

Board of Governors of the Federal Reserve System

2022 Audit of the Board's Information Security Program



Office of Inspector General

Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau



Executive Summary, 2022-IT-B-013, September 30, 2022

2022 Audit of the Board’s Information Security Program

Finding

The Board of Governors of the Federal Reserve System’s information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. Since our review last year, we found that the Board has taken steps to strengthen its information security program. For instance, the Board has developed a strategy for the implementation of a zero trust architecture (ZTA), in accordance with Executive Order 14028, *Improving the Nation’s Cybersecurity*. In support of its ZTA strategy, the Board has launched an organizationwide multifactor authentication effort and engaged with an external consultant to perform a ZTA maturity assessment for the agency. Further, the Board has continued to implement the U.S. Department of Homeland Security’s Continuous Diagnostics and Mitigation program, which provides cybersecurity tools, integration services, and dashboards to participating agencies to help them improve their security posture.

We identified opportunities to strengthen the Board’s cybersecurity risk management processes. Specifically, we found that the Board could strengthen its cybersecurity risk register process by categorizing and prioritizing risks. We also found that the questionnaire the Board uses to assess the information security posture of potential vendors could be updated to include specific questions related to (1) the protection of information at rest and (2) software, firmware, and information integrity.

Finally, the Board has taken sufficient actions to close three of the nine recommendations from our prior Federal Information Security Modernization Act of 2014 (FISMA) audit reports that remained open at the start of this audit. The closed recommendations are related to risk management. We are leaving open six recommendations related to risk management, identity and access management, data protection and privacy, security training, and information security continuous monitoring. We will update the status of these recommendations in our fall 2022 semiannual report to Congress and continue to monitor the Board’s progress as part of future FISMA audits.

Recommendation

This report includes one new recommendation and one matter for management consideration designed to strengthen the Board’s information security program in the area of cybersecurity risk management. In its response to a draft of our report, the Board concurs with our recommendation. We will monitor the Board’s progress in addressing this recommendation as part of future FISMA audits.

Purpose

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

Background

FISMA requires each inspector general to conduct an annual independent evaluation of their agency’s information security program, practices, and controls for select systems. The Office of Management and Budget’s (OMB) fiscal year 2022 guidance for FISMA reporting 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 across several core areas.

These core areas align to requirements outlined in Executive Order 14028, *Improving the Nation’s Cybersecurity*, as well as recent OMB guidance on modernizing federal cybersecurity. The guidance notes that level 4 (*managed and measurable*) represents an effective level of security.



Recommendations, 2022-IT-B-013, September 30, 2022

2022 Audit of the Board's Information Security Program

Finding: The Board's Cybersecurity Risk Register Could Be Strengthened by Categorizing and Prioritizing Risks

Number	Recommendation	Responsible office
1	Ensure that risks are appropriately categorized and prioritized on the Board's cybersecurity risk register.	Division of Information Technology



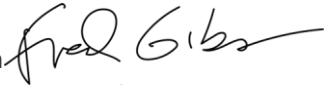
Office of Inspector General

Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

MEMORANDUM

DATE: September 30, 2022

TO: Distribution List

FROM: Fred W. Gibson 
Deputy Inspector General

SUBJECT: OIG Report 2022-IT-B-013: *2022 Audit of the Board's Information Security Program*

We have completed our report on the subject audit. We performed this audit pursuant to requirements in the Federal Information Security Modernization Act of 2014 (FISMA). Specifically, FISMA requires each agency inspector general to conduct an annual independent evaluation of the effectiveness of their agency's information security program and practices. As part of our work, we also reviewed security controls for select agency systems and performed data analytics, vulnerability scanning, and other technical tests; the detailed results of this testing will be transmitted in separate memorandums. In addition, we will use the results of this audit to respond to specific questions in the Office of Management and Budget's *FY22 Core IG Metrics Implementation Analysis and Guidelines*.

We provided you with a draft of our report for your review and comment. In your response, you state that you concur with our recommendation. We have included your response as appendix D to our report.

