Audit Report
2020-IT-B-020
November 2, 2020

Board of Governors of the Federal Reserve System

2020 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

Executive Summary, 2020-IT-B-020, November 2, 2020

2020 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. The Board continues to take steps to strengthen its information security program. For instance, the Board has finalized its *Vendor Risk Management Standard* and updated the information security clauses in its standard contracting language. In addition, the Board has implemented several role-based training offerings for individuals with significant security responsibilities, including application developers, system owners, and authorizing officials.

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. 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. In addition, the Board has not completed defining its enterprisewide risk management strategy, risk appetite, and risk tolerance levels, which could help guide cybersecurity processes across function areas. We also believe that the Board's ongoing efforts to implement the U.S. Department of Homeland Security's Continuous Diagnostic and Mitigation program will continue to mature the agency's information security program across multiple security functions and help address issues that result from the decentralization of information technology services.

Finally, the Board has taken sufficient actions to close 7 of the 18 recommendations from our prior FISMA audits that remained open at the start of this audit. We will update the status of these recommendations in our upcoming semiannual report to Congress and continue to monitor the Board's progress as part of future FISMA reviews.

Recommendations

This report includes 4 new recommendations and 2 items for management's consideration designed to strengthen the Board's information security program in the areas of risk management, configuration management, identity and access management, data protection and privacy, and information security continuous monitoring. In its response to a draft of our report, the Board concurs with our recommendations and notes that actions are underway to strengthen the Board's information security program. We will continue to monitor the Board's progress in addressing these recommendations as part of future 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 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, 2020-IT-B-020, November 2, 2020

2020 Audit of the Board's Information Security Program

Number	Recommendation	Responsible office
1	Ensure that the Board's FISMA compliance tool is consistently factoring information types into the resulting system classification levels.	Division of Information Technology
2	Work with the director of BDM to ensure that the necessary security control requirements, including privileged user access controls, are incorporated into the contractual provisions for applicable network devices.	Division of Information Technology
3	Ensure that the Board's continuous monitoring processes include the security control requirements for applicable network devices.	Division of Information Technology
4	Ensure that roles and responsibilities within the authorization process maintain a level of independence commensurate with the risk level of the information system.	Division of Information Technology

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

MEMORANDUM

DATE: November 2, 2020

TO: Distribution List

FROM: Peter Sheridan
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2020-IT-B-020: *2020 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, which 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, restricted 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 2020 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
Michelle Hercules
Lucretia Boyer
Cheryl Patterson

Distribution:
Patrick J. McClanahan, Chief Operating Officer
Ricardo A. Aguilera, Chief Financial Officer
Sharon Mowry, Chief Information Officer
Winona Varnon, Director, Division of Management
Michelle A. Smith, Assistant to the Board, Chief of Staff, and Director, Office of Board Members

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, and practices. 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 2020 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 eight 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 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 4.0, April 17, 2020.

[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
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 2020 IG FISMA Reporting Metrics*.

As noted in DHS's *FY 2020 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. Two of these priorities include the security of mobile devices and the modernization of the Trusted Internet Connections (TIC) initiative. Specifically, DHS's *FY 2020 CIO FISMA Metrics* include an additional focus on the security of mobile devices (government-furnished equipment and non-government-furnished equipment), particularly in the areas of mobile device management and enterprise mobility management.[4] In addition, the Office of Management and Budget (OMB) provided updated guidance to federal agencies on the use of TIC capabilities in modern architectures and frameworks, such as cloud environments.[5] As such, DHS's *FY 2020 IG FISMA Reporting Metrics* have been updated to gauge the effectiveness of agencies' processes to secure mobile endpoints, employ secure application development processes, and plan for the effective implementation of the security capabilities outlined in OMB's updated TIC guidance.

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 OMB, DHS, and other key stakeholders, developed a maturity model intended to better address and report on the effectiveness of an agency's information

[4] U.S. Department of Homeland Security, *FY 2020 CIO Reporting Metrics*, Version 1, October 2019.

[5] Office of Management and Budget, *Update to the Trusted Internet Connection (TIC) Initiative*, OMB Memorandum M-19-26, September 2019.

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 represent the degree to which policies and procedures are being developed and implemented, 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 2020 IG FISMA Reporting Metrics*, level 4 (*managed and measurable*) represents an effective level of security.[6] Details on the scoring methodology for the maturity model are included in appendix A.

[6] NIST defines *security control effectiveness* as the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing or mediating established security policies. National Institute of Standards and Technology, *Security and Privacy of Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4, updated January 22, 2015.

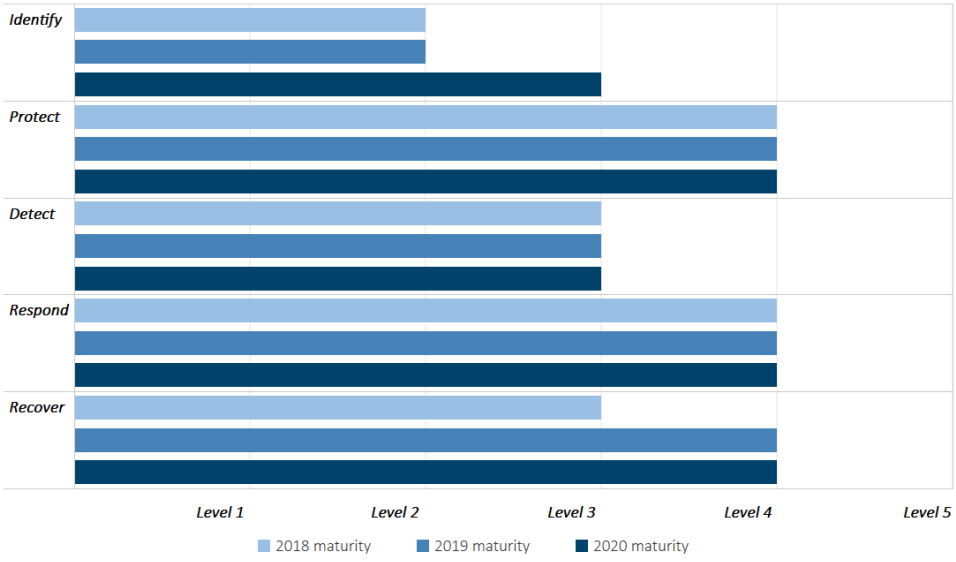
Figure 1. FISMA Maturity Model Rating Scale

Source: OIG analysis of DHS's *FY 2020 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).[7] Although the Board has strengthened its program since our 2019 FISMA report, it can mature its processes across specific FISMA domains in all five NIST Cybersecurity Framework security functions: *identify*, *protect*, *detect*, *respond*, and *recover*. For example, the Board has improved to a level-3 (*consistently implemented*) maturity in the *identify* function area. However, the Board continues to work toward its implementation of enterprise risk management (ERM). Specifically, significant aspects of the program are still to be determined, including the documentation of an ERM strategy; the use of agencywide risk appetite and tolerance levels; and the adoption of the Board's selected governance, risk, and compliance tool. We believe that the decentralization of information technology (IT) services results in an incomplete view of the risks affecting the Board's security posture. In addition, the Board's ongoing efforts to define an ERM strategy, risk appetite, and risk tolerance levels could help guide cybersecurity processes across function areas. We believe that the Board's work to strengthen the information security processes in the *identify* function and its ongoing efforts to implement DHS's Continuous Diagnostics and Mitigation (CDM) program will positively affect the Board's maturity in other areas.[8]

Figure 2. Maturity of the Board's Information Security Program, by Security Function, 2018–2020



Source: OIG analysis.

