



Federal Reserve: 2026 Information Security Program Audit



Report Highlights

Federal Reserve: 2026 Information Security Program Audit



Why This Matters

A strong information security program is essential for the Board of Governors of the Federal Reserve System to protect the sensitive data it uses to inform decisions that affect employment, inflation, and economic stability for 342 million Americans.

Key Results

According to federal metrics for evaluating agencies' information security programs, the Board's information security program has a maturity level of 2 out of a possible 5, meaning its program is defined but not consistently implemented, and is therefore not considered effective. We found weaknesses in several areas:

- Governance gaps, decentralized IT operations, and inconsistent policy enforcement limit comprehensive security oversight and create potential vulnerabilities.
- Outdated and incomplete policies and standards result in staff relying on institutional knowledge, which increases the risk of security vulnerabilities during personnel transitions.
- Contingency planning processes are not fully coordinated between IT groups, and contingency plans cover entire divisions instead of specific IT systems as required by federal guidelines. As a result, the Board has limited assurance that critical systems can be recovered consistently and timely during disruptions.

Further, 13 of 17 recommendations from our prior annual information security audits remain open and unimplemented.

Action Needed

We have 8 new recommendations to strengthen enterprise IT governance and oversight and to implement effective policy, standards, and processes. The Board agreed with our recommendations and outlined its planned actions to address them. We will follow up to ensure that the recommendations are fully addressed.

Contents

Introduction.....	5
Objective.....	5
Background	5
FISMA Maturity Model.....	7
Summary of the Board’s 2026 FISMA Maturity Rating	9
Finding 1: Enterprise IT Governance Gaps Limit Security Visibility and Create Operational Risks.....	11
Independent IT Operations Reduce Enterprisewide Security Visibility and Create Potential Security Risks	11
An Incomplete System Inventory Limits the Board’s Ability to Manage Its IT Environment.....	13
Inconsistent Implementation of Corrective Actions Results in Increased Risk of Delayed Incident Notification.....	14
Limited Centralized MFA Exception Governance Increases the Risk of Credential-Based Attacks.....	15
Vulnerability Management Deficiencies Increase Security Risk and Limit Leadership Visibility.....	16
Incomplete Cybersecurity Risk Registers Limit the Board’s Ability to Prioritize Risks and Allocate Resources Effectively	18
Finding 2: Outdated and Incomplete Policies and Standards Prevent Consistent Implementation and Limit Program Maturity	20
Outdated Cybersecurity Policies Increase the Risk of Inconsistent Implementation	20
Application Configuration Documentation Gaps Limit Security Verification	21
Lack of a Comprehensive ISCM Strategy Limits Risk-Based Prioritization of Monitoring Activities.....	22
Finding 3: Misaligned Continuity Governance Could Limit Program Effectiveness	24
Limited Coordination Between Contingency Planning Groups Undermines Reliability of BIAs and BPAs	24
Reliance on Division-Level Contingency Plans Limits System-Specific Recovery Assurance	25

Conclusion and Recommendations	27
Agency Response and Our Evaluation	30
Appendix A: Scope and Methodology	31
Appendix B: Status of Prior Recommendations.....	33
Appendix C: Agency Response	37
Abbreviations.....	44

Introduction

A strong information security program is essential for the Board of Governors of the Federal Reserve System to protect the sensitive data it uses to inform decisions that affect employment, inflation, and economic stability for 342 million Americans. Under the Federal Information Security Modernization Act of 2014 (FISMA), the Board is required to implement information security protections to protect its systems and data from increasingly sophisticated cyber threats.

Objective

In accordance with FISMA requirements, our audit objectives 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. 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 agency's operations and assets, 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 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.² In March 2026, OMB and CIGIE directed IGs to use the *FY 2025 IG FISMA Reporting Metrics* for fiscal year (FY) 2026 evaluations. Previously, reporting metrics were generally updated each year.

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.

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) 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 (table 1).⁴

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

Function	Cybersecurity outcomes	Associated IG FISMA reporting domain
<i>Govern</i>	Provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations.	Cybersecurity governance, supply chain risk management
<i>Identify</i>	Understand the organization’s assets, suppliers, and related cybersecurity risks to enable an organization to prioritize its efforts consistent with its risk management strategy.	Risk and asset management
<i>Protect</i>	Supports the ability to secure assets to prevent or lower the likelihood and impact of adverse cybersecurity events.	Configuration management, identity and access management, data protection and privacy, security training
<i>Detect</i>	Enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring.	Information security continuous monitoring
<i>Respond</i>	Supports the ability to contain the effects of cybersecurity incidents.	Incident response

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 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.

<i>Recover</i>	Supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.	Contingency planning
----------------	---	----------------------

Source: 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.⁵ Metric, domain, and function 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.

⁵ NIST defines security 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 security requirements for the information system in its operational environment or enforcing/mediating established security policies. National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5, December 10, 2020.

Figure 1. IG FISMA Maturity Model



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

Summary of the Board's 2026 FISMA Maturity Rating

For FY 2026, the Board's information security program operates at a level-2 (*defined*) maturity, which does not meet the level-4 (*managed and measurable*) effectiveness standard established by OMB. This level represents a decline from prior years (level 4 in FY 2024 and level 3 in FY 2025). While this decline is partly attributable to control weaknesses we've identified this year, it is also influenced by several contextual factors. In FY 2023, OMB and CIGIE changed the FISMA scoring methodology from a mode-based approach, where the most frequent rating determined maturity levels, to a calculated average. This updated methodology more accurately reflects an agency's security posture but makes higher ratings more difficult to achieve, as weaknesses in any core area directly reduce the overall score. In addition, cybersecurity governance became a formal FISMA domain in FY 2025, meaning governance challenges that we have previously identified now have increased impact on the maturity score. Further, recent OIG audits and evaluations have identified additional control weaknesses related to FISMA metric areas. For example, our recent findings regarding the Board's information technology (IT) asset management affected FISMA maturity ratings in the risk and asset management domain.⁶

Three interconnected factors contribute to this year's assessment: governance gaps, policy enforcement inconsistencies, and unresolved prior recommendations. Governance challenges stem from the Board's historically decentralized IT operating environment, where division-embedded IT groups have operated independently from the enterprise. Separately, inconsistently enforced security policies and outdated documentation do not fully reflect current operations. Lastly, there remains a significant backlog of unresolved recommendations in various metric areas from our prior audits. These deficiencies prevent the Board from establishing a governance structure with standardized processes required to consistently implement security controls across the enterprise.

We have repeatedly highlighted governance challenges stemming from the Board's decentralized IT operating environment, and the Board has taken some significant steps in response to our findings. For example, the Board has implemented an updated IT operating model in recent years to better integrate technology functions, optimize technology in support of strategic mission opportunities, provide a more holistic user experience, and keep pace with modernizing technologies. The Board also maintains robust technology capabilities and has made meaningful investments in security tools and infrastructure. Despite this progress in streamlining IT operations, as we detail in this report, deficiencies in enterprise IT governance and policy enforcement continue to limit the effectiveness of these technological investments.

⁶ Office of Inspector General, *The Board Should More Effectively Manage and Secure Its Inventory of Unassigned Laptops and Hard Drives Ready for Disposal*, [OIG Report 2026-FMIC-B-005](#), March 30, 2026.

