO)

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

Abbreviations

CIO	chief information officer
CSI	confidential supervisory information
Cybersecurity Framework	*Framework for Improving Critical Infrastructure Cybersecurity*
DLP	data loss prevention
FISMA	Federal Information Security Modernization Act of 2014
FOMC	Federal Open Market Committee
FY	fiscal year
GenAI	generative artificial intelligence
IG	inspector general
ISCM	information security continuous monitoring
IT	information technology
MDM	mobile device management
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	privacy impact assessment
SCRM	supply chain risk management

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

Hotline

Report fraud, waste, abuse, and mismanagement involving the programs and operations of the Board or the CFPB.

oig.federalreserve.gov/hotline

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

1-800-827-3340

General Contact Information

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

202-973-5000

Media and Congressional Inquiries

oig.media@frb.gov