[7] Appendix A explains the scoring methodology outlined in DHS's *FY 2020 IG FISMA Reporting Metrics* that we used to determine the maturity of the Board's information security program.

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

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 2020 IG FISMA Reporting Metrics*, that we assessed include the Board's processes for ERM; the development and implementation of an enterprise architecture; asset management, including mobile device management; and the use of plans of action and milestones (POA&Ms) to manage the remediation of security weaknesses.

Risk Management

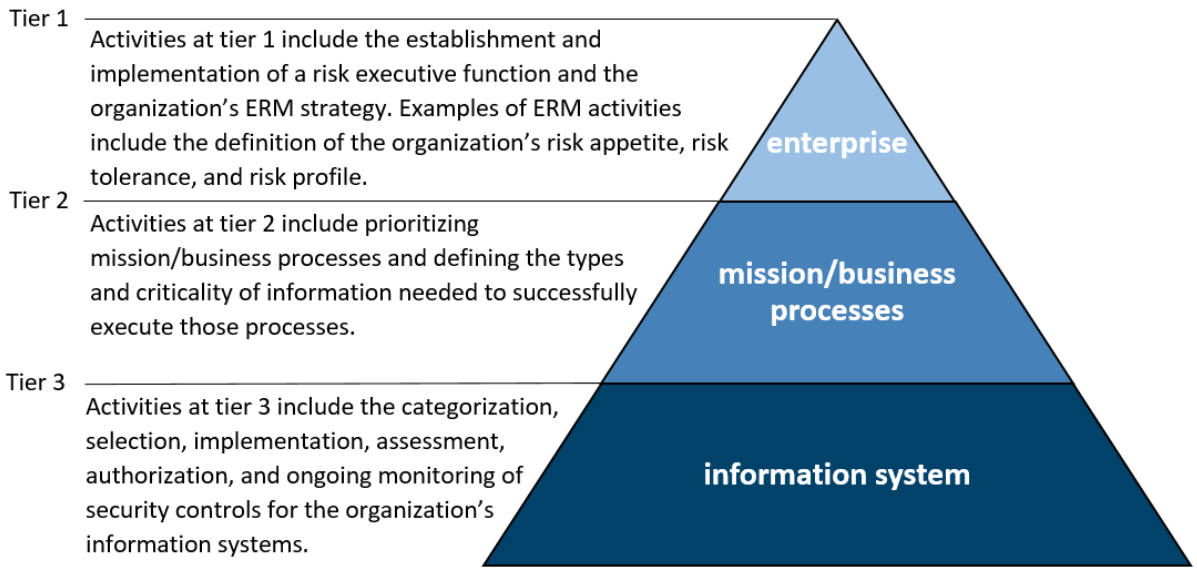
FISMA requires federal agencies to provide information security protections commensurate with their risk environment and to ensure that information security management processes are integrated with strategic, operational, and budgetary planning processes. *Risk management* refers to the program and supporting processes used to manage risk to organizational operations, assets, and individuals and is a holistic activity that affects every aspect of the organization. Federal guidance notes the importance of ERM, which is an effective agencywide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined effect of risks as an interrelated portfolio, rather than addressing risks within silos. Federal guidance also emphasizes that an effective ERM program promotes a common understanding for recognizing and describing potential risks, such as cybersecurity, strategic, market, legal, and reputations risks, that can affect an agency's mission.[9]

The relationship between cybersecurity risk management and ERM is further outlined in NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* (SP 800-39), which states that effective risk management involves the integration of activities at the enterprise, mission and business process, and information system levels.[10] The risk management process should be carried out across these three tiers, with the overall objective of continuous improvement in the organization's risk-related activities and effective communication among stakeholders (figure 3). The risk management guidance described in SP 800-39 is complementary to and should be used as part of a comprehensive ERM program.

[9] According to OMB Memorandum M-17-25, *cybersecurity risk management* refers to the full range of activities undertaken to protect IT and data from unauthorized access and other cyberthreats; to maintain awareness of cyberthreats; to detect anomalies and incidents adversely affecting IT and data; and to mitigate the effect of, respond to, and recover from incidents. Office of Management and Budget, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, OMB Memorandum M-17-25, May 9, 2018.

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

Figure 3. The Three Tiers of Risk Management

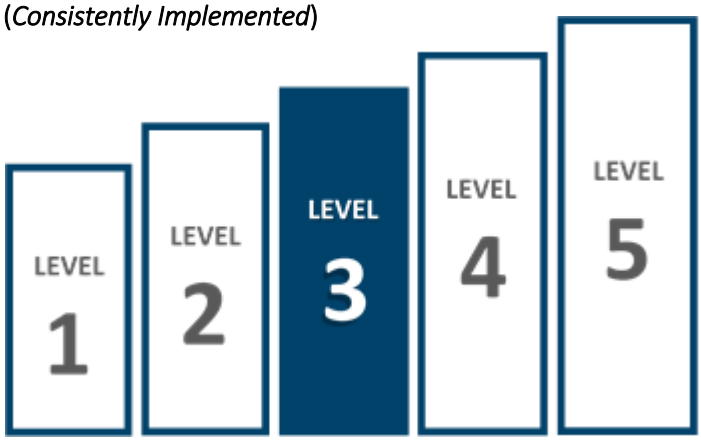


Source: NIST SP 800-39.

Current Agency Maturity

This year, we found that the Board's risk management program has matured and is operating at a level-3 (*consistently implemented*) maturity (figure 4). The Board has consistently implemented processes for hardware asset management and system-level risk assessments. In addition, we found that the agency's mobile device management processes are operating effectively. Specifically, the Board enforces the capability to deny access to agency enterprise services when mobile devices are out of compliance. The agency also enforces the capability to prevent the execution of unauthorized software through application blacklisting and further restricts the applications that can access Board data through cryptographic containerization. In addition, we found that the software assurance process for mobile applications is consistently implemented.

Figure 4. Risk Management, Level 3 (*Consistently Implemented*)



Source: OIG analysis.

We also found that the Board has continued to mature information security processes in the areas of vendor risk management, policies and procedures, and software asset management—areas we previously made recommendations in (appendix B).[11] Specifically, we noted the following:

- The Board finalized its *Vendor Risk Management Standard* and updated the information security clauses in its standard contracting language. This standard was developed jointly by the Division of Information Technology (Division of IT) and the Board's Procurement section and defines the security assurance requirements through each phase of the procurement process, as well as postaward continuous monitoring requirements.
- The Board has taken steps to ensure that its vendor inventory is complete and its vendor risk management process identifies system interconnections; however, we identified inconsistencies in the Board's cloud inventory and are looking at this area in greater detail in a concurrent evaluation of the Board's adoption of cloud solutions.
- The Board has also implemented a process to review its security policies and prioritize security policy updates for review.
- The Board has worked to expand the scope of its Software Review Board (SRB) and the associated agencywide review processes and is working with divisions to develop an agencywide software catalog. The SRB has already begun to conduct reviews for divisions other than the Division of IT.