Until these governance and policy challenges are fully addressed, the positive effect of the Board's technology investments and operational capabilities will be limited. These governance and policy challenges may therefore limit the Board's ability to achieve the *managed and measurable* security posture necessary to effectively protect its critical financial information and systems.

Further, 13 of the 17 unresolved recommendations made in our prior years' FISMA audit reports remain open (appendix B). Based on corrective actions taken by the Board, we are closing 4 recommendations related to risk and asset management and security training. However, these unresolved recommendations significantly affect the Board's information security maturity rating, as many recommendations address foundational control weaknesses. Persistent open recommendations in areas like mobile vulnerability management, risk assessment processes, and data protection and privacy practices prevent the Board from demonstrating the consistent implementation and effectiveness required to achieve higher maturity levels. Until these recommendations are fully implemented, the Board will continue to face challenges in establishing the *managed and measurable* security posture necessary for an effective information security program.

Finding 1: Enterprise IT Governance Gaps Limit Security Visibility and Create Operational Risks

The Board's decentralized IT environment presents governance challenges that limit comprehensive visibility of IT security issues and incidents across the organization. Although the Board has taken significant steps to consolidate IT operations under an enterprise model, remnants of the decentralized structure persist, including independent IT operations that function outside comprehensive enterprise oversight, fragmented system inventory management, decentralized oversight of multifactor authentication (MFA) exceptions, and inconsistent vulnerability remediation processes. These issues limit the Board's ability to establish comprehensive visibility into its IT security posture and to consistently implement security controls enterprisewide. The Board also faces broader policy enforcement challenges in areas like contract governance and cybersecurity risk management. These governance and policy enforcement gaps create specific operational risks, which we detail below.

Independent IT Operations Reduce Enterprisewide Security Visibility and Create Potential Security Risks

The Board has an enterprisewide information security program that established the framework for implementing security controls and processes across the agency's information and information systems. The Division of Information Technology serves as the Board's designated provider of enterprise IT services. However, the Board also operates a decentralized IT model in which embedded IT support groups within various divisions provide specialized, non-enterprise support for their division's specific business or mission needs. While these embedded IT groups operate within the Board's information security program, we observed governance issues in how the Board oversees these groups. Specifically, one embedded IT group, which supports multiple Board divisions, maintains independent operations that are not fully aligned with the enterprise information security program. As one example, this embedded IT group maintains separate policies and processes for vulnerability management that do not align with overall Board procedures or provide enterprisewide visibility into risk management decisions. While the embedded IT group's *Patching Policy* stipulates that this group should follow overall Board guidance, the policy itself does not specify remediation time frames and escalation processes that align with the Board. Further, the policy states that these vulnerabilities can be reported to the information security officer (ISO) at the group's discretion rather than following mandatory enterprise escalation requirements. Additional areas of misalignment include the group

maintaining its own MFA exceptions and inventorying processes that are not consistent with the Board's information security program practices.

The Board has several policies that seek to establish enterprisewide IT security practices, including but not limited to

- The *Board Information Security Program* (BISP) sets forth the Board's enterprisewide information security program and requires that an inventory of all information systems, including infrastructure components and business applications, be maintained by the ISO. The BISP establishes the framework for protecting Board information and information systems and defines roles, responsibilities, and processes to ensure consistent application of security controls across the enterprise.
- The Board's *Information System Inventory Standard* establishes the objective of developing a systematic approach to inventory all information systems, subsystems, and system components reportable by the Board, including those used or operated by Federal Reserve Banks on the Board's behalf or under delegated authority, as well as systems used or operated by contractors on the Board's behalf. The purpose is to properly identify all information systems, subsystems, and system components authorized under the BISP.
- The Board's *Risk Management Standard* identifies the Division of IT as the Board's enterprise IT service provider. Further, this standard requires that risks to Board information and systems be identified, assessed, and managed through consistent enterprise processes that enable informed, risk-based decisionmaking.

Board officials informed us that the embedded IT group was created in 1985 to address specialized research computing needs. Officials further stated that because the group maintains its own domain, servers, and applications and has unique operational requirements, it has maintained separate operational practices that do not fully align with the Board standards referenced above. Recently, the Board has undergone transition efforts to integrate several embedded IT groups into the Division of IT, including parts of this embedded IT group's operational environment. However, these plans do not involve moving the group's entire operational environment under the Division of IT. Although Board policies, including IT policies, apply to all divisions without exception, the decision not to transition some IT systems from this group may limit the chief information officer's (CIO) visibility into the agency's entire information security environment. This decision differs from the Board's recent approach with other embedded IT groups, which were fully consolidated to unify operations under an enterprise IT operating model.

While the embedded IT group operates within the Board's information security program, without full visibility into all IT operations, the Board cannot ensure consistent implementation of security controls, timely remediation of vulnerabilities, or comprehensive visibility into all potential security risks and entry points across its IT environment. These governance issues may limit visibility into the agency's security posture and could result in vulnerabilities that go

undetected or unaddressed, potentially compromising the confidentiality, integrity, or availability of Board information and systems.

An Incomplete System Inventory Limits the Board's Ability to Manage Its IT Environment

The Board's system inventory is incomplete. It does not capture all the information for each system as required by the Board's *Information System Inventory Standard*. Specifically, the inventory lacks 10 of 32 required fields, including information type, authorization boundary, system owner, and cloud service type. In addition, the system inventory does not correctly classify systems that contain personally identifiable information or essential mission functions. Further, the Board's system inventory is missing systems that are listed in the agency's comprehensive cyber risk management and compliance solution.

The Board requires specific fields to be captured for each system in its *Information System Inventory Standard* to ensure adequate visibility and management of the Board's IT environment. Additional federal guidelines also contain specific guidance for agency system inventories. The Cybersecurity Framework requires that agencies identify and maintain an inventory of systems that support organizational operations and assets. NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, further requires that organizations develop and update an inventory of organizational systems. Finally, the *FY 2025 IG FISMA Reporting Metrics* requires agencies to maintain system inventories that are both complete and accurate.

The Board's system inventory is incomplete for two reasons. First, the Board's *Information System Inventory Standard* is not aligned with current practices because the inventory tool does not capture certain fields required by the standard. Second, the Board has not established sufficient governance to ensure compliance with inventory requirements. The Board uses multiple tools for system management but lacks processes to ensure that the inventory includes all systems operating in the Board's environment with accurate information.

Incomplete system inventory information limits the Board's visibility into its IT environment, increasing the risk that systems are not consistently identified, assessed, and managed across the enterprise. For example, incomplete inventory information could prevent the Board from quickly identifying which systems might be affected by cybersecurity threats or other security incidents.

Inconsistent Implementation of Corrective Actions Results in Increased Risk of Delayed Incident Notification

In 2024, we recommended that the Board update its cloud service provider (CSP) contract language to require alignment with FedRAMP standards.⁷ FedRAMP's 2024 *Incident Communications Procedures* required CSPs to report IT security incidents within 1 hour. In October 2025, the Board's procurement team issued revised standard contract language requiring 1-hour notification. This revised standard contract language aligned with FedRAMP's 2024 requirements, and we closed our recommendation. However, the Board has not consistently implemented this updated language. We learned that procurement staff was informed that the standard contract language updates were applicable only to contracts involving specific classifications of information rather than to all CSP contracts. Consequently, a CSP purchase order issued in December 2025 did not include notification requirements that align with FedRAMP requirements.

