Audit Report
2021-IT-B-014
October 29, 2021

Board of Governors of the Federal Reserve System

2021 Audit of the Board's Information Security Program

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

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

Executive Summary, 2021-IT-B-014, October 29, 2021

2021 Audit of the Board's Information Security Program

Findings

The Board of Governors of the Federal Reserve System's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. Since our review last year, we found that the Board has taken several steps to strengthen its information security program. For instance, the Board has matured its software asset management processes and has developed a catalog of software installed on Board devices.

The Board has opportunities to mature its information security program in Federal Information Security Modernization Act of 2014 (FISMA) domains across all five National Institute of Standards and Technology Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective. For example, within the *identify* function area, we noted opportunities to strengthen the Board's cybersecurity risk management processes. Specifically, we noted that key information, such as finding severity level and remediation start and end dates, was not being captured for the majority of weaknesses identified within the Board's system-level plans of action and milestones. Further, we found that the majority of the agency's documented system-level risk acceptances did not include an expiration date indicating when the Board's risk decision should be reassessed. We also identified the need for improvements in the implementation of the Board's software and license asset management processes for one of the agency's divisions. Similar to our previous FISMA audits, a consistent theme we noted is that the decentralization of information technology services results in an incomplete view of the risks affecting the Board's security posture.

Finally, the Board has taken sufficient actions to close 8 of the 15 recommendations from our prior FISMA audit reports that remained open at the start of this audit. The closed recommendations relate to risk management, identity and access management, and information security continuous monitoring. We are leaving open 7 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 spring 2022 semiannual report to Congress and continue to monitor the Board's progress as part of future FISMA audits.

Recommendations

This report includes two new recommendations 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 recommendations and notes that actions are underway to strengthen the agency's information security program. We will continue to monitor the Board's progress in addressing these recommendations as part of future FISMA audits.

Purpose

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Board. Our specific audit objectives, based on the legislation's requirements, were to evaluate the effectiveness of the Board's (1) security controls and techniques for 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 U.S. Department of Homeland Security's fiscal year 2021 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 areas. The guidance notes that level 4 (*managed and measurable*) represents an effective level of security.

Recommendations, 2021-IT-B-014, October 29, 2021

2021 Audit of the Board's Information Security Program

Number	Recommendation	Responsible office
1	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.	Division of Information Technology
2	Ensure system owners document the periodic review of the Board's system-level risk acceptances.	Division of Information Technology

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

MEMORANDUM

DATE: October 29, 2021

TO: Distribution List

FROM: Peter Sheridan
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2021-IT-B-014: *2021 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 U.S. Department of Homeland Security's *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

We provided you with a draft of our report for your review and comment. In your response, you concur with our recommendations and state that plans of action and milestones will be provided to address our recommendations. We have included your response as appendix C to our report.

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

cc: Raymond Romero
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
Nicole Bennett, Senior Associate Director, Division of Research and Statistics
Binoy Agarwal, Chief, Automation and Research Computing, Division of Research and Statistics

Contents

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) publishes FISMA reporting metrics for IGs to respond to on an annual basis. The *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* directs IGs to evaluate the effectiveness of agency information security programs across a variety of attributes grouped into nine security domains.[2] These domains align with the five security functions defined by the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (table 1).[3]

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

[2] 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.

[3] The NIST Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018.

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

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

Source: U.S. Department of Homeland Security, *FY 2021 IG FISMA Reporting Metrics*.

As noted in DHS's *FY 2021 IG FISMA Reporting Metrics*, one of the goals of the annual FISMA evaluation is to assess agencies' progress toward achieving outcomes that strengthen federal cybersecurity, including implementation of the administration's priorities and best practices. One such area is increasing the maturity of the federal government's supply chain risk management (SCRM) practices. As such, DHS's *FY 2021 IG FISMA Reporting Metrics* includes a new domain on SCRM within the *identify* function, focusing on the maturity of agency SCRM strategies, plans, policies, and processes.[4]

In addition, DHS's *FY 2021 IG Reporting Metrics* introduces a new pilot concept of weighting specific metrics for assessment and scoring, with the goal of driving continued improvements in cybersecurity maturity. Additional details on these priority metrics, as well as the Board's maturity in these areas, are provided in a later section of this report.

FISMA Maturity Model

FISMA requires that IGs assess the effectiveness of information security controls that support the operations and assets of their respective agency. To that end, the Council of the Inspectors General on Integrity and Efficiency, in coordination with the Office of Management and Budget (OMB), DHS, and other key stakeholders, developed a maturity model intended to better address and report on the

[4] This new domain on SCRM references criteria in National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5, updated December 10, 2020. As noted in the *FY 2021 IG FISMA Reporting Metrics*, to provide agencies with sufficient time to implement requirements from Special Publication 800-53, Revision 5, these new metrics are not being considered for the purposes of the *identify* function maturity rating in 2021.

effectiveness of an agency's information security program. The purpose of the maturity model is (1) to summarize the status of agencies' information security programs and their maturity on a five-level scale; (2) to provide transparency to agency chief information officers (CIOs), top management officials, and other interested readers of IG FISMA reports regarding what has been accomplished and what still needs to be implemented to improve the information security program; and (3) to help ensure that annual FISMA reviews are consistent across IGs.

The five levels of the IG FISMA 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 security domains will dictate the overall maturity of an organization's information security program. As noted in DHS's *FY 2021 IG FISMA Reporting Metrics*, level 4 (*managed and measurable*) represents an effective level of security.[5] Details on the scoring methodology for the maturity model, including the proposed weighted average approach for priority metrics, are included in appendix A.

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

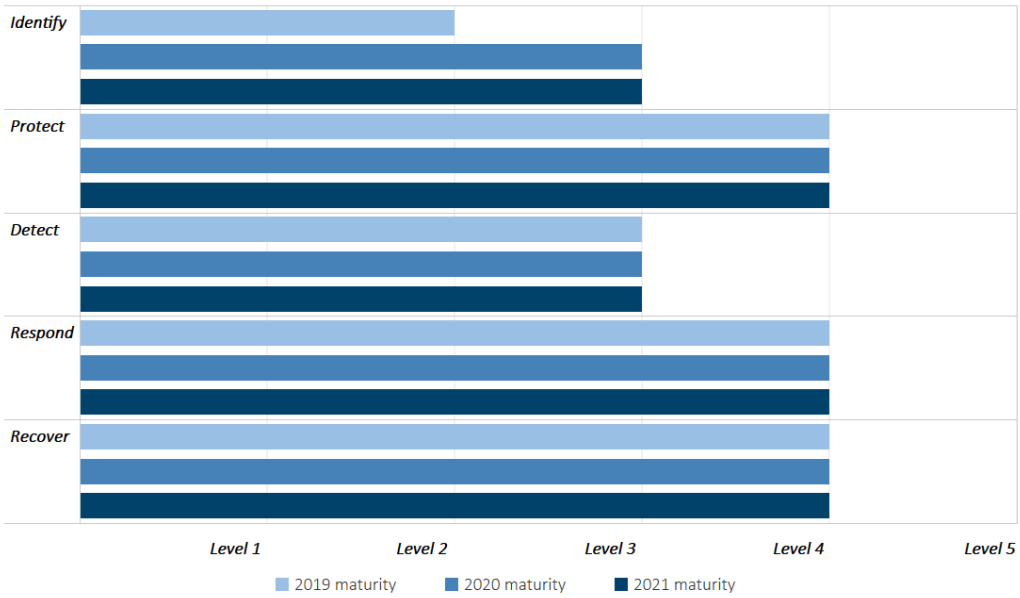
Figure 1. FISMA Maturity Model Rating Scale

Source: OIG analysis of DHS's *FY 2021 IG FISMA Reporting Metrics*.

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

The Board's overall information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity (figure 2).[6] Although the Board has strengthened its program since our 2020 FISMA audit report, the agency has opportunities to further mature its processes across specific FISMA domains in all five NIST Cybersecurity Framework security functions: *identify*, *protect*, *detect*, *respond*, and *recover*.

Figure 2. Maturity of the Board's Information Security Program, by Security Function, 2019–2021



Source: OIG analysis.