At the enterprise level, the Board continues to work toward its implementation of ERM. The agency has put a team in place to lead the ERM initiative, which is being conducted in a phased approach. Currently, the Board is conducting risk assessments and developing risk profiles for each division that reports administratively to the chief operating officer (COO). This phase is scheduled to be completed in early 2021. Agency officials informed us that once this phase is complete, the ERM team plans to present this work as a proof of concept to Board management for rollout across the agency. In the interim, the Board's Senior Officer Committee (SOC) is serving as the agency's risk committee, as noted in the committee's charter.[12] Further, agency officials informed us the committee is discussing enterprisewide risks.

Although we found that a phased approach to implementing ERM within the divisions that report to the COO has been defined, the Board has not yet defined a strategy that highlights the desired future state for ERM throughout the agency. Board officials leading the ERM initiative informed us that many elements of the agency's ERM program would depend in large part on the acceptance from all Board divisions of the work currently underway within the divisions that report to the COO. Significant aspects of the Board's ERM program are still to be determined, including the use of an agencywide risk appetite and tolerance levels and the adoption of the Board's selected governance, risk, and compliance tool. We believe that the Board will need to address these issues to have an effective risk management program.

[11] Office of Inspector General, *2017 Audit of the Board's Information Security Program*, OIG Report 2017-IT-B-018, October 31, 2017; Office of Inspector General, *2018 Audit of the Board's Information Security Program*, OIG Report 2018-IT-B-017, October 31, 2018; and Office of Inspector General, *2019 Audit of the Board's Information Security Program*, OIG Report 2019-IT-B-016, October 31, 2019.

[12] The SOC comprises delegates, such as deputy directors, from each Board division. The SOC's primary functions are to serve as an advisory committee for internal administrative issues and to serve as the Board's risk committee.

Further, we are looking at these areas in greater detail in a concurrent evaluation of the Board's implementation of ERM.

In coordination with the Board's ERM team, the Division of IT is currently developing and implementing an Enterprise Cyber Governance program. A charter for the program, which is cosponsored by the COO and the CIO, has been finalized. This program encompasses the Board's cybersecurity risk management framework, seeks to establish the normal range of acceptable enterprise cybersecurity risk, and determines a cybersecurity residual risk threshold for each of the Board's significant cybersecurity risk scenarios. In addition, to ensure broad enterprise input into the development of the program, a Governance Development Team has been formed with representation from all Board divisions. This team developed the cybersecurity risk identification process, which, at the time our fieldwork concluded, had just kicked off its first risk assessment in the Division of Financial Management. We believe that as the Division of IT matures its Enterprise Cyber Governance program, it will need to continue to ensure that the program is integrated with the agency's ERM program.

At the information system level, we also identified an opportunity for improvement related to the categorization of Board systems that contain sensitive personally identifiable information (SPII).[13] Specifically, we found that several systems on the FISMA inventory were not categorized in accordance with the Board's *Information Classification and Handling Standard*. The standard states that the security classification process requires all Board information to be classified into one of three levels—*low*, *moderate*, or *high*—based on the potential impact to the confidentiality, availability, or integrity of Board information. Systems with information classified as SPII should have a confidentiality rating of *moderate*; however, we found that these systems were categorized as *low*.

Board officials informed us that impact levels are automatically determined by the information type that is entered into the Board's compliance tool and cannot be modified. Specifically, the tool maps information types to a classification level. We believe that this mapping process is not accurately recognizing SPII and the resulting impact to system classification levels. Board officials also noted that regardless of the system's confidentiality rating, the system's security risk profile would require additional information security controls if the system were to contain SPII.[14] However, we found that the system security risk profile for the systems we identified did not require these additional security controls. We believe that consistent categorization of these systems can better ensure that controls are implemented based on risk.

Recommendation

We recommend that the CIO

1. Ensure that the Board's FISMA compliance tool is consistently factoring information types into the resulting system classification levels.

[13] The Board's *Information Classification and Handling Standard* defines *SPII* as personally identifiable information that, if lost or misused, has the potential to cause serious harm to an individual or to the Board's mission or operations.

[14] The Board's *Risk Management Program and Risk Assessment Standard* requires that each information system be assigned a security risk profile determined by the system security risk level questionnaire. The Board's risk management requirements (for example, security controls required and frequency of review) are determined by the risk profile.

Management Response

The CIO concurs with our recommendation and notes that a POA&M will be established to detail the steps the Board will take to address our recommendation.

OIG Comment

We plan to follow up on the steps outlined in the Board's POA&M to ensure that the recommendation is fully addressed, including the agency's risk-based implementation of controls.

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 prevent, 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 *protect* function has four security domains with associated components that IGs are required to assess (table 2).

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 2020 IG FISMA Reporting Metrics*.

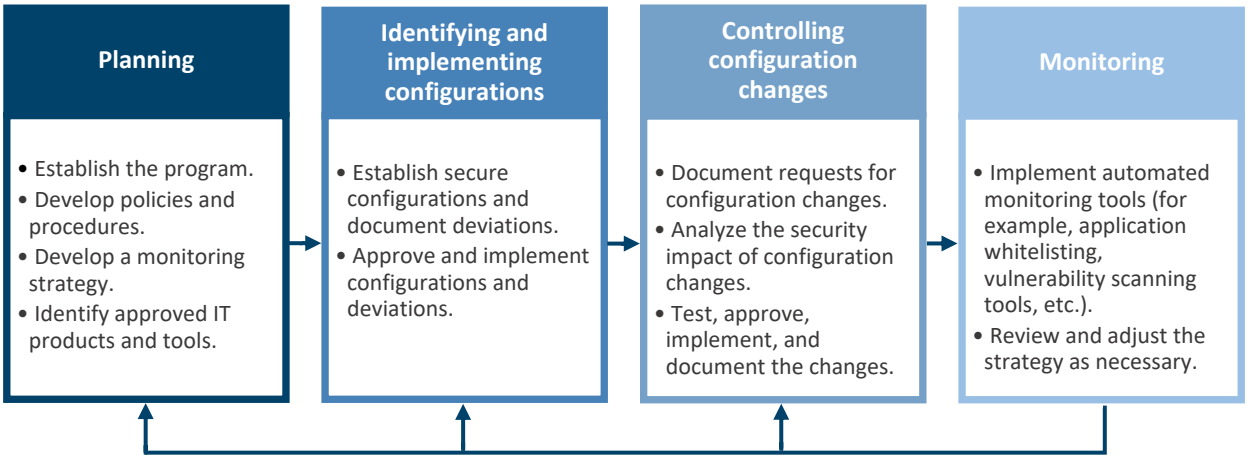
Configuration Management

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. NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems* (SP 800-128), recommends integrating information security into configuration management processes.[15] Security-focused

[15] National Institute of Standards and Technology, *Guide for Security-Focused Configuration Management of Information Systems*, Special Publication 800-128, updated October 10, 2019.

configuration management of information systems involves a set of activities that can be organized into four major phases: (1) planning, (2) identifying and implementing configurations, (3) controlling configuration changes, and (4) monitoring (figure 5).