The 2024 *Incident Communications Procedures* has since been updated with the *FedRAMP Consolidated Rules for 2026*. The new procedure focuses incident reporting on likely or confirmed incidents that threaten the confidentiality or integrity of federal customer data and modifies the time frame for reportable incidents to factor in the potential adverse impact and the CSP's FedRAMP certification class.⁸ Until FedRAMP requirements are consistently incorporated, there is increased risk of delayed breach notification, which could allow threat actors more time to compromise agency information. Untimely breach notification to the Board could also delay notification to affected parties.

⁷ We recommended that the Board update its standard language in CSP contracts to ensure that it is consistent with FedRAMP's *Incident Communications Procedures* incident reporting requirements. Office of Inspector General, *2024 Audit of the Board's Information Security Program*, [OIG Report 2024-IT-B-020](#), October 31, 2024.

⁸ FedRAMP assigns certification classes to CSPs based on the level of security assurance they provide to government customers. Lower certification classes are less expensive but provide less assurance, while higher classes cost more but offer greater security assurance.

Limited Centralized MFA Exception Governance Increases the Risk of Credential-Based Attacks

OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, requires agencies to use strong MFA, which requires users to verify their identity using multiple methods, throughout their organizations. These requirements include enforcing MFA throughout the enterprise and requiring phishing-resistant authentication methods that protect against common cyberattacks for all staff, contractors, and partners.

Agencies must also maintain backup authentication procedures that provide exceptions to the MFA requirements for emergencies and account recovery situations. For example, an alternative authentication procedure for certain situations may allow users to log in using only a username and password, bypassing the requirement for a second authentication factor like a cryptographic identification device or token. However, these recovery processes pose potential security vulnerabilities because they bypass standard authentication requirements. Therefore, agencies should design recovery processes to be rare exceptions that require robust verification methods that are difficult for adversaries to replicate.

While the Board currently enforces phishing-resistant MFA and has MFA exception practices, these processes are not consistently governed. The Board does not centrally track who is exempt from phishing-resistant MFA requirements, with multiple exemption groups administered through different processes and across various divisions. Management could not readily explain why certain users have exemptions or have been given exemptions in response to requests for IT support. In addition, the Division of IT does not currently have visibility into how long exemptions have been in place or when they expire. Separately, we also found that about 97 percent of users in one embedded IT group are exempt from phishing-resistant MFA enforcement for certain applications. Board management stated that they believe these concerns will be addressed through its ongoing operating environment migration project, which includes transitioning users from the embedded IT group's current MFA exemptions to the Division of IT's enterprisewide practices.

Phishing-Resistant MFA

MFA requires more than one authentication factor for successful authentication. Phishing-resistant MFA, considered the gold standard, is resistant to phishing attacks that target user credentials.

Authentication Factors

Something you know: password or personal identification number

Something you have: cryptographic identification device or token

Something you are: fingerprint or other biometric characteristic data

As the migration process to the Division of IT continues, the Board should address two issues that limit centralized governance over MFA exceptions. First, the Board has not adequately defined processes for documenting, approving, and tracking MFA exceptions. In addition, technical constraints in one embedded IT group's environment prevented its MFA remediation efforts from progressing. As previously noted, the Board is currently integrating part of this embedded IT group's operational environment into the Division of IT, and management expects this migration will resolve the exemption issues. However, the migration has not been completed and is expected to finish by the end of FY 2026, according to a Board stakeholder.

Users exempt from phishing-resistant MFA have increased exposure to credential-based attacks and potential unauthorized access to sensitive information. Without centralized governance, the Board may lack sufficient information to determine whether MFA exceptions remain appropriate, are supported by valid business need, or are removed timely. As a result, users may remain exempt from phishing-resistant MFA longer than necessary, increasing the Board's exposure to credential-based attacks.

Vulnerability Management Deficiencies Increase Security Risk and Limit Leadership Visibility

The Board's vulnerability management program has deficiencies, including overdue vulnerabilities lacking required documentation, inconsistent practices that have allowed embedded IT groups to operate outside mandatory escalation requirements, and ineffective end-of-life (EOL) software tracking.

The Board's *Vulnerability Remediation Policy* requires system owners to remediate discovered vulnerabilities within defined time frames.⁹ If a vulnerability cannot be remediated within the required time frame, staff members can submit a risk acceptance request form for approval by the application manager, ISO, or ISO delegate. In addition, enterprise standards require tracking remediation efforts through plans of action and milestones (POA&Ms). These requirements align with FISMA and NIST Special Publication 800-53, Revision 5, which mandate that agencies implement agencywide information security programs that include timely remediation of system flaws and replacement of system components when vendor support ends.

However, we found that the vulnerability management program is not operating fully as designed. Although the Board generally maintains a high rate of vulnerability resolution, we identified critical and high-severity vulnerabilities, including EOL software, that remained unresolved well beyond the Board's required remediation deadlines, with some exceeding the

⁹ The Board's *Vulnerability Remediation Policy* requires remediation within 30 days for critical vulnerabilities, 60 days for high-severity vulnerabilities, and 90 days for medium-severity vulnerabilities. Vulnerabilities exceeding these time frames by an additional 30 days (60, 90, or 120 days total) are classified as "critically late" and must be escalated to the Board ISO.

“critically late” threshold. These overdue vulnerabilities lacked the documentation that Board policy requires, such as formal risk acceptance decisions or POA&Ms. After we asked about the status of these vulnerabilities, staff remediated several of the vulnerabilities. In addition, we observed broader governance issues with the embedded IT group detailed above that have resulted in inconsistent implementation of the Board’s vulnerability management practices.

The Board also does not have an effective enterprisewide process to track EOL software. Instead, a Board official informed us that the agency relies on system owners to monitor when products approach EOL and on automated vulnerability scanning tools to detect when products reach EOL.

These deficiencies exist primarily because the Board has not established effective governance over vulnerability management and oversight. While the Board has policies requiring timely remediation and accepted cryptographic protocols, it has not fully implemented procedures to ensure compliance. The Board lacks monitoring mechanisms to ensure POA&Ms or risk acceptances are documented for discovered vulnerabilities, and the escalation process is not functioning as intended. In addition, the Board does not maintain a comprehensive enterprisewide software inventory essential for identifying software approaching EOL. For EOL software, a Board official informed us that the agency relies on automated vulnerability scanning tools and system owners for detection. However, the scanning tool has plugin limitations, and no compensating controls exist. The Board requires software owners to maintain the Approved Software Catalog and supported versions. However, the Board lacks effective controls to track those life cycles operationally.

These governance gaps create cumulative security risks and may limit the Board’s ability to aggregate and respond to risks effectively at the enterprise level. Every unpatched vulnerability represents a potential entry point that adversaries could actively exploit, with risks intensifying for EOL software that will never receive vendor patches. The Board’s systems process and store information whose compromise could disrupt financial markets, undermine monetary policy effectiveness, threaten financial institution stability, and erode public confidence in the Federal Reserve System’s independence. Without documented risk decisions and unified vulnerability visibility across divisions, Board leadership may be unable to determine whether the organization’s risk posture aligns with mission requirements or whether additional resources are needed. Gaps in enterprise-level visibility limit effective planning for system upgrades, which could lead the Board to choose between emergency replacements during sensitive operational periods or continuing to operate vulnerable systems without adequate safeguards.