For the *identify* function area, which continues to operate at a level-3 (*consistently implemented*) maturity, we identified three opportunities to mature the Board's cybersecurity risk management processes. First, we found that key information, such as finding severity level and remediation start and end dates, was not being captured for the majority of weaknesses identified within the Board's system-level plans of action and milestones (POA&Ms). Second, we found that the majority of the agency's documented system-level risk acceptances did not include an expiration date for when the Board's risk decision should be reassessed. Lastly, we identified improvements in the implementation of the Board's software and license asset management processes for one of the agency's divisions.

[6] Appendix A explains the scoring methodology outlined in DHS's *FY 2021 IG FISMA Reporting Metrics* that we used to determine the maturity of the Board's information security program.

For the *protect* function area, which continues to operate effectively at a level-4 (*managed and measurable*) maturity, our recommendations from previous FISMA audit reports related to strengthening data loss protection controls remain open. In the *detect* function area, the Board continues to take actions to develop and implement an information security continuous monitoring strategy that incorporates updated guidance from NIST. Our previous FISMA audit report from 2017 includes a recommendation that remains open in this area. We found that the *respond* and *recover* functions are operating effectively and we have no open recommendations in these areas.

Similar to our previous FISMA audit reports, a consistent theme we noted is that the decentralization of information technology (IT) services results in an incomplete view of the risks affecting the Board's security posture. We continue to believe that the Board's ongoing efforts to implement DHS's Continuous Diagnostics and Mitigation (CDM) program will help mature the agency's information security program across multiple security functions and address issues that result from the decentralization of IT services.[7]

Identify

The objective of the *identify* function in NIST's Cybersecurity Framework is to develop an organizational understanding of how to manage cybersecurity risks to agency systems, assets, data, and capabilities. The Cybersecurity Framework highlights risk management processes that organizations can implement to inform and prioritize decisions. Examples of the areas in this security function, as outlined in DHS's *FY 2021 IG FISMA Reporting Metrics*, that we assessed include the Board's cybersecurity risk management processes; the development and implementation of an enterprise architecture; asset management, including mobile device management; the use of POA&Ms to manage the remediation of security weaknesses; and the agency's understanding and control of the cybersecurity supply chain risks of the products and services that it uses.

Risk Management

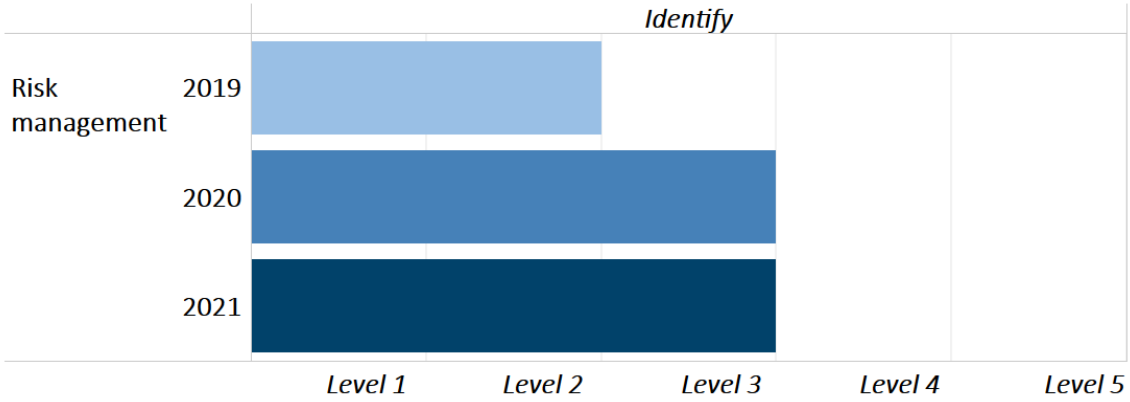
FISMA requires federal agencies to provide information security protections commensurate with their risk environment and to ensure that information security management processes are integrated with strategic, operational, and budgetary planning processes. *Risk management* refers to the program and supporting processes used to manage risk to organizational operations, assets, and individuals and is a holistic activity that affects every aspect of the organization. *Cybersecurity risk management* refers to the full range of activities undertaken to protect IT and data from unauthorized access and other cyberthreats; maintain awareness of cyberthreats; detect anomalies and incidents adversely affecting IT and data; and mitigate the impact of, respond to, and recover from incidents. Examples of cybersecurity risk management activities include hardware and software asset management, the use of a cybersecurity risk register to document and manage risks, and the use of POA&Ms to mitigate and monitor system-level security weaknesses.

[7] DHS's CDM program provides cybersecurity tools, integration services, and dashboards to participating agencies to help them improve their respective security posture.

Current Agency Maturity

As in 2020, we found that the Board's risk management program continues to operate at a level-3 (*consistently implemented*) maturity (figure 3).

Figure 3. Maturity of the Risk Management Domain, 2019–2021



Source: OIG analysis.

This year, we found that the Board has taken steps to strengthen its risk management program—most notably by expanding the agency's Software Review Board (SRB)[8] and developing and implementing additional software asset management processes. Specifically, we noted that the Division of Information Technology (Division of IT)

- issued the *Software Management Policy*, *SRB Approved Software Catalog Procedures*, and *SRB Software Review Procedures*, which include requirements for software license management and reviews
- worked with other agency divisions to develop and implement an enterprisewide catalog of software installed on Board devices, including approved desktop software, managed mobile applications, and server software[9]

In addition, we have made several recommendations in prior FISMA audit reports related to the agency's insider threat program, enterprise risk management (ERM), enterprise architecture, software asset management, POA&Ms, and system categorization processes. We found that actions have been taken to close of five of the seven risk recommendations in these areas. The status of prior FISMA recommendations made in these areas is detailed in appendix B.

Opportunities for Improvement

While the Board's risk management program is operating at a level-3 (*consistently implemented*) maturity, we identified opportunities for improvement related to the Board's POA&M and risk acceptance

[8] The SRB is a governance body, sponsored by the Board's CIO, that is responsible for software reviews and the maintenance of an enterprise-approved software catalog for desktop, mobile, and server software.

[9] We identified opportunities for improvement regarding one agency division's software review and inventory processes to ensure the division's processes are consistent with the agency's SRB.

processes, as well as software and license inventory management for one of the agency's divisions. Specifically, we found the following:

- The Board's system-level POA&Ms are not documenting all required components that contain information related to the identified vulnerabilities and associated remediation activities.
- The Board's system-level risk acceptance expiration dates are not consistently documented or updated.
- One agency division does not have a software and license inventory or review process that is consistent with the agency's software catalog and SRB. We plan to make a recommendation to this division in a separate, restricted memorandum.

System-Level POA&Ms

With regard to the agency's POA&M process,[10] we found that the majority of weaknesses listed on the Board's system-level POA&Ms were missing one or more required fields, such as finding severity level, remediation priority, activities completed to date, and remediation start and end date. The *Board POA&M Standard* requires that the suggested original remediation completion date, the revised completion date, the date the POA&M item is closed, and the activities completed to date be populated within the agency's FISMA compliance tool. Further, Board officials informed us that remediation start date, remediation priority, and finding severity level are expected to be completed as well.

We identified two key causes for this issue:

- The *Board POA&M Standard* does not require system owners to populate the remediation start date, remediation priority, or the finding severity level in the agency's FISMA compliance tool.
- Division of IT officials informed us that oversight of the Board's POA&M process through the agency's automated dashboard is limited.

We believe that the inclusion of these required POA&M components will allow the agency to prioritize its most critical risks and more accurately estimate scheduled POA&M completion.

System-Level Accepted Risks

In addition, we identified improvements needed related to the Board's monitoring of system-level risks that have been accepted. Specifically, we found that the majority of the agency's documented risk acceptances did not include an expiration date indicating when the Board's risk decision should be reassessed. In addition, for the risk acceptances that did include an expiration date, we found that many had been expired for more than a year.

[10] NIST Special Publication 800-53, Revision 4, defines a *POA&M* as a document that identifies tasks that need to be accomplished. A POA&M details resources required to accomplish the elements of the plan, milestones for meeting the tasks, and the scheduled completion dates for the milestones. National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 4, updated January 22, 2015.