Figure 5. Security-Focused Configuration Management Phases



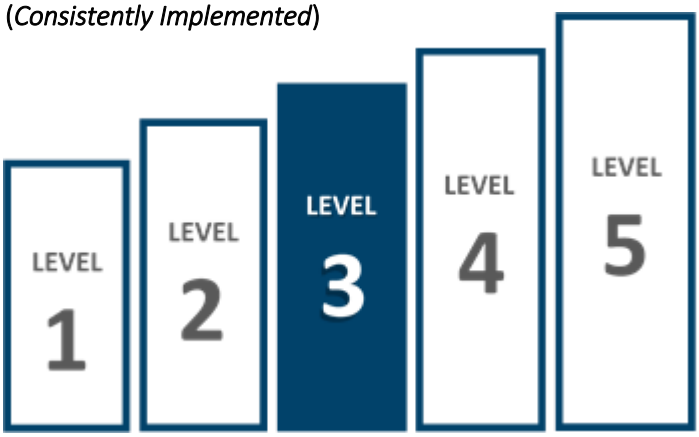
Source: NIST SP 800-128.

SP 800-128 states that monitoring identifies undiscovered or undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes, all of which, if not addressed, can expose the organization to increased risk. Further, SP 800-128 encourages organizations to perform vulnerability scanning activities to discover network components not recorded in the organization's asset inventory as well as to identify potential discrepancies between the approved configuration baselines and the actual configuration for an information system.[16]

Current Agency Maturity

As in 2019, we found that the Board's configuration management program is operating at a level-3 (*consistently implemented*) maturity (figure 6), with the agency performing some activities indicative of a higher maturity level. For example, we found that the Board maintains performance metrics for its change control processes. In addition, the Board continues to enhance the security configurations of its information systems by deploying automated mechanisms, such as application whitelisting software and network access controls. Further, we found that the Board routes various types of traffic,

Figure 6. Configuration Management, Level 3 (*Consistently Implemented*)



Source: OIG analysis.

[16] Vulnerability scanning can help identify outdated software versions, missing patches, and misconfigurations and validate compliance with or deviations from an organization's security policy.

including cloud and mobile, through defined access points and maintains an accurate inventory of agency network connections.

We identified an opportunity to improve the documentation of the agency's risk acceptances for critical and high-risk vulnerabilities that are not able to be remediated within the Board's required time frames. The Division of IT's *Vulnerability Remediation Policy* states that critical and high-risk vulnerabilities should be remediated within 30 and 60 days, respectively. This policy also states that if a vulnerability cannot be remediated within the established time frames, a risk acceptance should be requested. However, we noted that not all risk acceptances clearly identify which vulnerabilities and system components they apply to. As a result, Board officials informed us that they have to manually reconcile the status of these vulnerabilities within the agency's security event and incident management dashboard. While we are not making a recommendation in this area, we believe that management should consider clarifying its policies and procedures to ensure risk acceptances clearly identify which vulnerabilities and system components are affected. We plan to issue a separate, restricted memorandum in this area.

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) (figure 7).

Figure 7. ICAM Conceptual Design

Source: CIO Council, *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*.

Effective identity and access management is a key control area for managing the risk from insider threats, and FISMA requires agencies to implement controls to preserve authorized restrictions on access and disclosure. A key component of effective identity and access management is developing a comprehensive strategy that outlines the components of the agency's ICAM program within the business functions that they support.

The CIO Council has published *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance* to provide the government with a common framework and implementation guidance to plan and execute ICAM programs.[17] The guidance highlights several interrelated activities and use cases that should be considered when developing an ICAM strategy, including (1) an agency's specific ICAM challenges in its current state, (2) the desired method for completing the ICAM function, and (3) the gaps between the as-is and target states. Underscoring the importance of ICAM strategies, recent OMB guidance states that, in line with the federal government's

[17] CIO Council, *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, Version 2.0, December 2, 2011.

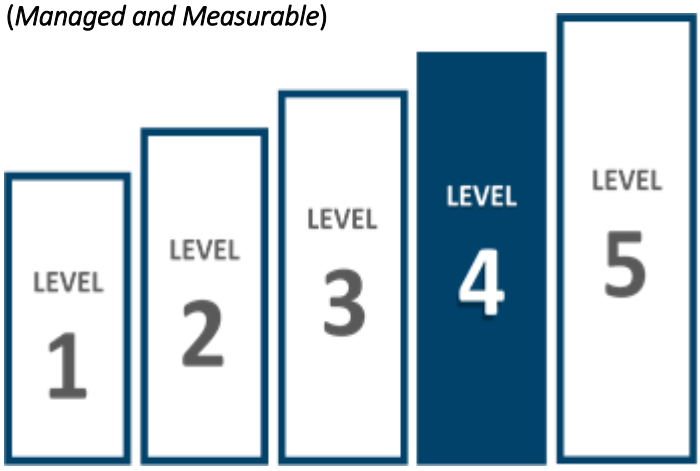
approach to modernization, it is essential that agencies' ICAM strategies and solutions shift toward a model informed by risk management perspectives, the federal resources accessed, and outcomes aligned to agency missions.[18]

Another key component to an effective ICAM program is the application of the principle of least privilege. This principle dictates that organizations should restrict access to accounts and authorize access for only those users (or processes acting on behalf of users) who need it to accomplish assigned tasks in accordance with organizational missions and business functions. The Board's information security policies and procedures cover multiple elements of ICAM, including the performance of background investigations to determine an individual's suitability to be employed in certain positions as well as procedures to ensure that the principle of least privilege is applied to the agency's account management processes.

Current Agency Maturity

As in 2019, we found that the Board's ICAM program continues to operate effectively at a level-4 (*managed and measurable*) maturity (figure 8). Specifically, the Board continues to require multifactor authentication for access to its network for both privileged and nonprivileged users. This multifactor authentication includes the use of a personal identity verification card–based solution for remote access to the network. Further, we found that the Board effectively screens agency personnel to determine an individual's suitability to perform particular job functions based on the risk designation assigned to the position.

Figure 8. Identity and Access Management, Level 4 (*Managed and Measurable*)



Source: OIG analysis.

This year, we found that the Board has continued to mature identity and access management processes related to its development of an agencywide ICAM strategy and its use of complete, visible warning banners on the agency's public-facing systems—areas we previously made recommendations in (appendix B).[19] Specifically, we noted the following:

- The Board has begun to draft an ICAM strategy designed to incorporate activities currently performed by the Division of IT as well as other infrastructure support teams across the agency. This draft strategy notes the complexities of the Board's IT environment, including the

[18] Office of Management and Budget, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, OMB Memorandum M-19-17, May 21, 2019.