Incomplete Cybersecurity Risk Registers Limit the Board's Ability to Prioritize Risks and Allocate Resources Effectively

A cybersecurity risk register is a central record of current risks and related information for a given scope or organization. Current risks include both accepted risks and risks that have a planned mitigation path. Risk registers are a key aspect of managing enterprise cybersecurity risks because they consistently capture, organize, and communicate risk-related information (such as risk assessments, evaluation decisions, responses, and monitoring activities) from the individual system level to the enterprise level.

We found that the Board's cybersecurity risk registers do not accurately reflect the agency's risk environment. Specifically, the Board relies heavily on external reviews rather than its own processes to identify risks. The risk registers also contain inaccurate information, including closed recommendations and identification dates. In addition, the risk registers are not consistently maintained for different divisions. Further, the Board does not document risk assessments because risk register entries lack documented explanations for risk ratings. Board officials informed us that they do not require risk assessment documentation and their risk ratings are ultimately subjective.

The Board requires risks to be identified, assessed, and managed through consistent processes with quarterly updates for POA&Ms and annual updates for accepted risks in its *Risk Management Standard*. Federal guidance further outlines requirements for cybersecurity risk registers. NIST Interagency Report 8286, Revision 1, *Integrating Cybersecurity and Enterprise Risk Management*, details that a cybersecurity risk register should include risk ID, risk priority, risk category, risk description, risk response type, risk response cost, risk response description, status, current risk assessment, and risk owner. The publication also notes that risk registers are critical documents for communicating risk information to senior leaders and should be supplemented with risk detail records documenting assumptions, results, and risk scenarios. Additional NIST publications also require supporting risk data be recorded in detail records.¹⁰

While the Board's *Risk Management Standard* contains overarching guidance for the agency's cybersecurity risk registers, it does not provide sufficient detail or specific requirements for documenting risk assessments and maintaining the cybersecurity risk register. As a result, staff lack clear guidance on required information and detail necessary for a cybersecurity risk register, leading to inconsistent interpretation and application across the organization. Inaccurate cybersecurity risk registers limit the Board's ability to prioritize risks and allocate resources effectively. Lack of clear cybersecurity risk register guidance has affected several additional

¹⁰ NIST Interagency Report 8286A, Revision 1, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*, December 2025; NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2012.

cybersecurity areas identified in this report, including contingency planning, EOL software tracking, and vulnerability management.

Finding 2: Outdated and Incomplete Policies and Standards Prevent Consistent Implementation and Limit Program Maturity

The Board's cybersecurity policies and procedures do not reflect current operations or fully incorporate federal requirements, preventing the Board from achieving a *consistently implemented* maturity. Under the FISMA maturity model, consistent implementation requires that security policies and procedures be defined and applied across the enterprise. However, when policies are outdated or absent, the Board cannot demonstrate standardized implementation or establish unified expectations, which can lead staff to rely on institutional knowledge rather than documented procedures. This lack of formalized, current guidance manifests across multiple areas: outdated cybersecurity policies that do not reflect current operations; incomplete application configuration documentation; and the absence of a comprehensive information security continuous monitoring (ISCM) strategy. These policy and documentation gaps are particularly important to address as the Board continues to transition staff from embedded IT groups to the Division of IT. Without adequately documented processes, the Board faces an elevated risk that critical security practices may be implemented inconsistently or lost entirely during personnel transitions. Without current, comprehensive policies that reflect operational practices and federal requirements, the Board cannot establish the consistent implementation necessary to advance beyond a defined maturity.

Outdated Cybersecurity Policies Increase the Risk of Inconsistent Implementation

The Board's cybersecurity policies and procedures do not reflect its operational environment. Specifically, multiple Board policies, including the BISP and *Information System Inventory Standard*, do not align with current operational practices. In addition, the Board's *Incident Response Program* and *Incident Response Manual* documentation contain outdated information.

The *FY 2025 IG FISMA Reporting Metrics* requires agencies to have formalized and documented security policies, procedures, standards, or processes to achieve a defined maturity. Identity and access management metrics are an exception, as they do not include a policy-specific maturity indicator. In addition, NIST Special Publication 800-53, Revision 5, requires that organizations

develop, document, and disseminate security and privacy policies and procedures and review and update policies and procedures to ensure they remain current.

The Board's policy review and update process did not keep pace with operational changes, resulting in multiple policies that no longer accurately reflect the agency's environment. Without updated enterprise policies, Board staff may lack awareness of current cybersecurity incident response procedures, resulting in inconsistent implementation. As noted above, this risk is particularly relevant as the Board transitions staff from embedded IT groups to an enterprise IT operating model. With outdated policies, roles and responsibilities and requirements for those in new roles may be unclear. Further, reliance on institutional knowledge increases the risk of knowledge loss when staff leave.

Application Configuration Documentation Gaps Limit Security Verification

While the Board's infrastructure components, such as servers and databases, demonstrate strong configuration documentation practices, applications have gaps in configuration documentation and do not consistently meet federal standards. System owners of commercial off-the-shelf (COTS) applications often rely on vendor upgrade guides as their baseline documentation, but the guides reviewed were not designed for that purpose. They do not capture current software versions installed in the Board's environment, configuration changes, or application-specific security settings that the Board has implemented. Documentation challenges are more pronounced for the Board's internally developed applications, which often lack baseline specifications. Instead, developers treat system development life cycle documentation and source code repositories as baseline documents, even though these materials serve different purposes. For these applications, configuration knowledge exists primarily in source code rather than formal baseline documentation.

The Board has established configuration baseline requirements in its *Secure Configuration Baseline Standard*, which requires system owners to develop and document information security configuration settings in a configuration baseline for infrastructure devices, middleware, COTS business applications, and development platforms. The standard further requires, along with the Board's *Application Development Security Standard*, that internally developed business applications be managed using a documented system development life cycle.

Federal information security requirements and configuration management best practices emphasize the importance of establishing, documenting, and maintaining baseline configurations that reflect the current approved state of information systems. For example, NIST requires organizations to develop, document, and maintain current baseline configurations with

periodic reviews and updates and to document and maintain configuration settings.¹¹ NIST also establishes that configuration management principles apply to all system components, which include COTS products and custom-developed applications.¹²

Baseline configuration documentation weaknesses occurred because the Board's standards do not provide system owners with enough direction for establishing and documenting authoritative baseline configurations that consistently identify the approved configuration of their system. For example, the Board's *Secure Configuration Baseline Standard* explicitly excludes internally developed applications and, in general, lacks specific content requirements for baseline documentation, such as current software versions or periodic review. For internally developed applications, the *Application Development Security Standard* requires system development life cycle processes but does not mandate baseline documentation. Further, while the *Secure Configuration Baseline Standard* requires automated monitoring or biannual manual review of baselines, it does not require that the baseline documentation be updated when system changes occur.

Without adequate baseline configuration documentation, the Board faces several operational security risks. When staff transition to new roles, institutional knowledge of security configuration decisions is lost, which can make it difficult for new personnel to validate or re-create intended security postures. In addition, the Board may not be able to identify when system configurations deviate from approved secure states. Configuration drift might go undetected because there is no documented standard against which to compare actual system states, and change management becomes inconsistent without a single baseline to assess the security impact of proposed changes.