NIST Special Publication 800-39, *Managing Information System Risk: Organization, Mission, and Information System View*,[11] notes that the evaluation of residual risk should be determined based on the organization's risk tolerance and can change over time.[12] Further, NIST Special Publication 800-30, *Guide for Conducting Risk Assessments*, states that because organizational mission, business functions, and risk environments change, the validity and usefulness of any risk assessment is bounded in time.[13] In the context of such change, existing risk controls and decisions may need to be reassessed for effectiveness.

We identified two key causes for this issue:

- The Board's *Risk Management Program and Risk Assessment Standard* requires system owners to document a justification for risks that are accepted, and the *Board POA&M Standard* requires system owners to review accepted risks only when there is a major change to the system.[14] However, the agency's policies do not provide guidance regarding the periodic review of risk acceptances.
- Division of IT officials informed us that the current build of the agency's FISMA compliance tool does not include a technical control to ensure that an expiration date is assigned to risk acceptances; however, there have been some considerations as to whether this field should be enforced.

Agency officials informed us that risk acceptances are expected to be reviewed annually; however, the risk acceptance expiration date is not currently part of the annual review. We believe that by ensuring that risk acceptances remain valid given a changing threat environment, the Board will have greater assurance that residual risks remain acceptable.

Recommendations

We recommend that the CIO

1. 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.
2. Ensure system owners document the periodic review of the Board's system-level risk acceptances.

[11] National Institute of Standards and Technology, *Managing Information System Risk: Organization, Mission, and Information System View*, Special Publication 800-39, March 2011.

[12] *Residual risk* refers to the risk that remains after risk responses, such as risk acceptances, have been documented and performed.

[13] National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, Special Publication 800-30, September 2012.

[14] The Board's *Change Control Procedures for Applications* states that a *major change* is the initial release of an application or a significant change to an application and/or its supporting data, including introducing a new security model, adopting a new technology, redesigning a feature that is used by a large number of users, or introducing a new feature that is critical to the business process.

Management Response

The CIO concurs with our recommendations and notes that progress has already been made to address our recommendations. The CIO also notes that POA&Ms will be established to detail the steps the Board will take to address our recommendations.

OIG Comment

We believe that the actions described by the CIO are responsive to our recommendations. We plan to follow up on the steps outlined in the Board's POA&Ms to ensure that the recommendations are fully addressed.

Supply Chain Risk Management

FISMA, as amended by the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act,[15] requires agencies to develop an overall risk management strategy, implementation plan, and policies and processes to govern SCRM activities.[16] The importance of SCRM is also highlighted in Executive Order 14028, *Improving the Nation's Cybersecurity*, which states that the federal government must take action to rapidly improve the security and integrity of the software supply chain.[17] In support of this goal, Executive Order 14028 tasks NIST, OMB, and other federal agencies to issue guidance on various elements of SCRM, such as secure software development, use of encryption, and maintenance of accurate and up-to-date information on the origin of software code or components.[18]

As noted earlier, SCRM is a new domain included in DHS's *FY 2021 IG FISMA Reporting Metrics.* This new domain focuses on the maturity of an agency's SCRM strategies, plans, policies, and processes and references criteria in NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (SP 800-53, Rev. 5).[19] As noted in the *FY 2021 IG FISMA Reporting Metrics*, to provide agencies with sufficient time to implement requirements from NIST SP 800-53, Rev. 5, these new metrics are not being considered for the purposes of the *identify* function maturity rating in 2021. As such, while we are not providing an overall maturity rating this year for the Board's SCRM program, we highlight the steps the agency has taken in this area and additional improvements we believe are needed. We will continue to monitor and report on the maturity of the Board's SCRM program and processes as part of our future FISMA audits.

[15] Strengthening and Enhancing Cyber-capabilities by Utilizing risk Exposure Technology Act of 2018, Pub. L. No. 115-290, 132 Stat. 5173 (2018) (codified at 41 U.S.C. §§ 1321–4713).

[16] National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, Revision 2, December 2018, defines *SCRM* as the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology product and service supply chains.

[17] Exec. Order 14028 (May 12, 2021).

[18] This guidance was not finalized at the time of our fieldwork.

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

Current Agency Maturity

The Board's information security program and supporting policies, procedures, and processes incorporate multiples areas of SCRM. Specifically, we noted the following:

- The Board's *Vendor Risk Management Standard* establishes a risk management process for vendors that will process, store, maintain, or transmit agency information. The standard outlines risk management related roles and responsibilities for information security, privacy, procurement, and system officials. In addition, the standard describes the activities the Board performs at the presolicitation, vendor evaluation, and postaward phases to manage risks to the agency's information assets. Further, we noted that the Board maintains an inventory of the types of information maintained by vendors as part of contractual agreements.
- The Board has developed standard information security contract clauses that are to be included in all contracts with vendors that will process, store, or maintain Board data. These clauses cover requirements for vendor risk management and compliance with the agency's information security program and policies.
- The Board has developed an evaluation process for commercial off-the-shelf technology products and services. This process includes steps to determine product or service functionality; system interoperability; alignment with enterprise architecture; business need fit; and compliance with legal requirements, including FISMA.

Opportunities for Improvement

As the Board continues to implement the new requirements found in NIST SP 800-53, Rev. 5, we identified several opportunities for the Board to mature its SCRM program. Specifically, we noted that the Board has not yet

- developed an organizationwide SCRM strategy based on NIST SP 800-53, Rev. 5, that covers areas such as supply chain risk appetite and tolerance and acceptable supply chain risk mitigation strategies and controls[20]
- tailored the SCRM-related system security control requirements from NIST SP 800-53, Rev. 5, to its operational environment

Board officials have informed us that they are waiting on further federal guidance to be finalized, as noted in Executive Order 14028, before developing a formal organizationwide SCRM strategy. In addition, the agency is in the process of updating its security controls baseline to account for the requirements of NIST SP 800-53, Rev. 5. We will continue to monitor the Board's activities in this area as part of our future FISMA audits.

[20] We realize that an organization-level SCRM strategy that addresses risk appetite and tolerance will need to be integrated with the agency's ERM strategy. As noted in our recent report, the Board has not yet developed an overall strategy for ERM or defined a risk appetite statement and associated tolerance levels. See Office of Inspector General, *The Board's Enterprise Risk Management Program Continues to Evolve and Can Be Enhanced*, OIG Report 2021-IT-B-011, September 15, 2021.

Protect

The objective of the *protect* function in NIST's Cybersecurity Framework is to develop and implement safeguards to secure information systems. This function supports the ability to limit or contain the effect of a cybersecurity event through applicable configuration management, identity and access management, data protection and privacy, and security training processes. The associated domains and components that IGs are required to assess within the *protect* function are highlighted in table 2 below.

Table 2. *Protect* Function Security Domains and Selected Components

Security domains	Examples of components assessed by IGs
Configuration management	Configuration management plans, configuration settings, flaw remediation, and change control
Identity and access management	Identity, credential, and access management strategy; access agreements; least privilege; and separation of duties
Data protection and privacy	Security controls for exfiltration, data breach response plan, and privacy security controls
Security training	Assessment of skills, knowledge, and abilities; security awareness; and specialized security training

Source: U.S. Department of Homeland Security, *FY 2021 IG FISMA Reporting Metrics*.

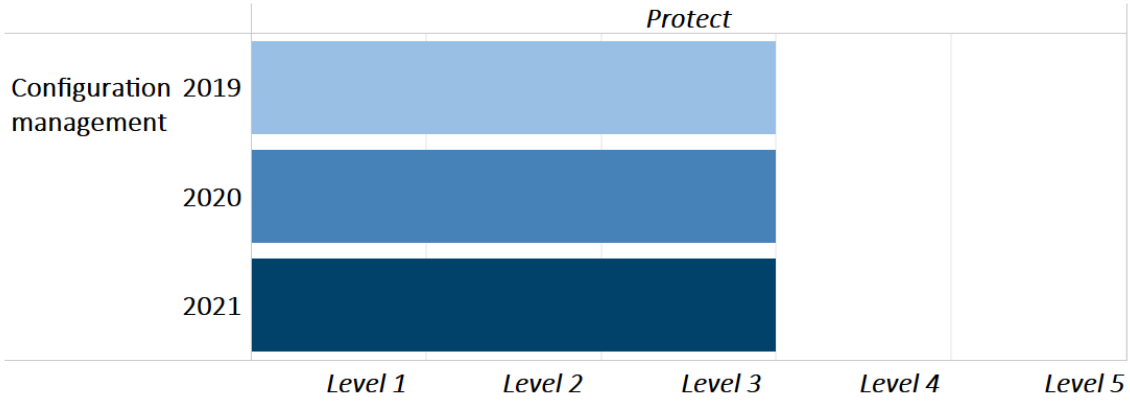
Configuration Management

FISMA requires agencies to develop and implement an information security program that includes policies and procedures that ensure compliance with minimally acceptable system configuration requirements. *Configuration management* refers to a collection of activities focused on establishing and maintaining the integrity of products and information systems through the control of processes for initializing, changing, and monitoring their configurations.