[19] Office of Inspector General, *2017 Audit of the Board's Information Security Program*; and Office of Inspector General, *2019 Audit of the Board's Information Security Program*.

decentralized management of various ICAM-related processes and solutions as well as the agency's ongoing introduction of additional cloud services.

- The Division of IT has worked to revise the agency's system warning banner language to ensure that it includes all components required by NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (SP 800-53) and has begun to update the warning banners for the subsystems accessible from the agency's public website.[20]

Further, in 2018 we reported that the Board was not including specific network devices in its vulnerability scanning processes. Board officials notified us that they cannot perform vulnerability scanning on these network devices because vendors own and manage the credentials; performing such scanning may void the Board's vendor maintenance agreements. As such, the Board accepted the risk of not performing vulnerability scanning on these devices, and we are closing our 2018 recommendation in this area. This year, we performed manual testing on these devices and identified opportunities for improvement in privileged user access controls. The specific details of these weaknesses and the affected devices were communicated in a separate, restricted memorandum.

Division of IT officials informed us that they are in the process of working with the Division of Board Members (BDM) to update the contractual provisions to include requirements for properly securing these devices, as well as implementing a broader continuous monitoring approach to ensure that those security requirements are met.[21] We believe that the inclusion and enforcement of security requirements in the Board's network device contracts will reduce the potential risk of unauthorized access to sensitive information, the unavailability of these network devices, and harm to the integrity of the agency's IT environment.

Recommendations

We recommend that the CIO

2. Work with the director of BDM to ensure that the necessary security control requirements, including privileged user access controls, are incorporated into the contractual provisions for applicable network devices.

3. Ensure that the Board's continuous monitoring processes include the security control requirements for applicable network devices.

Management Response

The CIO concurs with our recommendations and notes that POA&Ms will be established to detail the steps the Board will take to address our recommendations.

[20] National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4, updated January 22, 2015.

[21] BDM manages the contracts for these network devices.

OIG Comment

We plan to follow up on the steps outlined in the Board's POA&Ms to ensure that the recommendations are fully addressed.

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.[22]

In response to the increased use of computers and the internet to process government information, the E-Government Act of 2002 was enacted to ensure public trust in electronic government services. The act requires federal agencies to conduct privacy impact assessments (PIAs) for systems that collect, maintain, or disseminate information in identifiable form from or about members of the public and publish them on the agency's website.

The emphasis on PII protection is further highlighted in NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, which notes the importance of the identification of all PII residing in the organization or under the control of a third party on behalf of the organization.[23] Further, this special publication recommends measures to protect PII and other sensitive information, including operational safeguards (for example, policies, procedures, and awareness training); privacy-specific safeguards (for example, minimizing the use, collection, and retention of PII); and security controls (for example, analysis of audit records for indications of inappropriate activity affecting PII, automated solutions to monitor data exfiltration, and the protection of data at rest).

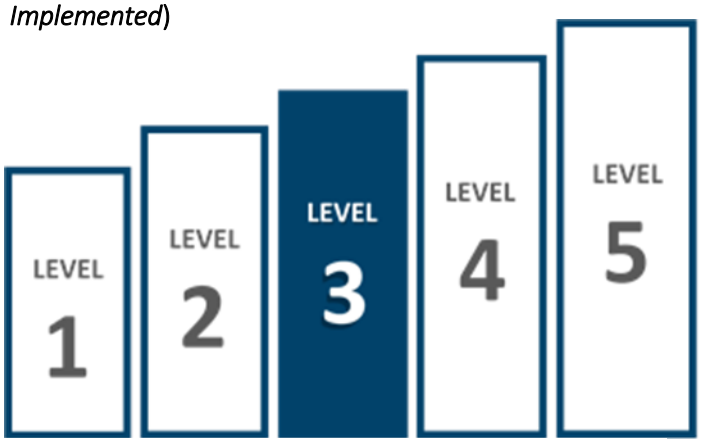
[22] Office of Management and Budget, *Managing Information as a Strategic Resource*, OMB Circular A-130, July 28, 2016.

[23] National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, Special Publication 800-122, April 6, 2010.

Current Agency Maturity

As in 2019, we found that the Board's data protection and privacy program is operating at a level-3 (*consistently implemented*) maturity (figure 9). For example, the Board has consistently implemented security controls for the protection of the PII that is collected, used, maintained, shared, or disposed of by the agency, including the encryption of data at rest in its database management systems. The Board has also consistently implemented its data breach response plan for any incidents involving SPII in its possession or under its control. In addition, we also found that the Board has implemented an agencywide privacy awareness training that all users are required to complete on an annual basis.

Figure 9. Data Protection and Privacy, Level 3 (*Consistently Implemented*)



Source: OIG analysis.

This year, we found that the Board has continued to mature its data loss protection (DLP) and privacy processes—an area we previously made recommendations in (appendix B).[24] Specifically, we noted the following:

- The Board has worked with the Federal Reserve System to identify a replacement network-based DLP solution and is in the process of establishing a test environment to work toward implementation.
- The agency is working to develop an enterprisewide DLP lookback process for employees leaving the organization. At the time our fieldwork concluded, Division of IT officials informed us that the process was close to implementation and that they were in the process of working with the many stakeholders involved in employee offboarding to streamline and automate the process.

We identified an opportunity for improvement this year regarding the timely completion of privacy threshold analyses (PTAs), which determine whether a PIA is required for systems.[25] Specifically, we identified several systems for which PIAs either were not published on the Board's public website or were not documented in the agency's FISMA compliance tools.[26] The majority of these systems had PTAs or PIAs that were in process and documented within the system's POA&Ms. Our review of the POA&Ms for these systems found that completion of the PTAs has been ongoing for over 12 months and was often delayed. Board officials informed us that the completion of PTAs is a complex process that requires coordination with various stakeholders. While we are not making a recommendation in this area, we believe that management should consider reviewing the resources allocated to this process to ensure

[24] Office of Inspector General, *2019 Audit of the Board's Information Security Program*.

[25] The Board uses PTAs to identify possible uses of PII or SPII maintained in agency systems. This information is then evaluated by the Board's privacy officials to ensure that the full scope of the PII and related safeguards are documented.

[26] The details of these systems and our testing in this area will be communicated in a separate memorandum.

that PTAs are completed timely and that their status is accurately reflected in the Board's FISMA compliance tools.

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*, states that, in general, people are one of the weakest links in attempting to secure agency systems and networks.[27] 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.

A key component to an enterprisewide security training program is the assurance that individuals with significant security responsibilities have the required knowledge, skills, and abilities to perform their roles within the organization. The *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, published by NIST in August 2017, is a resource designed to support a workforce capable of meeting an organization's cybersecurity needs and guidance to help leaders better understand, inventory, and track strengths and gaps in their cybersecurity workforce's knowledge, skills, and abilities.[28] Further, the framework organizes individuals with security responsibilities into seven general categories: *analyze*, *collect and operate*, *investigate*, *operate and maintain*, *oversee and govern*, *protect and defend*, and *securely provision*.