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

- cc: Andrew Krug
- Charles Young
- Annie Martin
- Craig Delaney
- Donna Butler
- Cheryl Patterson

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



Contents

Introduction	6
Objectives	6
Background	6
FISMA Maturity Model	7
Summary of the Board’s Information Security Program	9
Finding: The Board’s Cybersecurity Risk Register Could Be Strengthened by Categorizing and Prioritizing Risks	10
Recommendation	12
Management Response	12
OIG Comment	12
Matter for Management Consideration	13
The Board Can Strengthen Its Offeror Questionnaire	13
Appendix A: Scope and Methodology	14
Appendix B: Core Metrics	16
Appendix C: Status of Prior FISMA Recommendations	19
Appendix D: Management Response	22
Abbreviations	23



Introduction

Objectives

Our audit objectives, based on the requirements of the Federal Information Security Modernization Act of 2014 (FISMA), were to evaluate the effectiveness of the Board of Governors of the Federal Reserve System’s (1) security controls and techniques for select 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 select systems. To support independent evaluation requirements, the U.S. Department of Homeland Security (DHS), in coordination with the Office of Management and Budget (OMB), publishes FISMA reporting metrics for IGs to respond to on an annual basis.

OMB’s *FY22 Core IG Metrics Implementation Analysis and Guidelines* focuses on 20 key evaluation areas, also known as *core metrics*, that were chosen based on alignment with Executive Order 14028, *Improving the Nation’s Cybersecurity*, as well recent OMB guidance on modernizing federal cybersecurity. These core metrics are detailed in appendix B and cover areas such as

- zero trust architecture (ZTA)²
- multifactor authentication and encryption
- investigative and remediation capabilities related to cybersecurity incidents
- endpoint detection and response
- software supply chain security

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 According to Executive Order 14028, *ZTA* refers to a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries.

FISMA Maturity Model

OMB's *FY22 Core IG Metrics Implementation Analysis and Guidelines* notes that IGs are required to assess the effectiveness of their agencies' information security programs by assessing the core metrics against a maturity model spectrum.³ The five levels of the maturity model are

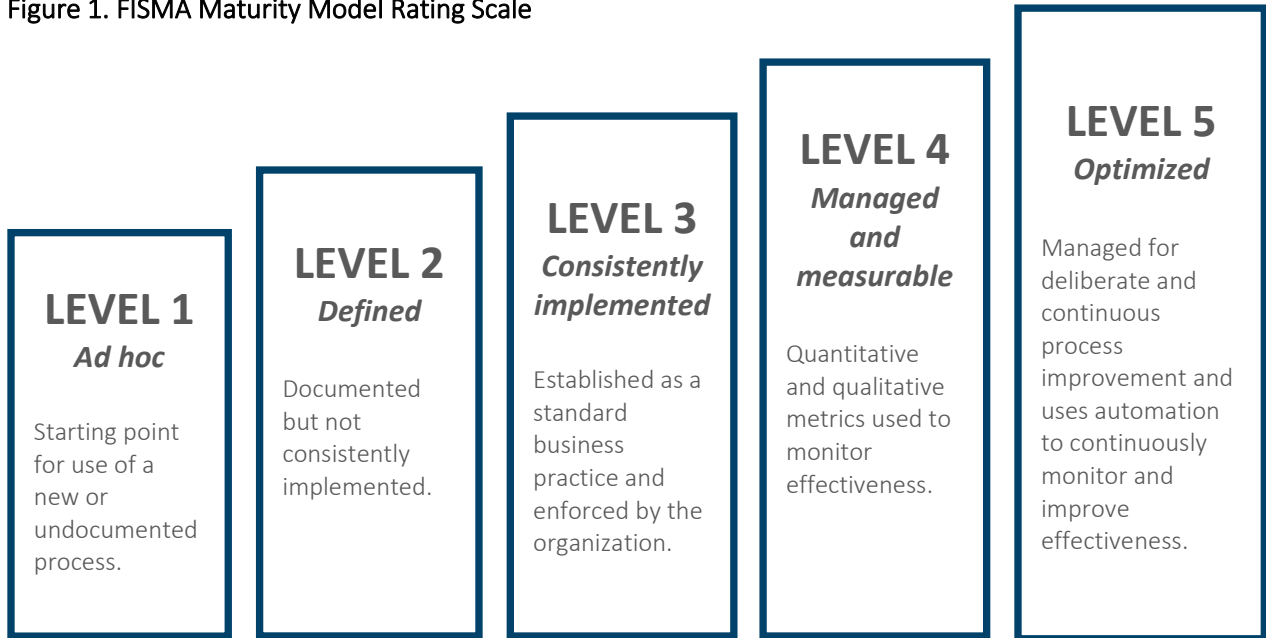
1. *ad hoc*
2. *defined*
3. *consistently implemented*
4. *managed and measurable*
5. *optimized*