Current Agency Maturity

As in 2020, we found that the Board's configuration management program is operating at a level-3 (*consistently implemented*) maturity (figure 4), with the agency performing some activities indicative of a higher maturity level.

Figure 4. Maturity of the Configuration Management Domain, 2019–2021



Source: OIG analysis.

This year, we found that the Board has continued to strengthen its configuration management processes related to the areas of flaw remediation and change control. Specifically, we noted that the Board has

- implemented a new web application–level vulnerability scanning tool
- increased the coverage of its operating system–level vulnerability scans
- implemented a new change-control board to oversee critical infrastructure changes

Opportunities for Improvement

We identified several opportunities for improvement related to the Board's configuration management processes.[21] Specifically, we noted the following:

- While the Board has various secure configuration guides for its technologies, the agency has not developed such a guide for one of its external collaboration tools. NIST defines a *secure configuration guide* as a series of instructions or procedures for configuring an IT product to a particular operational environment, verifying that the product has been configured properly, and/or identifying unauthorized changes to the product.
- The Trusted Internet Connection (TIC) initiative was initiated in 2007 to consolidate network connections and enhance visibility and security measures throughout the federal network. DHS's TIC 3.0 was updated to focus on strategy, architecture, and visibility, recognizing the need to account for multiple and diverse architectures rather than a single perimeter approach. While the Board has implemented TIC 2.0, which focuses on funneling all incoming and outgoing data through a TIC access point, the agency is researching steps to implement DHS's TIC 3.0 use cases.[22]

[21] We also identified improvements in change control processes for one Board division. The detailed results will be transmitted in a separate, restricted memorandum.

[22] According to DHS, agencies have the option to maintain the TIC 2.0 implementation while adopting TIC 3.0 capabilities. However, agencies are encouraged to leverage the flexibilities outlined in the modernized TIC 3.0 guidance to support the implementation of modern security practices like zero trust architecture.

While we are not issuing recommendations in these areas at this time, we will continue to monitor the Board's configuration management processes as part of future FISMA audits.

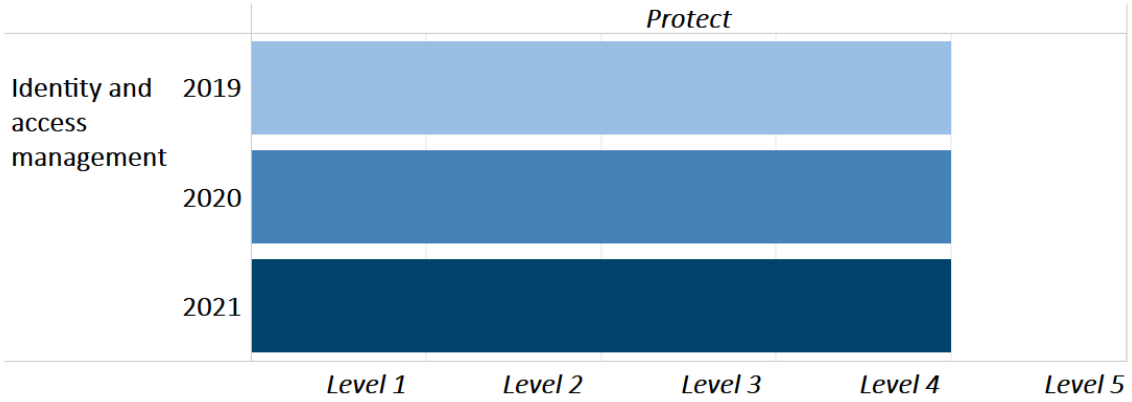
Identity and Access Management

Identity and access management includes implementing a set of capabilities to ensure that users authenticate to IT resources and have access to only those resources that are required for their job function, a concept referred to as *need to know*. Supporting activities include onboarding and personnel screening, issuing and maintaining user credentials, and managing logical and physical access privileges, which are collectively referred to as *identity, credential, and access management* (ICAM).

Current Agency Maturity

As in 2020, we found that the Board's ICAM program continues to operate effectively at a level-4 (*managed and measurable*) maturity (figure 5).

Figure 5. Maturity of the Identity and Access Management Domain, 2019–2021



Source: OIG analysis.

This year, we found that the Board has continued to strengthen its ICAM processes in the areas of remote access as well as the agency's ICAM strategy. Specifically, we noted the following:

- The Board has begun to use a recredentialing tool that allows the agency to update personal identity verification (PIV) certificates remotely.
- The Board has developed an ICAM strategy that includes guidelines regarding assurance levels and architectural designs to federate authentication, authorization, and users' attribute information across networked systems using digital identities and certificates. Agency officials informed us that they have obtained funding for a dedicated ICAM team to implement the strategy.

In addition, we have three recommendations from prior FISMA audit reports related to the Board's ICAM strategy as well as the agency's privileged user access controls and associated continuous monitoring for select network devices. We found that actions have been taken to close two of the three

recommendations. The status of prior FISMA recommendations made in these areas is detailed in appendix B.

Opportunities for Improvement

As we noted above, the Board has recently developed an ICAM strategy and has obtained funding for a dedicated ICAM team to implement the strategy. This ICAM strategy highlights the agency's proposed future state for the Board's identity management, credentials, logical access, and access validation processes, including the use of PIV-derived credentials for mobile devices, the implementation of a permissions-management platform, and a more centralized and automated access validation process. We will continue to monitor the Board's progress in implementing its ICAM strategy as well as the maturity of the agency's ICAM program as part of future FISMA audits.

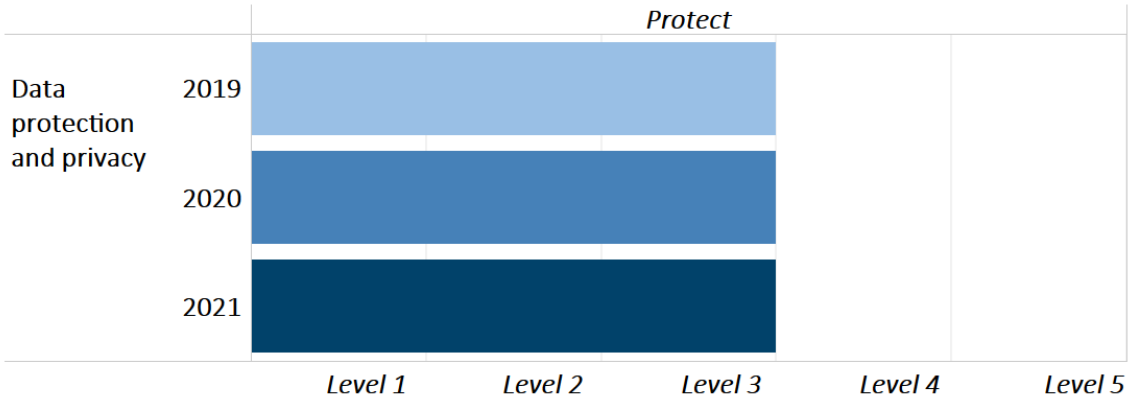
Data Protection and Privacy

Data protection and privacy refers to a collection of activities focused on preserving authorized restrictions on information access and protecting personal privacy and proprietary information. Effectively managing the risk to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their personally identifiable information (PII) increasingly depends on the safeguards employed for the information systems that process, store, and transmit the information. As such, federal guidance requires covered federal agencies to develop, implement, and maintain agencywide privacy programs that, where PII is involved, play a key role in information security and implementing the NIST Risk Management Framework.[23]

Current Agency Maturity

As in 2020, we found that the Board's data protection and privacy program is operating at a level-3 (*consistently implemented*) maturity (figure 6).