In accordance with FISMA requirements, the *Board Information Security Program and Policies* notes that all employees and contractors with access to agency information systems must complete security awareness training before being permitted access to the Board's network and each year thereafter. The program also requires that role-based training be provided for individuals with significant security responsibilities and that records of awareness and role-based training attendance be maintained.

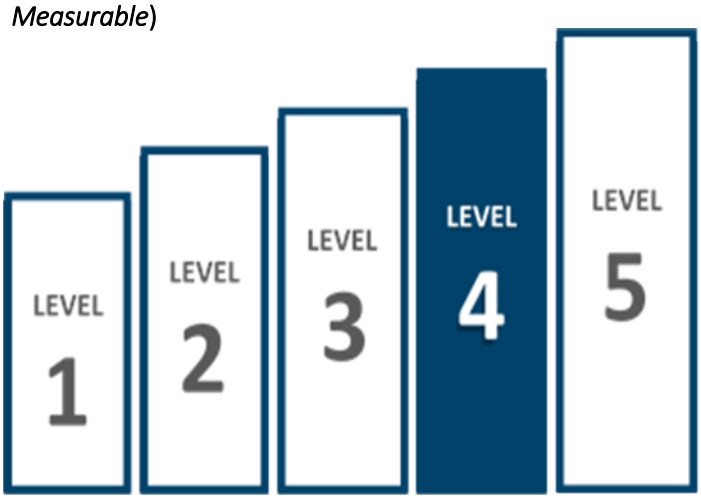
[27] National Institute of Standards and Technology, *Building an Information Technology Security Awareness and Training Program*, Special Publication 800-50, October 1, 2003.

[28] National Institute of Standards and Technology, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, Special Publication 800-181, August 7, 2017.

Current Agency Maturity

As in 2019, we found that the Board's security training program continues to operate effectively at a level-4 (*managed and measurable*) maturity (figure 10). Specifically, we noted that the Board conducts ongoing security awareness activities for its workforce throughout the year on a variety of topics, including phishing, malware, mobile device security, remote access security, and security incident reporting. This year, in response to the COVID-19 pandemic, the Division of IT issued communications to all employees reminding them of certain security-related practices that are of heightened importance. Further, the Board conducts regular phishing exercises, tracks metrics on the effectiveness of those exercises, and uses a tool to report suspicious emails. The Board has been steadily increasing the complexity of its phishing exercises to increase the awareness level of the agency's employees.

Figure 10. Security Training, Level 4 (*Managed and Measurable*)



Source: OIG analysis.

This year, we found that the Board has continued to mature its security training program through the implementation of several role-based trainings for individuals with significant security responsibilities, including application developers, system owners, and authorizing officials. Although these trainings are not required, Board officials informed us that these areas have been identified as ones in which additional role-based training would enhance the skill sets of individuals performing these respective responsibilities. The Board acknowledges that it is still working toward a process to assess the knowledge, skills, and abilities of its workforce, in accordance with the recommendation made in our 2018 FISMA audit report,[29] and these trainings represent progress in the identification of the organization's cybersecurity needs and the methods by which to close any identified skill gaps. The status of prior FISMA recommendations made in this area can be found 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 2020 IG FISMA Reporting Metrics*, that we assessed include the Board's progress in developing and implementing

[29] Office of Inspector General, *2018 Audit of the Board's Information Security Program*.

an information security continuous monitoring (ISCM) strategy, performing ongoing system authorizations, and using ISCM-related performance measures.

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* (SP 800-137).[30] SP 800-137 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 and awareness of vulnerabilities, up-to-date threat information, and mission and business impacts.

SP 800-137 emphasizes that an ISCM strategy is meaningful only within the context of broader organizational needs, objectives, or strategies and as part of a broader risk management strategy. Once a strategy is defined, SP 800-137 states that the next step in establishing an effective ISCM program is to establish and collect security-related metrics to support risk-based decisionmaking throughout the organization. An ISCM strategy is periodically reviewed to ensure that (1) it sufficiently supports the organization in operating within acceptable risk tolerance levels, (2) metrics remain relevant, and (3) data are current and complete. In addition to SP 800-137, NIST has published additional guidance in Special Publication 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment* (SP 800-137A), that can be used to guide the development of an ISCM strategy.[31] This special publication states that creating and using an ISCM program assessment can help guide the development of an ISCM strategy and reduce the overall risk to organizations by identifying gaps in an ISCM program. Further, an ISCM program assessment can indicate the level of readiness for ongoing system-level authorization.

Current Agency Maturity

As in 2019, we found that the Board's ISCM program is operating at a level-3 (*consistently implemented*) maturity (figure 11). For instance, the Board has implemented a *Continuous Monitoring Standard* that outlines the key components of its ISCM program at the system level. Further, the agency continues to perform ongoing security control assessments; grant system authorizations; and monitor security controls to provide a view of the organizational security posture, including the use of a security dashboard that

Figure 11. ISCM, Level 3 (*Consistently Implemented*)

Source: OIG analysis.

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

[31] National Institute of Standards and Technology, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*, Special Publication 800-137A, May 21, 2020.

captures metrics on IT security operations. These metrics include activities related to incident response functions, phishing exercises, user activity, web traffic, and DLP. In addition, the Board has developed dashboards and metrics related to information system POA&Ms and risk acceptances.

This year, we found that the Board has continued to mature information security processes related to the development of an ISCM strategy—an area we previously made a recommendation in (appendix B).[32] Specifically, we noted the following:

- The Board has worked with DHS to deploy the CDM program in the areas of configuration management and vulnerability management. Board officials notified us that they continue to work with DHS to ensure that the information collected in these areas is accurate and complete. However, the timeline for implementing the full suite of CDM capabilities has been delayed due to the COVID-19 pandemic.
- The Board is working to update existing information security policies to incorporate NIST Cybersecurity Framework requirements and will also incorporate changes from the upcoming revision of NIST SP 800-53. In addition, the Board is working to incorporate additional security requirements for cloud systems as the agency begins to implement more cloud-based solutions.

Board officials informed us that the agency plans to develop an ISCM strategy after these efforts are completed. We believe that as the agency develops its ISCM strategy, it should consider using the ISCM program assessment criteria noted in NIST 800-137A to identify any potential gaps in the implementation of its ISCM program.

In addition, we identified an opportunity for improvement related to the independence of the Board's security assessors. Specifically, we found that the Board's security assessors, who work in the Information Security Compliance Unit, report to the agency's chief information security officer (CISO), who also serves as the authorizing official for 47 of the organization's information systems.[33] NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, states that the authorizing official determines the level of assessor independence based on applicable laws, executive orders, directives, regulations, policies, or standards.[34]

The *Board's Information Security Program and Policies* states that the CISO ensures that independent reviews conducted by the Information Security Compliance Unit are in compliance with FISMA and its supporting regulations. However, the Board's information security control baseline states that its assessors' level of independence is determined by the risk level of the system for which they conduct security control assessments. Further, Board officials informed us that the decision to have the CISO office within the Division of IT was purposeful and that the CISO's ultimate responsibility for information security necessitated that they be the authorizing official of the identified systems. Although we did not find that security assessments have been conducted in a partial or biased manner, a lack of independence

[32] Office of Inspector General, *2017 Audit of the Board's Information Security Program*.