Lack of a Comprehensive ISCM Strategy Limits Risk-Based Prioritization of Monitoring Activities

While the Board has established ISCM standards, those standards do not fully align with federal guidelines or address all federal requirements for an ISCM strategy. The Board uses multiple standards that document ongoing control assessments, ISCM processes, and security weakness remediation, but lacks a comprehensive ISCM strategy that defines monitoring requirements across organizational tiers and establishes how risk tolerance determines continuous monitoring frequencies. In addition, the Board's ISCM governance documentation contains inconsistencies across related standards. For example, the Board's *Risk Management Standard* refers to the Board's continuous monitoring strategy, which does not exist.

¹¹ NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, CM-2 and CM-6 controls, December 10, 2020.

¹² NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011.

The *FY 2025 IG FISMA Reporting Metrics* requires agencies to have an organizationwide ISCM strategy. The reporting metrics further require agencies to define monitoring requirements across organizational tiers and establish how risk tolerance determines minimum monitoring frequencies within their ISCM policies and strategy. In addition, NIST Special Publication 800-53, Revision 5, requires agencies to develop an organizationwide continuous monitoring strategy that includes establishing metrics to monitor control effectiveness. Further, NIST Special Publication 800-137, *ISCM for Federal Information Systems and Organizations*, emphasizes that ISCM should operate at three organizational tiers—organization, mission/business process, and information system—and that security controls are aligned with organizational risk tolerance.

The Board lacks a comprehensive ISCM strategy because it relies on separate policies, such as the *Continuous Monitoring Standard* and *POA&M Standard*, that focus on system-specific requirements rather than a comprehensive ISCM strategy incorporating all organizational tiers. Without an established ISCM strategy, the Board lacks a foundational framework for risk-based continuous monitoring, which affects multiple areas of the agency's information security program. The Board may lack sufficient information to consistently prioritize monitoring activities based on risk; evaluate the effectiveness of monitoring activities; or make timely, risk-informed decisions about its cybersecurity posture. In addition, inconsistencies across ISCM-related documentation may reduce clarity about monitoring expectations.

Finding 3: Misaligned Continuity Governance Could Limit Program Effectiveness

While the Board has established contingency planning practices and processes, the agency's *recover* function maturity is limited by fragmented governance and a lack of coordinated contingency guidance. At a *defined* maturity, organizations must have documented policies and processes for developing contingency plans, which include conducting business impact analyses (BIAs). To achieve consistent implementation across the enterprise for the *recover* function, agencies must consistently incorporate BIA results into strategy and plan development; integrate system-level BIAs with organizational BIAs to determine recovery priorities and resource requirements; and implement information system contingency plan (ISCP) testing that integrates with related plans, such as incident response and continuity of operations (COOP). However, the Board maintains separate contingency planning processes that are not fully coordinated between its Intelligence, Insider Risk, and National Security Programs (IINS) and the Division of IT. In addition, the Board has not established a contingency planning or continuity policy that defines requirements, roles, responsibilities, or procedures for conducting BIAs and business process analyses (BPAs). Further, the Board has not developed ISCPs for individual systems and instead relies on division-level COOP plans and system security plans that lack required technical recovery procedures, recovery priorities, and system restoration activities. Without established governance coordinating IINS and Division of IT contingency planning responsibilities, the Board cannot achieve optimal maturity and has limited assurance that critical systems can be recovered consistently and timely during disruptions, potentially affecting its ability to maintain essential functions.

Limited Coordination Between Contingency Planning Groups Undermines Reliability of BIAs and BPAs

While the Board has established contingency planning responsibilities, those responsibilities are split between two groups. IINS manages business-focused BIA and BPA activities and continuity planning, and the Division of IT manages technical contingency planning. However, these groups do not have defined policies or procedures that include requirements, roles, and responsibilities for coordination or alignment. This governance gap has led to discrepancies in the BIA and BPA documentation the Board relies on for continuity planning.

Specifically, existing procedures neither define how IINS and the Division of IT should coordinate on organizational roles and responsibilities for BIA, BPA, and contingency planning activities, nor establish requirements for how frequently documentation maintained by each group should be reviewed and updated in coordination with the other. As a result, we observed outdated and inconsistent continuity documentation across the Board. Most BIAs have not been updated since 2023 or earlier, over half of BPAs have not been updated since 2024 or earlier, and several 2025 BPA updates were not reflected in corresponding BIAs. In addition, BIA and BPA maintenance and review practices varied across Board divisions, with no coordinated approach to ensure technical contingency information aligned with business impact determinations.

The Board's COOP plan establishes an expectation that the Board maintain formal, documented, approved, and periodically reviewed procedures governing the readiness and preparedness activities to support guidance and performance of Board essential functions. Specific to the *recover* function, the *FY 2025 IG FISMA Reporting Metrics* establishes that agencies must have documented policies, procedures, and processes for conducting organizational and system-level BIAs. Agencies are further required to incorporate results into the development and maintenance of relevant response, recovery, and continuity strategies and plans for contingency planning efforts to be consistently implemented.

Without an established governance framework defining coordination between IINS and the Division of IT, business impact documentation may not align with technical recovery capabilities. This lack of alignment increases the risk that recovery priorities and time frames documented in BIAs and BPAs may conflict with technical contingency information. In addition, personnel may rely on outdated or inconsistent recovery information during disruptions, and contingency testing may not validate recovery of the Board's most critical business functions.

Reliance on Division-Level Contingency Plans Limits System-Specific Recovery Assurance

The Board currently performs biannual contingency testing and maintains division-level COOP plans. However, the agency has not developed ISCPs for individual information systems that contain all required components, such as detailed technical recovery procedures, system-specific recovery priorities, recovery point objectives, alternate processing procedures, recovery testing requirements, or system restoration activities for individual systems. A Board official stated that the agency captures ISCP information as part of system security plans. However, these plans do not provide the system-specific recovery procedures required for individual information systems.

The Board's BISP only requires division-level contingency plans. However, the *FY 2025 IG FISMA Reporting Metrics* requires agencies to have defined policies, procedures, and processes for information system contingency plan testing that are integrated, to the extent practicable, with the testing of COOP plans. The metrics also require integration of system-level BIAs with organizational BIAs to determine recovery priorities and resource requirements. NIST SP 800-34,

Revision 1, *Contingency Planning Guide for Federal Information Systems*, defines an ISCP's purpose as providing procedures and capabilities for recovering an information system. It further states that the ISCP is an information system-focused plan that may be activated independently from other plans or as part of a larger recovery effort coordinated with a COOP.

COOP versus ISCP

COOPs apply to mission-essential functions of federal agencies.

ISCPs apply to all information systems in federal agencies.

The Board has not developed ISCPs because it has not established policies and procedures requiring the creation, maintenance, and implementation of ISCPs for individual information systems. Without ISCPs, the Board has limited assurance that individual systems can be recovered consistently and timely, reducing its ability to establish recovery priorities, validate recovery time and point objectives, conduct comprehensive recovery testing, and demonstrate compliance with federal contingency planning requirements.

Conclusion and Recommendations

The Board's information security program operates at a level-2 (*defined*) maturity, falling short of the *managed and measurable* effectiveness standard set by federal guidance. This gap stems from three interconnected challenges: fragmented governance that has allowed certain systems to operate outside comprehensive enterprise oversight, inconsistently enforced security policies and outdated documentation that does not fully reflect current operations, and governance gaps that reduce assurance of timely system recovery during disruptions. In addition, 13 of 17 recommendations from our prior FISMA audits remain open and continue to affect the Board's maturity level. These deficiencies extend beyond administrative concerns and create vulnerabilities in systems that protect sensitive financial data, supervisory information, and Board operations. Collectively, these gaps limit the Board's ability to maintain a consistent, enterprisewide security posture necessary to protect against increasingly sophisticated threats to the nation's financial infrastructure.