The foundational levels (1–3) of the model are geared toward the development and implementation of policies and procedures, and the advanced levels (4–5) capture the extent to which agencies institutionalize those policies and procedures (figure 1). The maturity levels of each of the core metrics are to be used to determine the overall maturity of an organization's information security program. As noted in the *FY22 Core IG Metrics Implementation Analysis and Guidelines*, level 4 (*managed and measurable*) represents an effective level of security.⁴ Details on the scoring methodology for the maturity model are included in appendix A.

³ As noted in the *FY22 Core IG Metrics Implementation Analysis and Guidelines*, IGs should use the Cyberscope application to submit the results of their core metrics evaluation. As such, our detailed responses and assessment of the Board's progress in implementing the core metrics were provided to DHS in the Cyberscope application. Because of the sensitive nature of our responses, they are restricted and not included in this report.

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

Figure 1. FISMA Maturity Model Rating Scale



Source: OIG analysis of DHS's FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 1.1, May 12, 2021.



Summary of the Board's Information Security Program

The Board's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. Since our review last year, we found that the Board has taken several steps to strengthen its information security program. For instance, pursuant to OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, the Board has developed a strategy for the implementation of a ZTA.⁵ As part of this implementation, the Board established a formal identity, credential, and access management program; launched an organizationwide multifactor authentication effort; and engaged with an external consultant to perform a ZTA maturity assessment for the agency. OMB Memorandum M-22-09 sets September 2024 as a target by which agencies should fully implement their ZTA architectures, and the Board's strategy outlines a plan for the agency to transition all applications that are feasible to its new ZTA by that target.

Further, the Board has continued with its implementation of DHS's Continuous Diagnostics and Mitigation program, which provides cybersecurity tools, integration services, and dashboards to participating agencies to help them improve their respective security posture. For example, Board officials informed us that they have begun implementing Continuous Diagnostics and Mitigation tools for hardware and vulnerability management.

The agency has also taken actions to close three of the nine recommendations from our prior FISMA audits that remained open at the start of this audit (appendix C). In addition to the six open recommendations, we identified opportunities to mature the Board's information security program in the area of cybersecurity risk management. Specifically, we found that the Board could strengthen its cybersecurity risk register process by categorizing and prioritizing risks. Our report includes a recommendation in this area. We also found that the questionnaire the Board uses to assess the information security posture of potential vendors could be updated to include specific questions related to (1) protection of information at rest and (2) software, firmware, and information integrity. Our report includes a matter for management consideration in this area.

⁵ Office of Management and Budget, Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, January 26, 2022.



Finding: The Board's Cybersecurity Risk Register Could Be Strengthened by Categorizing and Prioritizing Risks

National Institute of Standards and Technology (NIST), Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* (NISTIR 8286) highlights the importance of, and the relationships between, cybersecurity risk management and enterprise risk management.⁶ NISTIR 8286 notes that one way to ensure that cybersecurity risk information is able to be aggregated, normalized, and prioritized at the enterprise level is through the use of a cybersecurity risk register.⁷ The Board's Division of Information Technology uses a cybersecurity risk register to capture risks from across the enterprise. Division of IT officials contact representatives from each Board division on a quarterly basis to gather information on new and existing cybersecurity risks and ensure that this information is documented in the Board's FISMA compliance tool.

We found that risks are not consistently categorized within the Board's cybersecurity risk register. The agency's cybersecurity risk register does contain information on *competency* and *domain*, which are based on the security functions from the NIST Cybersecurity Framework and FISMA reporting domains, respectively; however, these attributes are optional and only consistently captured for recommendations made in prior OIG reports. In addition, we noted that the Board's cybersecurity risk register does not have an attribute or sorting mechanism to prioritize risk response. For example, while risk level is assessed and documented within the risk register, the Board does not have a process to prioritize risks that are assigned the same risk level within the tool.

NISTIR 8286 includes a template that details suggested cybersecurity risk register elements, which we compared against the Board's cybersecurity risk register (table 1).

⁶ NISTIR 8286 defines *cybersecurity risk* as an effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality; integrity; or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the nation. NISTIR 8286 defines *enterprise risk management* as an effective agencywide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. National Institute of Standards and Technology, Internal Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, October 2020.