[33] Of the 47 systems, 40 are infrastructure systems and 7 are business applications.

[34] 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.

could compromise the unbiased nature and credibility of future security control assessments as the agency works to implement ongoing authorization processes.

Recommendation

We recommend that the CIO

4. Ensure that roles and responsibilities within the authorization process maintain a level of independence commensurate with the risk level of the information system.

Management Response

The CIO concurs with our recommendation and notes that a POA&M will be established to detail the steps the Board will take to address our recommendation.

OIG Comment

We plan to follow up on the steps outlined in the Board's POA&M to ensure that the recommendation is fully addressed.

Respond

The objective of the *respond* function in NIST's Cybersecurity Framework is to implement processes to contain the impact of detected cybersecurity events. Activities include developing and implementing incident response plans and procedures, analyzing security events, and effectively communicating incident response activities. Examples of the assessment areas in this security function, as outlined in DHS's *FY 2020 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 states that an incident response process consists of four key phases: preparation; detection and analysis; containment, eradication, and recovery; and postincident activity (table 3).[35] It further states that establishing an incident response capability should include creating an incident response policy and plan; developing procedures for performing incident handling and reporting; and establishing relationships and lines of communications between the incident response team and other groups, both internal and external to the agency.

[35] National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61, Revision 2, August 6, 2012.

Table 3. Key Incident Response Phases

Incident response phase	Description
Preparation	Establish and train the incident response team and acquire the necessary tools and resources.
Detection and analysis	Detect and analyze precursors and indicators. A *precursor* is a sign that an incident may occur in the future and an *indicator* is a sign that an incident may have occurred or is occurring currently.
Containment, eradication, and recovery	Contain an incident to limit its impact, gather and handle evidence, eliminate components of the incident, and restore affected systems to normal operations.
Postincident activity	Capture lessons learned to improve security measures and the incident response process.

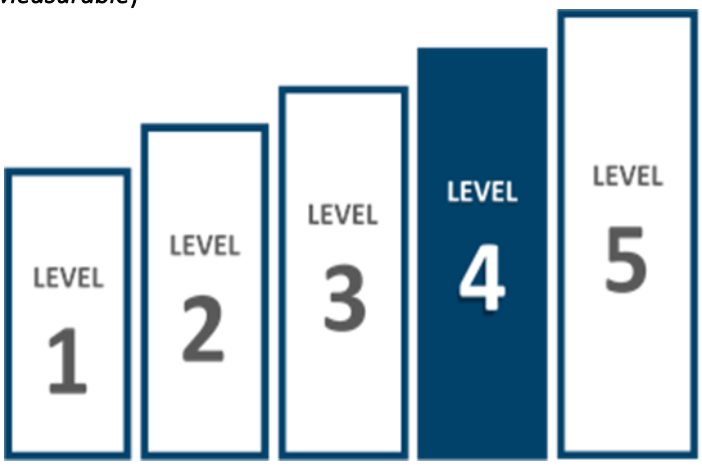
Source: NIST Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide.*

The Board's *Incident Response Program* documents the procedures for addressing the detection, response, and reporting of information security incidents related to Board data and resources. The procedures include scope, roles and responsibilities, incident notification and escalation tasks, external reporting requirements, and a threat vector taxonomy. The Board also uses the services of the National Incident Response Team, which is an IT service provider for the Federal Reserve System that administers intrusion detection, incident response, and security intelligence services.

Current Agency Maturity

As in 2019, we found that the Board's incident response program is operating effectively at a level-4 (*managed and measurable*) maturity (figure 12). For example, the Board continues to implement incident response metrics that are used to measure and manage the timely reporting of incident information to agency officials and external stakeholders. In addition, the Board effectively shares information on incident activities with internal stakeholders and ensures that security incidents are reported timely to the U.S. Computer Emergency Readiness Team; law enforcement; and, for major incidents, Congress.

Figure 12. Incident Response, Level 4 (*Managed and Measurable*)



Source: OIG analysis.

This year, we also found that the Board has continued to make improvements to the technologies supporting its incident response program. For example, the Board has incorporated additional data feeds into its existing incident response dashboards; as these data feeds have been adjusted and optimized, the number of false positives has decreased. Further, the Board is testing simulation technology to determine how its existing defenses would respond to a potential incident. Lastly, the Board has matured its incident response capabilities by implementing all iterations of DHS's EINSTEIN program.[36]

As noted earlier, the Board is working with DHS to deploy 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. For instance, tools offered through the CDM program could strengthen the Board's processes for analyzing the enterprisewide effect of potential security incidents and vulnerabilities. We believe that the implementation of CDM will further mature the agency's incident response program through greater integration with its vulnerability management processes. We will continue to monitor the Board's progress in implementing the tools offered through the CDM program as part of future FISMA reviews.

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 2020 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 (ICT) 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.[37] It highlights the importance of conducting a business impact analysis, which helps identify and prioritize information systems and components critical to supporting the organization's mission and business processes, as a foundational step to effective contingency planning. A business impact analysis allows an organization to measure priorities and interdependencies (internal or external to the entity) by risk

[36] DHS's EINSTEIN program detects and blocks cyberattacks from compromising federal agencies and provides DHS with situational awareness by using threat information detected in one agency to protect the rest of the government.

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

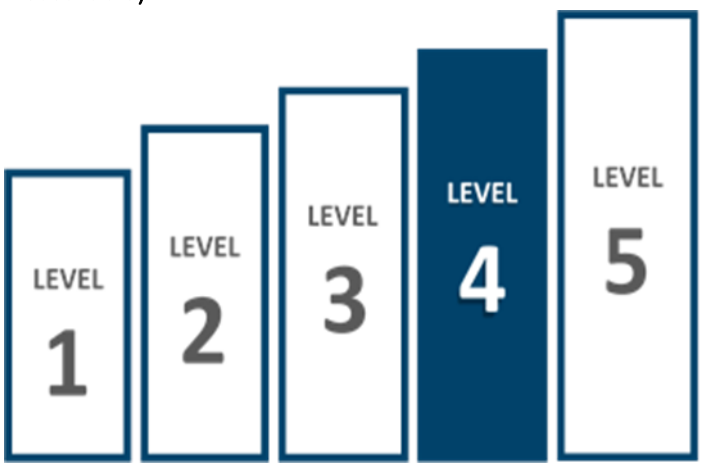
factors that could affect mission-essential functions. The information obtained from an agency's business impact assessment can serve as an important input to an organization's ERM program.

A key component of an effective contingency planning program is the consideration of risk associated with an organization's ICT supply chain. NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, highlights ICT supply chain concerns associated with contingency planning, including alternative suppliers of system components and services, denial-of-service attacks to the supply chain, and alternate delivery routes for critical system components.[38] In addition, in December 2018 the SECURE Technology Act was passed to strengthen agency supply chain risk management practices. The act establishes a Federal Acquisition Security Council to provide agencies with guidance related to mitigating supply chain risks in IT procurement and to establish criteria for determining the types of products that pose supply chain security risks to the federal government. The importance of supply chain risk management is also highlighted by its inclusion and enhanced focus in the recent update to the NIST Cybersecurity Framework. For example, with respect to contingency planning, the framework notes that response and recovery planning and testing should be conducted with suppliers and third-party providers.