To strengthen the Board's information security program, we have 8 new recommendations focused on two areas: (1) establishing comprehensive enterprise IT governance and oversight mechanisms and (2) implementing effective policy enforcement and monitoring controls supported by documentation that reflects current operations and federal requirements. Implementing these recommendations will enable the Board to achieve comprehensive visibility into its security posture, consistently implement security controls across the enterprise, and effectively manage cybersecurity risks to Board information and information systems.

We recommend that the CIO

1. Conduct a comprehensive risk assessment of the embedded IT group's independent IT operations and establish appropriate governance and oversight mechanisms based on the assessment results.
2. Establish oversight mechanisms to ensure all systems comply with the Board's inventory requirements.
3. Enhance management and oversight of MFA exceptions to align with the Board's risk tolerance by
 - a. Developing and implementing an enterprisewide policy governing MFA exceptions that is aligned with the Board's risk tolerance.
 - b. Evaluating MFA exception populations and implementing appropriate measures to reduce or otherwise manage exceptions consistent with the Board's organizational risk tolerance.

4. Strengthen vulnerability management processes and oversight to ensure timely remediation and appropriate risk management by
 - a. Ensuring critically late vulnerabilities are escalated to the ISO as required by Board policy, with defined accountability for resolution or risk acceptance decisions.
 - b. Ensuring the ISO has the capability to monitor vulnerability remediation status across all divisions, track vulnerabilities that remain unresolved beyond remediation deadlines, and verify that POA&Ms or risk acceptance decisions are documented for all vulnerabilities that cannot be mitigated by Board's established deadlines.
 - c. Establishing processes to proactively identify and manage software approaching or reaching EOL.
5. Establish and implement formal, standardized processes for identifying and assessing organizational risk.
6. Update and develop the Board's information security policies, procedures, standards, and processes to reflect federal requirements and operational practices by
 - a. Updating all information security policies to reflect operational practices.
 - b. Developing comprehensive configuration documentation standards that establish specific baseline requirements for all system types, including COTS applications, internally developed applications, and infrastructure components.
 - c. Developing an enterprisewide ISCM strategy that aligns with federal requirements and organizational risk tolerance.
7. Work with IINS to
 - a. Develop and implement enterprisewide policies that define the responsibilities and requirements for performing and maintaining BIAs and BPAs, including coordination mechanisms to ensure alignment between BIAs and technical contingency planning.
 - b. Develop and implement policies for information system contingency plans consistent with federal requirements.

We recommend that the chief financial officer (CFO)

8. Strengthen CSP contract management to ensure alignment with FedRAMP requirements and establish appropriate oversight by

- a. Updating the Board's standard language in CSP contracts to ensure that the language is consistent with FedRAMP incident reporting requirements.
- b. Performing a review of contracts executed after issuance of the revised incident reporting language to identify agreements with outdated requirements and, where appropriate, coordinate with the CIO to determine whether contract modifications or other correction actions are necessary.
- c. Ensuring that the CIO reviews revisions to standard cybersecurity clauses and communicates recommended changes and final concurrence.

Agency Response and Our Evaluation

In response to our official draft report, the CIO and the CFO concurred with the findings and recommendations and conveyed the Board's commitment to addressing the items outlined in our recommendations. The agency's formal response to the report is included in its entirety in appendix C.

The actions described by the CIO and the CFO appear to be responsive to our recommendations. We will follow up with the Board quarterly to ensure that the recommendations are fully addressed.

Appendix A: Scope and Methodology

Our audit objectives, based on FISMA requirements, were to evaluate the effectiveness of the Board's information security program and practices for FY 2026, as required by FISMA and OMB Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*.

To conduct our work, we used the *FY 2025 IG FISMA Reporting Metrics* (Version 2.0, dated April 3, 2025), which aligns with the Cybersecurity Framework. The assessment uses a maturity model spectrum with five levels: *ad hoc* (level 1), *defined* (level 2), *consistently implemented* (level 3), *managed and measurable* (level 4), and *optimized* (level 5). In this context, achieving level 4 or above represents an effective level of security.

Our scope encompassed six Cybersecurity Framework function areas:

1. *Govern*: cybersecurity governance and cybersecurity supply chain risk management
2. *Identify*: risk and asset management
3. *Protect*: configuration management, identity and access management, data protection and privacy, and security training
4. *Detect*: ISCM
5. *Respond*: incident response
6. *Recover*: contingency planning

The assessment period covered FY 2026, with our responses required for submission to the CyberScope reporting tool no later than July 30, 2026.

We used a calculated average approach wherein the average of metrics in a particular domain determines the effectiveness of individual function areas and the overall program. Calculated averages are not automatically rounded to a particular maturity level. We retain discretion to determine overall effectiveness based on core metric results; supplemental metric results as supporting data points; as well as other factors, such as results of other cybersecurity audits and evaluations conducted during the review period, progress in addressing outstanding recommendations, and security incidents reported during the review period.

To assess the effectiveness of the Board's information security program across all FISMA function areas, we

- conducted structured interviews with senior leadership in the Division of IT

- observed IT tools and processes in use
- analyzed security policies, procedures, and documentation, including but not limited to system security plans, authorization packages, risk assessments, BIAs, configuration management baselines, access control records, security training materials, MFA records, and contract records.
- performed data analysis in select areas, such as system inventory, cybersecurity risk registers, vulnerability scan results, network and endpoint monitoring capabilities, security configurations, MFA exception populations, data protection and encryption controls, BIAs, and BPAs.

In addition, we selected nonstatistical, judgmental samples in select areas across the *govern*, *protect*, *detect*, and *respond* functions. We selected each sample based primarily on specific risk factors unique to each population as well as document availability. The results cannot be projected to the full populations. However, these samples informed our testing in the following security functions and were used in conjunction with additional testing to support our conclusions.

- *Govern*: We sampled about 4.5 percent of awarded contracts, focusing on factors like contract type and handling of sensitive data.
- *Protect*: In total, we sampled about 7 percent of various asset inventories to review application baseline configurations, EOL software, system-level access controls, and system backup configurations. We focused these samples on risk factors, such as system type, types of sensitive data handled, and risk level of the assets. In addition, because of documentation availability, we sampled less than 1 percent of overdue critical and high vulnerabilities from agency scans covering December 2025–March 2026. We focused our sample on the longest outstanding vulnerabilities and those related to unsupported or EOL software.
- *Detect*: We sampled about 2 percent of information systems to review continuous monitoring processes, such as authorizations, control assessments, and system-security plan maintenance. We focused our sample on risk factors, such as system type, types of sensitive data handled, business function, and risk level.
- *Respond*: We sampled about 7 percent of potential incident types, based on judgmental review of alert names, to identify potential data loss incidents.

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 April to October 2026.