⁷ NISTIR 8286 defines a *risk register* as a repository of risk information, including the data understood about risks over time.

Table 1. Comparison of the Board’s Cybersecurity Risk Register Against NISTIR 8286

NISTIR 8286 register element	NISTIR 8286 element description	Board cybersecurity risk register
ID risk identifier	A sequential numeric identifier for referring to a risk in the risk register.	✓
Risk description	A brief explanation of the cybersecurity risk scenario (potentially) impacting the organization and enterprise.	✓
Current assessment–likelihood	An estimation of the probability, before any risk response, that this scenario will occur.	✓
Current assessment–impact	An analysis of the potential benefits or consequences that might result from this scenario if no additional response is provided.	✓
Current assessment–exposure rating	A calculation of the probability of risk exposure based on the likelihood estimate and determination of benefits or consequences of the risk (may also be called <i>level of risk</i>).	✓
Risk response type	The risk response for handling the identified risk (accept, transfer, mitigate, or avoid).	✓
Risk response cost	The estimated cost of applying the risk response.	✓
Risk response description	A brief description of the risk response.	✓
Risk owner	The designated party responsible and accountable for ensuring the risk is maintained in accordance with enterprise requirements.	✓
Status	A field for tracking the current condition of the risk and any next activities.	✓
Risk category	An organizing construct that enables multiple risk register entries to be consolidated (such as the control families from NIST Special Publication 800-53, <i>Security and Privacy Controls for Information Systems and Organizations</i>).	
Priority	A relative indicator of the criticality of this entry in the risk register, either expressed in ordinal value (1, 2, 3) or in reference to a given scale (<i>high, moderate, low</i>).	

Source: OIG analysis.

Board officials informed us that the agency is transitioning to a new governance, risk, and compliance tool, which will enable them to prioritize items in the cybersecurity risk register. In addition, the new tool contains a default attribute for risk categorization; however, the categorization of risk is not something the Board plans to add during its immediate transition to the new tool. As we have previously reported, the Board continues to take steps to implement an enterprise risk management program.⁸ We believe that consistently categorizing and prioritizing risks within the agency’s cybersecurity risk register could assist the Board in aggregating risks that affect similar security functions as well as allocating resources to priority areas.

Recommendation

We recommend that the chief information officer (CIO)

1. Ensure that risks are appropriately categorized and prioritized on the Board’s cybersecurity risk register.

Management Response

The CIO concurs with our recommendation and states that the agency intends to pursue corrective actions as a key priority. The CIO also notes that the agency will work with our office to confirm that the planned actions fully address the issues identified in our report.

OIG Comment

We believe that the actions described by the CIO are responsive to our recommendation. We will follow up on the steps outlined in the Board’s plan of action and milestones (POA&M) to ensure that the recommendation is fully addressed.

⁸ Office of Inspector General, *The Board’s Implementation of Enterprise Risk Management Continues to Evolve and Can Be Enhanced*, [OIG Report 2021-IT-B-011](#), September 15, 2021.



Matter for Management Consideration

We identified one matter for management consideration related to the Board’s Offeror Questionnaire, which is completed by agency vendors that process, store, or transmit Board data. Although we are not making a formal recommendation, we will continue to monitor the Board’s progress in this area.

The Board Can Strengthen Its Offeror Questionnaire

The Board’s *Vendor Risk Management Standard* establishes information security and privacy information handling requirements for the acquisition of third-party services that process, store, or transmit Board information. During the evaluation phase of the vendor solicitation process, the Board determines the vendor’s ability to meet the agency’s information security requirements, including a requirement for the vendor to complete an Offeror Questionnaire. The Offeror Questionnaire includes a list of questions that refer to select NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (SP 800-53, Rev. 5)⁹ controls for the software application provided by the vendor.

We noted that the Board’s Offeror Questionnaire does not include controls related to (1) the protection of information at rest or (2) software, firmware, and information integrity. Specifically, the Federal Risk and Authorization Management Program (FedRAMP) issued guidance on contractual language for contracts involving cloud computing solutions related to specific controls that may be required to govern agency user interaction.¹⁰ Examples of these FedRAMP controls include encryption standards, data jurisdiction, nonrepudiation, audit record retention, and multifactor authentication.