Figure 6. Maturity of the Data Protection and Privacy Domain, 2019–2021



Source: OIG analysis.

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

This year, we noted that the Board strengthened its data protection and privacy processes in the areas of data exfiltration and privacy training. Specifically, the Board

- conducted a tabletop data exfiltration exercise
- implemented a privacy awareness training for all employees and developed a role-based privacy training for individuals with significant privacy-related responsibilities

In addition, we have two recommendations from our prior FISMA audit reports that remain open related to the replacement of the agency's data loss protection (DLP) solution and the incorporation of a DLP log review into the Board's employee and contractor offboarding process. Further detail on the status of these recommendations is detailed in appendix B.

Opportunities for Improvement

This year, we noted that three of the five privacy impact assessments (PIAs) sampled had not been updated in over 8 years.[24] Board officials informed us that they are currently streamlining their PIA review process and are examining an automated solution to assist with inventorying PII. Agency officials also informed us that they have recently added two staff members to their team to assist in the review and update of the agency's PIAs. While we are not making a recommendation in this area, we will continue to monitor the Board's efforts to enhance its PIA review process as a part of future audit activities.

Security Training

FISMA requires agencies to develop an information security program that provides security awareness training to personnel, including contractors, who support the operations and assets of the organization, as well as role-based training for individuals with significant information security responsibilities. NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, notes that in general, people are one of the weakest links in attempting to secure agency systems and networks.[25] As such, a robust, enterprisewide security awareness and training program is paramount to ensuring that people understand their IT security responsibilities and organizational policies and know how to properly use and protect the IT resources entrusted to them.

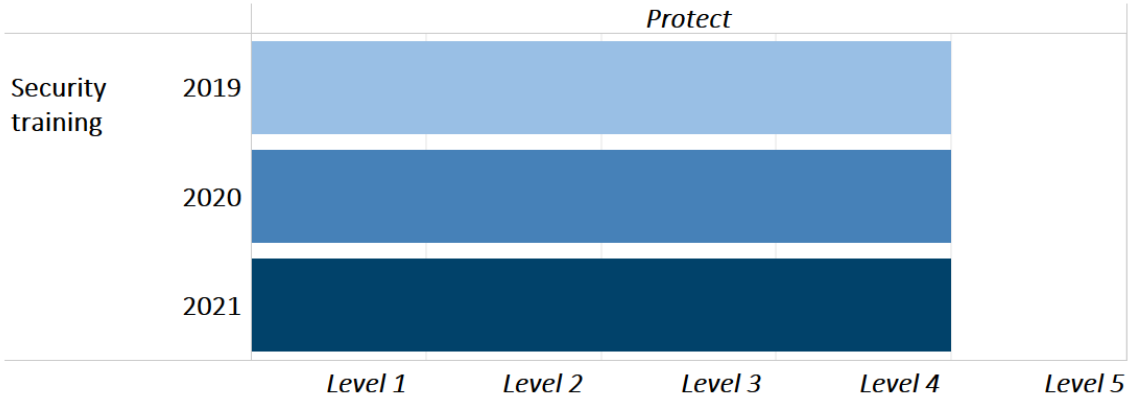
Current Agency Maturity

As in 2020, we found that the Board's security training program continues to operate effectively at a level-4 (*managed and measurable*) maturity (figure 7).

[24] NIST SP 800-53, Rev. 5., defines a PIA as an analysis of how PII is handled (1) to ensure that handling conforms to applicable privacy requirements, (2) to determine the privacy risks associated with an information system or activity, and (3) to evaluate ways to mitigate privacy risks. National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5, updated December 10, 2020.

[25] National Institute of Standards and Technology, *Building an Information Technology Security Awareness and Training Program*, Special Publication 800-50, October 2003.

Figure 7. Maturity of the Security Training Domain, 2019–2021



Source: OIG analysis.

Specifically, we noted that the Board continues

- to provide security awareness activities for its workforce throughout the year on a variety of topics, including phishing, malware, and security incident reporting
- to conduct regular phishing exercises and track metrics on the effectiveness of those exercises. In addition, the agency now removes links within emails for employees who fail an exercise until they complete a phishing training course

Opportunities for Improvement

Our 2018 FISMA audit report includes a recommendation that remains open for the CIO to develop and implement a process to assess the knowledge, skills, and abilities of Board staff with significant security responsibilities and to establish plans to close identified gaps.[26] The status of our prior FISMA recommendation in this area is detailed in appendix B.

Detect

The objective of the *detect* function in the NIST Cybersecurity Framework is to implement activities to discover and identify the occurrence of cybersecurity events in a timely manner. The Cybersecurity Framework notes that continuous monitoring processes are used to detect anomalies and changes in the organization's environment of operation, maintain knowledge of threats, and ensure security control effectiveness. Examples of the assessment areas in this security function, as outlined in DHS's *FY 2021 IG FISMA Reporting Metrics*, that we assessed include the Board's progress in developing and implementing an information security continuous monitoring (ISCM) strategy, performing ongoing system authorizations, and using ISCM-related performance measures.

[26] Office of Inspector General, *2018 Audit of the Board's Information Security Program*, OIG Report 2018-IT-B-017, October 31, 2018.

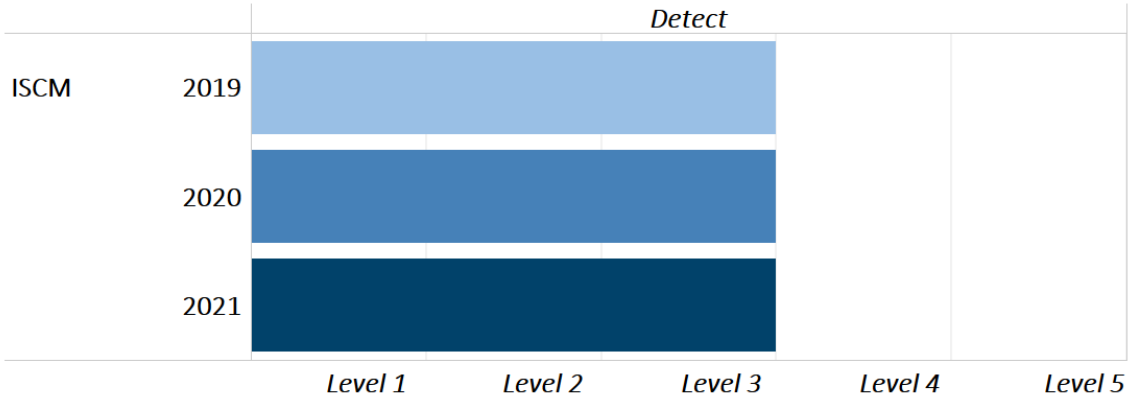
Information Security Continuous Monitoring

ISCM refers to the process of maintaining an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Best practices for implementing ISCM are outlined in NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*.[27] This publication notes that a key component of an effective ISCM program is a comprehensive ISCM strategy based on a risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission and business impacts.

Current Agency Maturity

As in 2020, we found that the Board's ISCM program is operating at a level-3 (*consistently implemented*) maturity (figure 8).

Figure 8. Maturity of the ISCM Domain, 2019–2021



Source: OIG analysis.

This year, we found that the Board continues to strengthen its ISCM program—most notably with regard to system authorization and performance measurement processes. Specifically, we noted that the Board

- continues to consistently implement its system authorization policies and procedures and has taken steps to further strengthen the independence of the agency's security assessors
- uses security dashboards to continuously monitor data related to phishing exercises, incident response, DLP, and web traffic

In addition, we have two recommendations from previous FISMA audit reports related to the development and implementation of an ISCM strategy as well as roles and responsibilities related to the authorization process. We found that actions have been taken to close our recommendation related to the authorization process. The status of prior FISMA recommendations made in these areas is detailed in appendix B.

[27] National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, Special Publication 800-137, September 30, 2011.