Appendix B: Status of Prior Recommendations

Table B-1. Status of FISMA Recommendations That Were Open as of the Start of Our FY 2026 FISMA Audit, by Security Function

Year	Recommendation	Status	Explanation
Govern			
2024	1 We recommend that the chief operating officer develop a supply chain risk management strategy that includes (a) a supply chain risk appetite and tolerance, (b) an enterprise supply chain risk management governance structure, and (c) supply chain risk assessment processes that include mitigation strategies or controls.	Open	Board officials informed us that work to address this recommendation is ongoing.
2025	1 We recommend that the CIO 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.	Open	The Board recently developed current and target cybersecurity profiles in response to the recommendation. However, the agency has not yet determined its organizational risk tolerance.
Identify			
2023	1 We recommend that the CIO prioritize the definition and incorporation of a cybersecurity risk tolerance into the agency's cybersecurity policies,	Open	Board officials informed us that work to address this recommendation is ongoing.

Year	Recommendation	Status	Explanation
	procedures, and processes, as appropriate.		
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 work to address this recommendation is ongoing.
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	The Board has demonstrated progress by beginning to identify subcontractors for certain contracts executed in FY 2026. However, the practice has not been implemented consistently across the vendor population.
2023	5 We recommend that the CIO enforce the agency's <i>iOS Update and Device Inactivity Policy</i> to ensure that agency services are denied to mobile devices that are out of compliance.	Open	Board officials informed us that work to address this recommendation is ongoing.
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.	Closed	The Board incorporated system interconnection requirements into the FY 2026 FISMA training and designated the training as mandatory for the relevant individuals.
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.	Closed	The Board implemented mechanisms to enforce its existing guidance by updating assessor test steps to verify information exchange documentation in system security plans and creating a dashboard to track compliance.
2024	5 We recommend that the CIO develop and implement a mobile application scanning program	Open	Board officials informed us that work to address this recommendation is ongoing.

Year	Recommendation	Status	Explanation
	that includes a vulnerability scanning solution and process to identify and remediate vulnerabilities.		
Protect			
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.	Closed	The Board developed a formal training standard, defined security-significant roles, required role-based training, and implemented operational assignment and completion tracking mechanisms.
2019	5 We recommend that the CIO work with the System to ensure that the data loss prevention 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 work to address this recommendation is ongoing.
2019	6 We recommend that the CIO develop and implement a Boardwide process to incorporate the review of data loss prevention logs into employee and contractor offboarding processes to identify any potential unauthorized data exfiltration or access.	Open	Board officials informed us that work to address this recommendation is ongoing.
2024	2 We recommend that the CIO document and implement a baseline review and escalation process for data loss prevention alerts.	Open	Board officials informed us that work to address this recommendation is ongoing.

Year	Recommendation	Status	Explanation
2024	6 We recommend that the CIO ensure that the Board's <i>Incident Notification and Breach Response Plan</i> is reviewed, tested, and approved annually.	Open	Board officials informed us that work to address this recommendation is ongoing.
2024	8 We recommend that the CIO incorporate targeted phishing exercises into the Board's security awareness and training program and processes.	Closed	The Board has implemented a formal phishing simulation program supported by the newly established standard, which incorporates targeted phishing exercises into the security awareness program.
2025	2 We recommend that the CIO 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 <i>Information Technology Resources Use</i> policy as appropriate.	Open	Board officials informed us that work to address this recommendation is ongoing.
2025	3 We recommend that the CIO strengthen mobile device security controls to enforce content and data protection policies.	Open	Board officials informed us that work to address this recommendation is ongoing.

Table B-2. Status of Non-FISMA Recommendations That Were Submitted for Closure

Year	Recommendation	Status	Explanation
2022	1 Ensure that the Cloud Resource Center's inventory of cloud projects in the configuration and production phases is comprehensive and periodically maintained.	Closed	The Cloud Resource Center has been placed on pause, and the Board has moved to a different technology approach for managing cloud projects. As such, this recommendation is no longer applicable to the Board.

Appendix C: Agency Response



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

DIVISION OF
INFORMATION TECHNOLOGY

October 23, 2026

Michael VanHuysen
Associate Inspector General for Audits and Evaluation
Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Mr. VanHuysen:

Thank you for the opportunity to comment on the Office of the Inspector General's (OIG) draft report titled *Federal Reserve: 2026 Information Security Program Audit*. We appreciate the OIG's work to develop the report and the recommendations.

Overview

We concur with the recommendations from the Office of Inspector General's comprehensive evaluation of the Board's information security program for fiscal year 2026. We appreciate the thorough assessment and recognize the value of the findings presented in identifying areas where the Board can strengthen its security posture and advance program maturity. We view this audit as an important opportunity to enhance our information security program's effectiveness across all Cybersecurity Framework function areas.

In developing our corrective action plans for the 2026 FISMA audit findings, we have conducted a comprehensive assessment of the relationship between these recommendations and the thirteen outstanding recommendations from prior annual FISMA audits. We have identified substantial overlap and interconnected remediation opportunities where addressing the current findings will concurrently resolve or significantly advance progress on prior recommendations. Our approach recognizes that many of the governance gaps, policy enforcement challenges, and documentation deficiencies identified in the current audit share common root causes with previously identified weaknesses. Therefore, we have structured our remediation efforts to leverage this shared foundation and ensure that corrective actions address both current and historical findings where the underlying issues are related.

Draft corrective action plans have been developed for each recommendation. These plans incorporate consideration of prior findings to ensure comprehensive and

www.federalreserve.gov

sustainable solutions that will advance the Board's information security program toward the managed and measurable maturity level required for program effectiveness. We look forward to working collaboratively with the Office of Inspector General toward our shared goal of establishing a robust, enterprise-wide information security program that effectively protects the Board's critical information and systems supporting the nation's financial infrastructure and monetary policy operations.

We appreciate your professionalism and diligence during the audit. We look forward to continuing to work with your office in the future.

Regards,

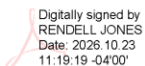
JEFFREY
RIEDEL



Digitally signed by
JEFFREY RIEDEL
Date: 2026.10.23
13:20:16 -04'00'

Jeff M. Riedel
Chief Information Officer, and Director, Division of Information Technology

RENDELL
JONES



Digitally signed by
RENDELL JONES
Date: 2026.10.23
11:19:19 -04'00'

Rendell L. Jones
Chief Financial Officer and Director, Division of Management and Financial Services
(with respect to recommendation 8)

cc: Winona Varnon
Tara Pelitere
Charles Young
Kim Briggs
Kelly Gibbs

**Response to recommendations presented in the Draft OIG Audit Report,
“Federal Reserve: 2026 Information Security Program Audit”**

Finding 1: Enterprise IT Governance Gaps Limit Security Visibility and Create Operational Risks

Recommendation 1:

We recommend that the chief information officer conduct a comprehensive risk assessment of the embedded IT group's independent IT operations and establish appropriate governance and oversight mechanisms based on the assessment results.

Management Response:

We concur with the finding and recommendation. The Board will conduct a comprehensive risk assessment of the embedded IT group's independent IT operations to evaluate security vulnerabilities, governance gaps, and operational risks. Based on the assessment results, the Board will establish appropriate governance and oversight mechanisms commensurate with the risks identified, including measures to improve Chief Information Officer visibility into IT operations.

Target date: Fourth quarter of 2027.

Recommendation 2:

We recommend that the chief information officer establish oversight mechanisms to ensure all systems comply with the Board's inventory requirements.

Management Response:

We concur with the finding and recommendation. The Board will establish oversight mechanisms to ensure systems comply with the Board's inventory requirements as specified in the Information System Inventory Standard. This will include controls to verify inventory completeness and accuracy and processes to confirm that systems are recorded consistent with the Information System Inventory Standard.