A Board official informed us that they are planning to revamp the agency’s Offeror Questionnaire next year as a part of the agency’s transition to the latest revision of SP 800-53, Rev. 5, which will introduce additional controls into the vendor’s evaluation process. As the Board continues to increase its use of cloud computing solutions to perform its mission and meet its information technology needs, we suggest that the agency consider the inclusion of these FedRAMP-specific controls within its Offeror Questionnaire to enable it to ensure that vendors can meet the Board’s information security requirements. Although we are not making a formal recommendation, we will monitor the agency’s progress in this area.

⁹ National Institute of Standards and Technology, Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, updated December 10, 2020.

¹⁰ Federal Risk and Authorization Management Program, *FedRAMP Control Specific Contract Clauses*, Version 3.0, December 8, 2017.



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 select information systems and (2) information security policies, procedures, and practices. To accomplish our objectives, we reviewed the effectiveness of the Board's information security program across the 20 core metrics outlined in OMB's *FY22 Core IG Metrics Implementation Analysis and Guidelines*. These core metrics cover nine security domains: *risk management, supply chain risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning*.

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

- used a risk-based approach and focused our testing activities on the 20 core metrics identified in OMB's *FY22 Core IG Metrics Implementation Analysis and Guidelines*
- analyzed security policies, procedures, and documentation
- interviewed Board management and staff
- performed vulnerability scans at the network, operating system, and database levels for select systems¹¹
- observed and tested specific security processes and controls at the program level as well as for three sampled Board systems¹²

The *FY22 Core IG Metrics Implementation Analysis and Guidelines* directs IGs to assess the effectiveness of information security programs on a maturity model spectrum. In prior years, to rate the maturity of the Board's information security program and functional areas, we used a scoring methodology outlined in the FISMA guidance and based on a simple majority by which the most frequent level (that is, the mode) across the metrics serves as the overall rating. However, the *FY22 Core IG Metrics Implementation Analysis and Guidelines* notes that an assessment of the 20 core metrics should provide sufficient data to determine the effectiveness of an agency's information security program. Further, the guidance also provides an IG with additional flexibility to use supplemental reports (including past evaluations in which results have varied little year over year) and any additional evidence of information security program effectiveness to provide context within this evaluation period.

We performed our fieldwork from March 2022 to August 2022. We conducted this 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

¹¹ We plan to transmit the detailed results of our vulnerability scans in separate, restricted memorandums because of the sensitive nature of the information.

¹² We plan to transmit the detailed results of our testing of these systems in separate, restricted memorandums because of the sensitive nature of the information.

and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.



Appendix B: Core Metrics

The table below shows the 20 core metrics for use in the fiscal year 2022 IG evaluation period. These metrics were selected from DHS's *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*¹³ for their applicability to critical efforts emanating from Executive Order 14028 and OMB Memorandum M-22-09.¹⁴

Table B-1. Core Metrics, by Security Domain

Metric title	Metric
Risk management	
System/interconnection inventory	To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems) and system interconnections?
Hardware inventory	To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including government-furnished equipment and bring-your-own-device mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?
Software/license inventory	To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?
Policies and procedures	To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?
Automated view of risk	To what extent does the organization utilize technology/automation to provide a centralized, enterprisewide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?

¹³ U.S. Department of Homeland Security, *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.1, May 12, 2021.

¹⁴ Because of the sensitive nature of the information, the details of our analysis of the *FY22 Core IG Metrics Implementation Analysis and Guidelines*, including the maturity ratings, were provided separately to applicable stakeholders.

Metric title	Metric
Supply chain risk management	
Requirements for external providers	To what extent does the organization ensure that the products, system components, systems, and services of external providers are consistent with the organization’s cybersecurity and supply chain requirements?
Configuration management	
Configuration settings	To what extent does the organization utilize settings/common secure configurations for its information systems?
Flaw remediation	To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities?
Identity and access management	
Authentication mechanisms (nonprivileged users)	To what extent has the organization implemented strong authentication mechanisms (a personal identity verification (PIV) or an identity assurance level (IAL) 3/authenticator assurance level (AAL) 3 credential) for nonprivileged users to access the organization’s facilities (organization-defined entry/exit points), networks, and systems, including for remote access?
Authentication mechanisms (privileged users)	To what extent has the organization implemented strong authentication mechanisms (a PIV or IAL 3/AAL 3 credential) for privileged users to access the organization’s facilities (organization-defined entry/exit points), networks, and systems, including for remote access?
Least privilege and separation of duties	To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed.
Data protection and privacy	
Privacy security controls	To what extent has the organization implemented the encryption of data at rest, in transit, limitation of transference of data by removable media, and sanitization of digital media prior to disposal or reuse to protect its personally identifiable information and other agency sensitive data, as appropriate, throughout the data life cycle?