Opportunities for Improvement

As we noted above, the Board is planning to develop an ISCM strategy that incorporates requirements from NIST SP 800-53, Rev. 5, as well as any process changes resulting from the agency's ongoing implementation of CDM. We believe that the ISCM program assessment criteria noted in NIST Special Publication 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*, could be an important part of this effort.[28] Specifically, the program assessment can help identify gaps in an ISCM program and indicate the level of readiness for ongoing system-level authorization.

Respond

The objective of the *respond* function in NIST's Cybersecurity Framework is to implement processes to contain the impact of detected cybersecurity events. Examples of the assessment areas in this security function, as outlined in DHS's *FY 2021 IG FISMA Reporting Metrics*, that we assessed include the Board's incident detection, analysis, handling, and reporting processes.

Incident Response

FISMA requires each agency to develop, document, and implement an agencywide information security program that includes policies and procedures for incident response. Best practices for incident response are detailed in NIST Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide*, which notes that an incident response process consists of four key phases: preparation; detection and analysis; containment, eradication, and recovery; and postincident activity.[29]

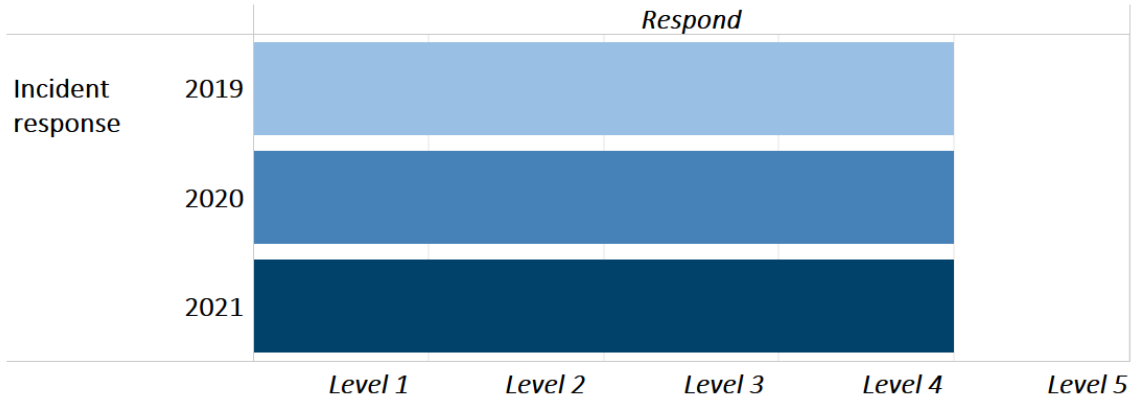
Current Agency Maturity

As in 2020, we found that the Board's incident response program is operating effectively at a level-4 (*managed and measurable*) maturity (figure 9).

[28] National Institute of Standards and Technology, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*, Special Publication 800-137A, May 2020.

[29] National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61, Revision 2, August 2012.

Figure 9. Maturity of the Incident Response Domain, 2019–2021



Source: OIG analysis.

This year, we found that the Board has incorporated new technologies to strengthen incident response processes. Specifically, Board officials informed us that the agency

- has implemented simulation technology to determine how its existing defenses would respond to a potential security incident
- is testing network traffic tools to inspect encrypted network traffic

Opportunities for Improvement

As noted earlier, the Board continues to work with DHS to implement the CDM program in the areas of configuration management and vulnerability management. These CDM capabilities could provide greater visibility into the security configurations and posture of agency systems, thus enabling the Board to strengthen its incident response processes. We will continue to monitor the Board's progress in implementing the tools offered through the CDM program as part of future FISMA audits.

Recover

The objective of the *recover* function in NIST's Cybersecurity Framework is to ensure that organizations maintain resilience by implementing appropriate activities to restore capabilities or infrastructure services that were impaired by a cybersecurity event. The Cybersecurity Framework outlines contingency planning processes that support timely recovery to normal operations and reduce the effect of a cybersecurity event. Examples of the assessment areas in this security function, as outlined in DHS's *FY 2021 IG FISMA Reporting Metrics*, that we assessed include the Board's processes for developing and testing information system contingency plans and the management of contingency planning considerations related to the agency's information and communications technology supply chain.

Contingency Planning

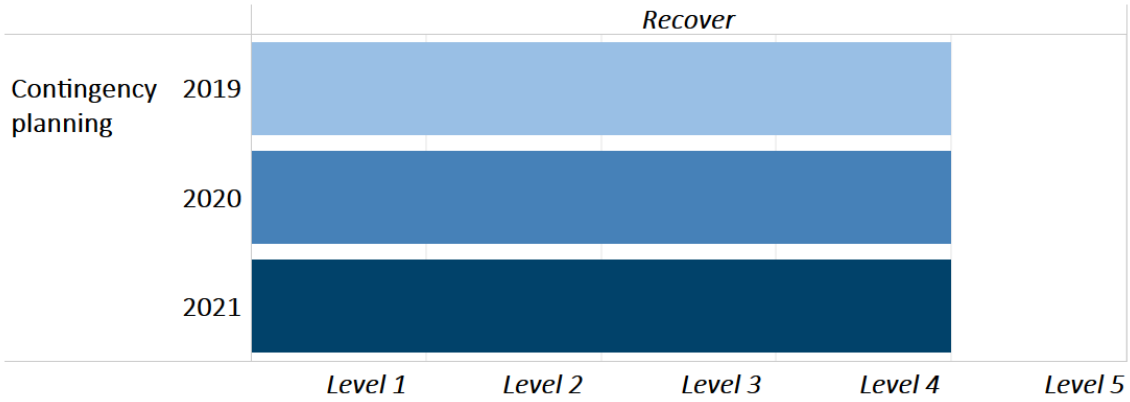
FISMA requires agencies to develop, document, and implement plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization. *Information system contingency planning* refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and

data after a disruption. NIST Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, provides best practices for information system contingency planning.[30]

Current Agency Maturity

As in 2020, we found that the Board's contingency planning program continues to operate effectively at a level-4 (*managed and measurable*) maturity (figure 10).

Figure 10. Maturity of the Contingency Planning Domain, 2019–2021



Source: OIG analysis.

This year, we found that the Board has improved its contingency planning processes as follows:

- The Board has recently completed a devolution exercise with Federal Reserve Bank personnel to simulate the unavailability of agency personnel and is in the process of updating its devolution plan with lessons learned from the exercise.
- The Board has begun to leverage basic ordering agreements to mitigate processing time concerns for its information and communications technology supply chain risks.[31]
- The Board uses an automated solution to continuously monitor its information system backups and to send alerts to responsible parties in the event of a backup failure.

Opportunities for Improvement

In May 2020, the Board issued its cloud-smart strategy, which emphasizes cloud solutions that support business capabilities and opportunities for the efficient execution of the Board's mission. In support of this strategy, the agency is focusing on building and enabling existing platform offerings with cloud enhancements, leveraging cloud offerings to meet increasing infrastructure demands. Board officials

[30] National Institute of Standards and Technology, *Contingency Planning Guide for Federal Information Systems*, Special Publication 800-34, Revision 1, updated November 11, 2010.

[31] A basic ordering agreement may be used to expedite contracting for supplies or services when specific items, quantities, and prices are not known at the time the agreement is executed but a substantial amount of supplies or services covered by the agreement are anticipated to be purchased from the contractor. Under proper circumstances, the use of these procedures can result in economies in ordering parts for equipment by reducing administrative lead time, inventory investment, and inventory obsolescence due to design changes.

informed us that they are working on a review of all cloud-based solutions to determine whether there is an effect on any mission-essential functions. We believe this understanding should help ensure that contingency planning considerations are fully incorporated into the acquisition phase as well as the Board's enterprisewide processes, such as its business impact analysis.

Summary of Priority Metrics

DHS's *FY 2021 IG FISMA Reporting Metrics* directs IGs to use a mode-based approach to determine maturity at the individual domain, function, and programmatic levels.[32] Under this approach, the individual FISMA metrics that compose a domain and function are weighed equally. To drive continued improvements in cybersecurity maturity and to focus agency efforts, DHS's *FY 2021 IG FISMA Reporting Metrics* introduce a pilot concept of weighting specific metrics for assessment and scoring. While IGs are instructed to continue to use the mode-based approach for the 2021 FISMA cycle, this pilot approach will help evaluate the effects of these metrics and prepare agencies for the possibility of changing the calculation process in the future.