Target date: Third quarter of 2027.

Recommendation 3:

We recommend that the chief information officer enhance management and oversight of MFA exceptions to align with the Board's risk tolerance by

- a. Developing and implementing an enterprise-wide policy governing MFA exceptions that is aligned with the Board's risk tolerance.
- b. Evaluating MFA exception populations and implementing appropriate measures to reduce or otherwise manage exceptions consistent with the Board's organizational risk tolerance.

Management Response:

We concur with the finding and recommendations. For Recommendation 3a, the Board will develop and implement an enterprise-wide policy governing multifactor authentication (MFA) exceptions that clearly defines approval processes, documentation requirements, review frequencies, and aligns with the Board's organizational risk tolerance. For Recommendation 3b, the Board will evaluate MFA exception populations across the enterprise, including those maintained by embedded IT environments, and implement appropriate measures to reduce exceptions or otherwise manage them consistent with the Board's risk tolerance. This will include completing the ongoing consolidation of embedded IT environments to enterprise-wide authentication services, including MFA enforcement practices.

Target date: Third quarter of 2027.

Recommendation 4:

We recommend that the chief information officer strengthen vulnerability management processes and oversight to ensure timely remediation and appropriate risk management by

- a. Ensuring critically late vulnerabilities are escalated to the ISO as required by Board policy, with defined accountability for resolution or risk-acceptance decisions.
- b. Ensuring the ISO has the capability to monitor vulnerability remediation status across all divisions, track vulnerabilities that remain unresolved beyond remediation deadlines, and verify that POA&Ms or risk-acceptance decisions are documented for all vulnerabilities that cannot be mitigated by Board's established deadlines.
- c. Establishing processes to proactively identify and manage software approaching or reaching EOL.

Management Response:

We concur with the finding and recommendations. For Recommendation 4a, the Board will implement enhanced escalation processes to ensure critically late vulnerabilities are escalated to the Information Security Officer (ISO) as required by Board policy, with clearly defined accountability for resolution or risk-acceptance decisions. For Recommendation 4b, the Board will enhance the ISO's capability to monitor vulnerability remediation status across all divisions, track vulnerabilities that remain unresolved beyond remediation deadlines, and verify that plans of actions and milestones (POA&Ms) or risk-acceptance decisions are documented for vulnerabilities that cannot be mitigated within established deadlines. For Recommendation 4c, the Board will establish proactive processes to identify software approaching or reaching end-of-life (EOL) and to manage the associated risk.

Target date: Fourth quarter of 2027.

Recommendation 5:

We recommend that the chief information officer establish and implement formal, standardized processes for identifying and assessing organizational risk.

Management Response:

We concur with the finding and recommendation. The Board will establish and implement formal, standardized processes for identifying and assessing organizational cybersecurity risk. This will include developing comprehensive guidance for maintaining cybersecurity risk registers that accurately document risk assessments, evaluation decisions, responses, and monitoring activities.

Target date: Third quarter of 2027.

Finding 2: Outdated and Incomplete Policies and Standards Prevent Consistent Implementation and Limit Program Maturity**Recommendation 6:**

We recommend that the chief information officer update and develop the Board's information security policies, procedures, standards, and processes to reflect federal requirements and operational practices by

- a. Updating all information security policies to reflect operational practices.
- b. Developing comprehensive configuration documentation standards that establish specific baseline requirements for all system types, including COTS applications, internally developed applications, and infrastructure components.
- c. Developing an enterprise-wide ISCM strategy that aligns with federal requirements and organizational risk tolerance.

Management Response:

We concur with the finding and recommendations. For Recommendation 6a, the Board will update all information security policies, including the Board Information Security Program, Information System Inventory Standard, Incident Response Program, and Incident Response Manual, to reflect current operational practices and the Board's enterprise IT operating model. For Recommendation 6b, the Board will develop comprehensive configuration documentation standards that establish specific baseline requirements for all system types, including commercial off-the-shelf (COTS) applications, internally developed applications, and infrastructure components. These standards will define content requirements such as current software versions, configuration settings, periodic review frequencies, and update processes. For Recommendation 6c, the Board will develop an enterprise-wide information security continuous monitoring (ISCM) strategy that defines monitoring requirements across organizational tiers, establishes how risk tolerance determines minimum monitoring frequencies, and aligns with federal requirements.

Target date: Fourth quarter of 2027.

Finding 3: Misaligned Continuity Governance Could Limit Program Effectiveness

Recommendation 7:

Work with IINS to

- a. Develop and implement enterprise-wide policies that define the responsibilities and requirements for performing and maintaining BIAs and BPAs, including coordination mechanisms to ensure alignment between BIAs and technical contingency planning.
- b. Develop and implement policies for information system contingency plans consistent with federal requirements.

Management Response:

We concur with the finding and recommendation. The Board will work with the Intelligence, Insider Risk, and National Security Programs (IINS) to develop and implement enterprise-wide policies that define the responsibilities and requirements for performing and maintaining business impact analyses (BIAs) and business process analyses (BPAs). These policies will include coordination mechanisms between IINS and the Division of Information Technology to ensure alignment between business impact determinations and technical contingency planning capabilities, establish requirements for documentation maintenance and review frequencies, and define processes for maintaining current and consistent BIA and BPA information across the organization. For Recommendation 7b, the Board will develop and implement policies for information system contingency plans consistent with federal requirements, including requirements for system-specific recovery procedures, recovery priorities, and testing protocols.

Target date: Fourth quarter of 2027.

Recommendation 8:

We recommend that the chief financial officer

- a) Strengthen CSP contract management to ensure alignment with FedRAMP requirements and establish appropriate oversight by Updating the Board's standard language in CSP contracts to ensure that the language is consistent with FedRAMP incident reporting requirements.
- b) Performing a review of contracts executed after issuance of the revised incident reporting language to identify agreements with outdated requirements and, where appropriate, coordinate with the CIO to determine whether contract modifications or other correction actions are necessary.
- c) Ensuring that the CIO reviews revisions to standard cybersecurity clauses and communicates recommended changes and final concurrence.

Management Response:

We concur with the finding and recommendation. The CFO has reviewed and updated the language to align with FedRAMP requirements and will update the Board's standard language in CSP contracts accordingly. While a comprehensive review of existing contracts was completed to identify any contracts that may require modification to align with the revised language, it was determined by Board Legal that the Board is sufficiently covered given the terms and conditions issued with each Purchase Order. Under Section 15 of Purchase Order Terms and Conditions, the Contractor agrees to comply with the Federal Information Security Modernization Act of 2014 and all regulations thereunder.

The standard cybersecurity clauses were updated accordingly on September 9, 2026. Moving forward, the CFO will work with the CIO to annually review the standard cybersecurity clauses to communicate recommended changes and final concurrence.

Target date: November 30, 2026

Abbreviations

BISP	<i>Board Information Security Program</i>
BIA	business impact analysis
BPA	business process analysis
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	chief information officer
CFO	chief financial officer
COOP	continuity of operations
COTS	commercial off-the-shelf
CSP	cloud service provider
EOL	end-of-life
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
IG	inspector general
IINS	Intelligence, Insider Risk, and National Security Programs
ISCM	information security continuous monitoring
ISCP	information system contingency plan
ISO	information security officer
IT	information technology
MFA	multifactor authentication
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POA&M	plan of action and milestones



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

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