Metric title	Metric
Security controls for exfiltration	To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses?
Security training	
Assessment of skills, knowledge, and abilities	To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of <i>identify, protect, detect, respond, and recover</i> ?
Information security continuous monitoring	
Information security continuous monitoring (ISCM) policies and strategy	To what extent does the organization utilize ISCM policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?
Ongoing system authorizations	How mature are the organization's processes for performing ongoing information system assessments; granting system authorizations, including developing and maintaining system security plans; and monitoring system security controls?
Incident response	
Incident detection and analysis	How mature are the organization's processes for incident detection and analysis?
Incident handling	How mature are the organization's processes for incident handling?
Contingency planning	
Business impact analysis	To what extent does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts?
Contingency testing	To what extent does the organization perform tests/exercises of its information system contingency planning processes?

Source: OMB's FY22 Core IG Metrics Implementation Analysis and Guidelines.



Appendix C: Status of Prior FISMA Recommendations

As part of our 2022 FISMA audit, we reviewed the actions taken by the Board to address the outstanding recommendations from prior FISMA audit reports. Below is a summary of the status of the nine recommendations that were open at the start of our 2022 FISMA audit and the related 20 core metrics (table C-1). Based on the corrective actions taken by the Board, we are closing three recommendations related to the *risk management* domain. The remaining six recommendations—which are related to the *risk management*, *identity and access management*, *data protection and privacy*, *security training*, and *information security continuous monitoring* domains—remain open. We will update the status of these recommendations in our fall 2022 semiannual report to Congress, and we will continue to monitor the Board’s progress in addressing our open recommendations as a part of our future FISMA audits.

Table C-1. Status of 2016–2021 FISMA Recommendations That Were Open as of the Start of Our Fieldwork, by Security Domain

Year	Recommendation	Core metric	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.	Risk management—policies and procedures	Open	Board officials informed us that they intend to accept the risk related to this recommendation but have not yet documented this acceptance.
2020	1 We recommend that the CIO ensure that the Board’s FISMA compliance tool is consistently factoring information types into the resulting system classification levels.	Risk management—policies and procedures	Closed	Board officials informed us that they have added steps to their annual security review process to ensure that information types are accurately selected within the agency’s FISMA compliance tool, which in turn ensures that systems are categorized appropriately. Our analysis of Board systems showed that information types were being selected consistently.

Year	Recommendation	Core metric	Status	Explanation
2021	1 We recommend that the CIO ensure the Board's POA&M policies and guidance, as appropriate, address requirements for all necessary POA&M attributes to be populated within the agency's FISMA compliance tool and documented consistently.	Risk management—policies and procedures	Closed	The Board has updated the agency's POA&M policy to require the necessary POA&M attributes. The Division of IT has also created a monitoring dashboard to identify POA&Ms that are missing the required fields and is working to follow up with system managers to address the missing fields, as necessary.
2021	2 We recommend that the CIO ensure system owners document the periodic review of the Board's system-level risk acceptances.	Risk management—policies and procedures	Closed	The Board has updated the agency's POA&M policy to require that risk acceptances are reviewed annually. These risk acceptances are required to be documented and approved in the system's security plan and risk assessment by the system owner.

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.	Identity and access management—least privilege and separation of duties	Open	The Board's continuous monitoring processes now include vulnerability scanning for applicable network devices. Further, the agency has developed a process to check the security of administrator credentials for network devices. However, our testing continues to identify opportunities to improve in this area.
------	---	---	------	--

Data protection and privacy

2019	5 We recommend that the CIO work with the Federal Reserve System to ensure that the data loss protection (DLP) replacement solution (a) functions consistently across the Board's technology platforms and (b) supports rulesets that limit the exfiltration weaknesses we identified, to the extent practicable.	Data protection and privacy—data exfiltration	Open	Board officials informed us that they continue to work with the Federal Reserve System to test the agency's replacement DLP solution. These same officials informed us that they are hoping to complete testing of the solution by the third quarter of 2022.
------	---	---	------	---