This weighted-average pilot approach consists of 10 priority metrics that represent a combination of the lowest average performing metrics from previous IG assessments, administration priorities, and the highest value controls. Below is a summary of our analysis of the Board's maturity for these priority metrics (table 3).

Table 3. Summary of Board's Maturity Across Priority Metrics, by Security Domain

Metric	Maturity summary
Risk management	
Cybersecurity risk management and integration with ERM	The Board has defined cybersecurity risk management policies and processes for framing, assessing, responding to, and monitoring cybersecurity risk. The agency uses its cybersecurity risk register for some enterprise- and division-level information but is not using it to manage system-level risk information. System-level risk information is maintained within the agency's FISMA compliance tools. Further, the agency's ERM program is in the early stages of implementation, with efforts currently focused on operational risk within the divisions operating under the Office of the Chief Operating Officer.[33]

[32] For example, if there are seven questions in a domain and the agency receives a *defined* rating for three questions and *managed and measurable* for four questions, the domain rating is *managed and measurable*.

[33] 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.

Metric	Maturity summary
Automated view of risk	The Board continues to consistently implement two compliance tools to document system-level risk information, including risk control and remediation activities, throughout the agency. However, as noted in our ERM evaluation, the Board has not yet defined requirements for a governance, risk, and compliance (GRC) tool that will provide an automated view of all risks across the agency. Agency officials charged with ERM implementation informed us that once stakeholder needs have been defined, they intend to select a GRC tool that will support the broader rollout of the Board's ERM program. To further mature the agency's automated view of risk, the selected GRC tool will need to integrate with the Board's FISMA compliance tools.
Identity and access management	
Strong authentication measures for privileged users	The Board effectively implements multifactor authentication for access to its network for both privileged and nonprivileged users. The agency maintains a dashboard monitoring the status of PIV workstation compliance for all users. Further, the Board has implemented its PIV card–based solution for remote access authentication.
Least privilege and separation of duties	The *Board Information Security Program* requires the documentation of procedures for ensuring that separation of duties and least privilege principles are applied to the account management process. The agency effectively implements automated mechanisms to support account management processes, including a script to ensure that user accounts are properly deactivated when employees leave the Board.
Data protection and privacy	
PII security controls	Overall, the Board consistently implemented its policies and procedures for the protection of PII as it relates to encrypting data in transit, limiting data transfer to removable media, and sanitizing digital media before disposal or reuse. Board officials informed us that they are still in the process of encrypting the agency's data at rest.
Security controls for exfiltration	The Board continues to monitor inbound and outbound network traffic and quarantines or blocks any traffic that is suspected to be malicious. Further, the Board uses email authentication technology, reviews its Domain Name System records, and ensures the use of valid encryption certificates for its domains. As noted in appendix B, we have two open recommendation related to this metric in the area of DLP.

Metric	Maturity summary
ISCM	
ISCM policies and strategy	The Board is in the process of planning for an ISCM strategy that incorporates the requirements of the latest revision of NIST SP 800-53, Rev. 5. Agency officials informed us that they intend for this plan to be finalized by the fourth quarter of 2021, with strategy development and implementation coming over the next few years. The Board's ongoing implementation of the CDM program will also influence the development of an ISCM strategy, but development has been delayed because of the COVID-19 pandemic and because changes to the CDM program are still being determined by DHS. As noted in appendix B, we have an open recommendation in this area.
Incident response	
Incident detection and analysis	The Board effectively implements its processes and supporting technologies for detecting and analyzing incidents. Further, the agency uses profiling techniques to measure the characteristics of expected activity on its network and systems so that it can more effectively detect security incidents. The Board has conducted a tabletop exercise related to a potential data breach, and agency officials have informed us that they intend to revisit a prior tabletop exercise regarding a ransomware attack. These same officials noted these exercises are used to update the Board's incident response playbooks, as necessary.
Incident handling	The Board effectively implements its incident handling policies, procedures, containment strategies, and eradication processes. Further, responsibility for conducting vulnerability scans has shifted to the Board's IT Security Operations team, which is the team responsible for the agency's incident response program. As a result of this change, we believe there has been greater integration of the Board's incident response and vulnerability management processes.
Contingency planning	
Testing of information system contingency plans	The Board continues to effectively test information system contingency plans on a semiannual basis to ensure that they are performing as intended. The agency employs automated mechanisms to test system-level contingency plans where applicable and documents any issues that arise during its contingency tests so that they can be resolved and retested at a later date. Agency officials also informed us that they continue to conduct regular accountability exercises for Board personnel with contingency-related responsibilities and to coordinate contingency testing with external service providers, as necessary.

Source: OIG analysis.

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 five function areas outlined in DHS's *FY 2021 IG FISMA Reporting Metrics*: *identify*, *protect*, *detect*, *respond*, and *recover*. These five function areas consist of nine security domains: risk management, SCRM, configuration management, identity and access management, data protection and privacy, security training, ISCM, incident response, and contingency planning.

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

- used a risk-based approach and focused our detailed testing activities on the 10 priority metrics identified in DHS's *FY 2021 IG FISMA Reporting Metrics*
- analyzed security policies, procedures, and documentation
- interviewed Board management and staff
- performed vulnerability scans at the network, operating system, and database levels for select systems
- observed and tested specific security processes and controls at the program level
- performed data analytics using a commercially available tool to support our testing in multiple security domains

We contracted with an independent public accounting firm who assessed the effectiveness of the Board's identity and access management and data protection and privacy domains. We reviewed and monitored the work of the contractor to ensure compliance with the contract and *Government Auditing Standards*.

To rate the maturity of the Board's information security program and functional areas, we used the scoring methodology defined in DHS's *FY 2021 IG FISMA Reporting Metrics*. The maturity ratings are determined by a simple majority, where the most frequent level (that is, the mode) across the metrics serves as the overall rating.

We performed our fieldwork from June 2021 to September 2021. 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 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: Status of Prior FISMA Recommendations

As part of our 2021 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 15 recommendations that were open at the start of our 2021 FISMA audit (table B-1). Based on corrective actions taken by the Board, we are closing 8 recommendations related to the risk management, identity and access management, and ISCM domains. The remaining 7 recommendations—which are related to risk management, identity and access management, data protection and privacy, security training, and ISCM—remain open. We will update the status of these recommendations in our spring 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 B-1. Status of 2016–2020 FISMA Recommendations That Were Open as of the Start of Our Fieldwork, by Security Domain

Year	Recommendation		Status	Explanation
Risk management				
2016	1	We recommend that the CIO work with the chief operating officer (COO) to perform a risk assessment to determine which aspects of an insider threat program are applicable to other types of sensitive Board information and develop and implement an agencywide insider threat strategy for sensitive but unclassified Board information, as appropriate.	Open	Board officials informed us that they intend to accept the risk related to this recommendation; however, this acceptance has not yet been documented.

Year	Recommendation		Status	Explanation
2017	1	We recommend that the COO ensure that (a) an optimal governance structure for ERM is implemented that includes considerations for a chief risk officer or equivalent function and (b) an ERM strategy is used to maintain a risk profile for the Board.	Closed	In 2021, we concluded our evaluation of the Board's implementation of ERM.[34] In that report, we issued three recommendations related to assessing the current division-level risk management practices and risk culture, determining the optimal governance structure, and developing an early-stage ERM framework. As such, we are closing our FISMA recommendation because more-specific recommendations are included in our ERM report that we believe, when implemented, will better address this risk.
2017	4	We recommend that the CIO ensure that the Board's enterprise architecture includes technologies managed by all divisions, and work with the COO to enforce associated review processes agencywide.	Closed	The Board is relying on the SRB software catalog and associated review processes to enforce its desired architecture. The Board has developed the software catalog and implemented its SRB processes across all but one agency division. As such, we are closing this recommendation and plan to issue a more targeted recommendation to this one division in a separate, restricted memorandum.
2019	1	We recommend that the CIO develop comprehensive enterprisewide guidance for the inventory of software and associated licenses throughout the Board.	Closed	In 2020, the Board expanded the scope of its SRB and associated review processes across the organization. Since our last review, the agency issued three policies that apply to all software installed on Board devices: the *Software Management Policy*, the *SRB Approved Software Catalog Procedures*, and the *SRB Software Review Procedures*. Divisions that choose to opt out of the SRB must remain in compliance with the *Software Management Policy*. As such, we are closing this recommendation. However, we found that one Board division was not participating in the SRB or maintaining compliance with this policy. As such, we plan to issue a more targeted recommendation to this division in a separate, restricted memorandum.

[34] 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.

Year	Recommendation		Status	Explanation
2019	2	We recommend that the CIO work with all Board divisions to ensure that an accurate and complete software and license inventory is maintained.	Closed	As part of the Board's work to expand the scope of its SRB, the agency worked with divisions to develop an agencywide software catalog of all software installed on Board devices, including approved desktop software, managed mobile applications, and server software. As such, we are closing this recommendation. However, we found that one division did not participate in this effort and is not participating in the SRB or maintaining a comparable software inventory. We plan to issue a targeted recommendation to this division in a separate, restricted memorandum.
2019	3	We recommend that the CIO ensure the consistent application of the Board's POA&M standard for the tracking of system- and program-level security vulnerabilities.	Closed	The Division of IT tracks program-level vulnerabilities and recommendations in its risk register, which includes the necessary fields from the Board's POA&M standard. The risk register is inclusive of all recommendations made to Board divisions. Our 2021 report includes a new recommendation to further improve the agency's POA&M process.
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.	Open	The Division of IT is in the process of working with relevant stakeholders to make necessary updates to information types within the agency's FISMA compliance tool.
Identity and access management				
2017	5	We recommend that the CIO develop and implement an agencywide ICAM strategy that assesses current processes, provides a vision for the desired future state, and identifies plans to achieve that future state.	Closed	The Board has developed and finalized an ICAM strategy. In addition, agency officials informed us that they have obtained funding for a dedicated ICAM team to implement the strategy.

Year		Recommendation	Status	Explanation
2020	2	We recommend that the CIO work with the director of the Division of Board Members to ensure that the necessary security control requirements, including privileged user access controls, are incorporated into the contractual provisions for applicable network devices.	Closed	The Board has included security control requirements within its contractual provisions for applicable network devices. However, the agency decided to address privileged user access controls through a separate process. As such, while we are closing this recommendation, we have identified opportunities to improve this process.
2020	3	We recommend that the CIO ensure that the Board's continuous monitoring processes include the security control requirements for applicable network devices.	Open	The Board's continuous monitoring processes now include vulnerability scanning for applicable network devices. Further, the agency has developed a process to check the security of administrator credentials for network devices. However, our testing continues to identify opportunities to improve this area.
Data protection and privacy				
2019	5	We recommend that the CIO work with the Federal Reserve System to ensure that the DLP replacement solution (a) functions consistently across the Board's technology platforms and (b) supports rulesets that limit the exfiltration weaknesses we identified, to the extent practicable.	Open	Although the Board has worked with the System to identify a replacement DLP solution, Board officials informed us that testing of the new solution has not started. Further, we continue to find exfiltration weaknesses related to the agency's existing DLP solution. The Board currently plans to begin testing and implementing the replacement solution in the fourth quarter of 2021.
2019	6	We recommend that the CIO develop and implement a Boardwide process to incorporate the review of DLP logs into employee and contractor offboarding processes to identify any potential unauthorized data exfiltrations or access.	Open	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 efforts to address our recommendation are ongoing and are planned to be completed by the fourth quarter of 2021.

Year	Recommendation		Status	Explanation
Security training				
2018	6	We recommend that the CIO develop and implement a process to assess the knowledge, skills, and abilities of Board staff with significant security responsibilities and establish plans to close identified gaps.	Open	Although the Board has identified some additional training opportunities to enhance skills for some users with significant security responsibilities, it has not yet performed a complete assessment of the knowledge, skills, and abilities of its security workforce. We recognize that not all individuals performing cybersecurity responsibilities throughout the Board report to the CIO or to the information security officer because of the decentralized nature of the agency's IT security workforce. The Board informed us it plans to accept the risk associated with this recommendation; however, this acceptance has not yet been documented.
ISCM				
2017	8	We recommend that the CIO develop, implement, and regularly update an ISCM strategy that includes performance measures to gauge the effectiveness of related processes and provides agencywide security status.	Open	The Board is in the process of developing an ISCM strategy that incorporates the requirements of the latest revision of NIST SP 800-53, Rev. 5. Agency officials informed us that they intend to first develop an ISCM plan by the fourth quarter of 2021, with strategy development and implementation coming over the next few years. The Board's ongoing implementation of the CDM program will also influence the development of an ISCM strategy but has been delayed because of the COVID-19 pandemic and because changes to the CDM program are still being determined by DHS.
2020	4	We recommend the CIO ensure that roles and responsibilities within the authorization process maintain a level of independence commensurate with the risk level of the information system.	Closed	The Board has transferred the authorizing official role for the systems identified to a senior Division of IT official who is not responsible for the group performing annual security assessments of the agency's information systems.

Source: OIG analysis.

Appendix C: Management Response

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

DIVISION OF
INFORMATION TECHNOLOGY

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

Dear Mark:
We have reviewed your report entitled "2021 Audit of the Board's Information Security Program" prepared as part of your office's oversight responsibilities pursuant of the Federal Information Security Management Act of 2014 (FISMA). The report evaluates the Board of Governors of the Federal Reserve System (Board) with FISMA and related information security and privacy policies, procedures, and standards and guidelines. The report addresses the successful remediation of eight of fifteen recommendations from prior FISMA audits and continues to recognize that the Board operates a comprehensive and effective information security program that has been continually enhanced.

We agree with the recommendations offered in your report. We have already made progress in addressing many of the recommendations. We will provide you with our Plan of Actions and Milestones (POA&Ms) shortly and review our status towards addressing those recommendations.

We appreciate the professionalism and courtesies provided by the staff of the Office of the Inspector General and we look forward to working with your office in the future. Thank you for the opportunity to provide comments on this report.

Sincerely,

SHARON MOWRY
Digitally signed by SHARON MOWRY
Date: 2021.10.25 08:02:09 -04'00'

Sharon Mowry
Chief Information Officer (CIO)

cc: Mr. Peter Sheridan
Mr. Raymond Romero
Mr. Charles Young
Ms. Annie Martin

www.federalreserve.gov

Abbreviations

CDM	Continuous Diagnostics and Mitigation
CIO	chief information officer
COO	chief operating officer
DHS	U.S. Department of Homeland Security
Division of IT	Division of Information Technology
DLP	data loss protection
ERM	enterprise risk management
FISMA	Federal Information Security Modernization Act of 2014
GRC	governance, risk, and compliance
ICAM	identity, credential, and access management
IG	inspector general
ISCM	information security continuous monitoring
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	privacy impact assessment
PII	personally identifiable information
PIV	personal identity verification
POA&M	plan of action and milestones
SCRM	supply chain risk management
SP 800-53, Rev. 5	Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*
SRB	Software Review Board
TIC	Trusted Internet Connection

Report Contributors

Khalid Hasan, Senior OIG Manager for Information Technology
Paul Vaclavik, OIG Manager, Information Technology Audits
Andrew Gibson, OIG Manager, Information Technology Audits
Joshua Dieckert, OIG Manager, Information Technology Audits
Chelsea Nguyen, Senior IT Auditor
Jeffrey Woodward, Senior Policy and Planning Analyst
Trang Do, IT Auditor
Melissa Fortson, IT Auditor
Nick Gallegos, Criminal Investigator
Lauren Alston, IT Audit Intern
Alexander Karst, Senior Information Technology Management Specialist
Fay Tang, Senior Information Technology Management Specialist
Peter Sheridan, Associate Inspector General for Information Technology

Contact Information

General

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551

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

Media and Congressional

OIG.Media@frb.gov

OIG

Hotline

Report fraud, waste, and abuse.

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

OIG Hotline
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551

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