Year	Recommendation	Core metric	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 exfiltrations or access.	Data protection and privacy–data exfiltration	Open	The Board continues to make progress in this area, including developing draft documentation, coordinating with stakeholders across the agency, and working to automate the process. However, Board officials noted that they are still searching for an ideal solution to address the offboarding process and that efforts are ongoing.
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.	Security training–assessment of skills, knowledge, and abilities	Open	The agency’s risk register notes that the Board plans to map the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework security roles identified in the FISMA CIO metrics to the Board’s positions. This will allow the agency to customize the skills, knowledge, and abilities that are necessary to meet the Board’s needs. This work is ongoing.
Information security continuous monitoring				
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.	ISCM–ISCM policies and strategy	Open	The Board continues to make progress in the development and implementation of an ISCM strategy. However, agency officials informed us that the strategy is being revised to ensure it is fully comprehensive with respect to the Board’s needs and provides the necessary flexibility for the agency’s constantly changing technology.

Source: OIG analysis.

Appendix D: Management Response



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

DIVISION OF
INFORMATION TECHNOLOGY

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

Dear Mark,

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG) report on the Board of Governors of the Federal Reserve System's (the Board) compliance with the Federal Information Security Management Act of 2014 (FISMA) for 2022. The report evaluates the Board's information security program in accordance with the fiscal year 2022 Core IG Metrics¹ which were chosen based on alignment with Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," as well as recent Office of Management and Budget (OMB) guidance to agencies in furtherance of the modernization of federal cybersecurity.

I am pleased your report found that the Board's information security program continues to operate effectively and recognized the agency's work in making progress towards implementing federal cybersecurity mandates including those pertaining to the establishment of a zero-trust architecture. We remain committed to improving the Board's security posture, including with respect to your report's recommendations, with which we concur.

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

Sincerely,

SHARON
MOWRY

Digitally signed by SHARON
MOWRY
Date: 2022.09.23 14:22:06 -0400

Sharon Mowry
Chief Information Officer (CIO)

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

¹ [FY 2022 Core IG FISMA Metrics Evaluation Guide \(cisa.gov\)](https://www.cisa.gov/sites/default/files/publications/FY2022%20Core%20IG%20FISMA%20Metrics%20Evaluation%20Guide.pdf) -
[https://www.cisa.gov/sites/default/files/publications/FY2022 Core IG FISMA Metrics Evaluation Guide %2805-12-22%29.pdf](https://www.cisa.gov/sites/default/files/publications/FY2022%20Core%20IG%20FISMA%20Metrics%20Evaluation%20Guide%202805-12-22%29.pdf)



Abbreviations

AAL	authenticator assurance level
CIO	chief information officer
DHS	U.S. Department of Homeland Security
DLP	data loss protection
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
IAL	identity assurance level
IG	inspector general
ISCM	information security continuous monitoring
NIST	National Institute of Standards and Technology
NISTIR 8286	National Institute of Standards and Technology, Interagency Report 8286, <i>Integrating Cybersecurity and Enterprise Risk Management (ERM)</i>
OMB	Office of Management and Budget
PIV	personal identity verification
POA&M	plan of action and milestones
SP 800-53, Rev. 5	Special Publication 800-53, Revision 5, <i>Security and Privacy Controls for Information Systems and Organizations</i>
ZTA	zero trust architecture

Report Contributors

Khalid Hasan, Senior OIG Manager for Information Technology
Joshua Dieckert, OIG Manager, Information Technology Audits
Paul Vaclavik, OIG Manager, Information Technology Audits
Ken Dyke, Senior IT Auditor
Chelsea Nguyen, Senior IT Auditor
Nilesh Patel, Senior IT Auditor
Justin Byun, IT Auditor
Aaliyah Clark, IT Auditor
Trang Do, IT Auditor
Melissa Fortson, IT Auditor
Deyanara Gonzalez, IT Auditor
Nick Stefaniak, Forensic Auditor
Eric Shapiro, Auditor
Alexander Karst, Senior Information Technology Management Specialist
Fay Tang, Senior Information Technology Management Specialist
Fred Gibson, Deputy Inspector General

Contact Information

General

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

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

Media and Congressional

OIG.Media@frb.gov



Hotline

Report fraud, waste, and abuse.

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, [web form](#), phone, or fax.

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

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