Current Agency Maturity

As in 2019, we found that the Board's contingency planning program continues to operate effectively at a level-4 (*managed and measurable*) maturity (figure 13). Specifically, we noted that the Board has implemented processes to identify mission-essential functions and essential supporting activities within each of the agency's divisions. These division-level determinations are incorporated into an enterprisewide business impact analysis that is used to establish contingency planning requirements and priorities. Further, we found that the Board's enterprisewide, division-level, and information system contingency plans are tested consistently to ensure that they are performing as intended. The agency employs automated mechanisms to test system-level contingency plans, to the extent practicable, and documents any issues that are identified so they can be resolved and retested at a later date.

Figure 13. Contingency Planning, Level 4 (*Managed and Measurable*)



Source. OIG analysis.

[38] National Institute of Standards and Technology, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Special Publication 800-161, April 8, 2015. The guidance and controls in this special publication are recommended for use with high-impact systems according to Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*. However, according to NIST, because of interdependencies and individual needs, agencies may choose to apply the guidance to systems at a lower impact level or to specific system components.

We also noted that the Board coordinates its contingency exercises with several external stakeholders, including members of its ICT supply chain. A Board official charged with continuity-related responsibilities informed us that agency personnel continue to attend briefings regarding national supply chain risk efforts and that several discussions have been held with the Federal Reserve Banks regarding the development of a Systemwide approach to supply chain risk. This collaboration has resulted in increased information sharing related to hardware and software vendors; however, this work is in its early stages and will continue to evolve.

Further, as noted earlier, the Board is in the process of establishing an ERM program that will focus on addressing the full spectrum of the agency's significant risks by considering them as an interrelated portfolio. As it continues its work to implement ERM, the Board has an opportunity to further mature its contingency planning program by ensuring that it is fully integrated with the agency's ERM processes. This integration should help ensure that contingency planning considerations are incorporated into the Board's strategic and capital budget planning processes and are embedded into daily decisionmaking across the organization.

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 2020 IG FISMA Reporting Metrics*: *identify*, *protect*, *detect*, *respond*, and *recover*. These five function areas consist of eight security domains: risk management, configuration management, identity and access management, data protection and privacy, security training, ISCM, incident response, and contingency planning.

To assess the Board's information security program, we analyzed security policies, procedures, and documentation. In addition, we

- interviewed Board and Reserve Bank 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, as well as for a sample of five Board systems
- conducted specific testing of the security configurations of select agency network devices
- assessed access controls for the System's collaboration tools as they relate to the protection of Board information
- performed data analytics using a commercially available tool to support our testing in multiple security domains

To rate the maturity of the Board's information security program and functional areas, we used the scoring methodology defined in DHS's *FY 2020 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 April 2020 to September 2020. 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 2020 FISMA audit, we reviewed the actions taken by the Board to address the outstanding recommendations from prior FISMA audits. Below is a summary of the status of the 18 recommendations that were open at the start of our 2020 FISMA audit (table B-1). Based on corrective actions taken by the Board, we are closing 7 recommendations related to the risk management, configuration management, identity and access management, and data protection and privacy domains. The remaining 11 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 2021 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 reviews.

Table B-1. Status of 2016–2019 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 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 risk acceptance has not yet been documented.
2017	1	We recommend that the COO ensure that (a) an optimal governance structure for enterprise risk management 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.	Open	The Board continues to work toward its implementation of ERM. In the interim, the Board's SOC is serving as the agency's risk committee, as noted in the committee's charter; however, the Board has not yet defined a strategy that highlights the desired future state for ERM throughout the agency.

Year		Recommendation	Status	Explanation
2017	2	We recommend that the chief financial officer work with the CIO to ensure that the agency's standard contracting language includes the Board's security assurance requirements for third parties, as necessary.	Closed	Board Procurement and the Division of IT have developed and implemented a *Vendor Risk Management Standard*, which defines the security assurance requirements throughout each phase of the procurement process, as well as postaward continuous monitoring requirements for contracts. Further, the Board has updated its contract language to include security assurance and continuous monitoring requirements.
2017	3	We recommend that that the chief financial officer work with the CIO to evaluate applicable contracts with third-party providers to determine whether additional amendments are needed to ensure that the necessary security assurance requirements are referenced.	Closed	Board Procurement and the Division of IT have reviewed existing contracts to determine whether additional amendments were needed. Based on this review, the Board determined no additional amendments were necessary and documented its acceptance of the risk for all applicable contracts. The Board's *Vendor Risk Management Standard* ensures that the appropriate contract language will be used going forward.
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.	Open	The Board is working to implement its enterprisewide software and license management processes prior to updating its enterprise architecture to ensure that all applicable technologies across the organization are included. The associated review processes will be enforced agencywide as part of the SRB's expanded scope. Refer to the Risk Management section above for additional detail on the Board's software and license management processes.
2018	1	We recommend that that the CIO ensure that the Board's information security policy, procedure, standard, and process documentation is maintained to reflect changes to federal requirements and agency processes.	Closed	The Board has developed and implemented a process for reviewing and updating its information security policies. The Board tracks necessary policy updates and maintains a schedule to ensure that all polices are reviewed and updated on an annual basis. We observed evidence of the first group of policies scheduled for review with this new process.

Year	Recommendation		Status	Explanation
2018	2	We recommend that that the CIO ensure that all required inventory components, including the identification of PII as well as internal and external interconnections, are maintained for all Board and third-party systems.	Closed	The Board has taken steps to ensure that its vendor inventory is complete and its vendor risk management process identifies system interconnections. However, we identified inconsistencies in the Board's cloud inventory and are looking at this area in greater detail in a concurrent evaluation of the Board's adoption of cloud solutions.
2019	1	We recommend that the CIO develop comprehensive enterprisewide guidance for the inventory of software and associated licenses throughout the Board.	Open	The Board has expanded the scope of its SRB and associated review processes across the organization. The SRB has already begun to conduct reviews for divisions other than the Division of IT. However, Board officials informed us that work in this area, including additional guidance and process workflows, is ongoing and targeted for completion after the conclusion of our FISMA fieldwork.
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.	Open	As part of the Board's work to expand the scope of its SRB, the agency is working with divisions to develop an agencywide software catalog. This work is ongoing and is expected to be completed after the conclusion of our FISMA fieldwork.
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.	Open	The Division of IT has developed a spreadsheet to track program-level vulnerabilities and recommendations. However, we noted that this spreadsheet is not yet tracking all program-level vulnerabilities, nor does it document all required elements of a POA&M. Board officials informed us that work to transition all program-level recommendations into the Division of IT's spreadsheet is ongoing and expected to be completed after the conclusion of our FISMA fieldwork.

Year		Recommendation	Status	Explanation
Configuration management				
2018	3	We recommend that the CIO ensure that all of the Board's network devices are included in the agency's vulnerability scanning processes, as appropriate.	Closed	For the network devices identified during our original review, we found that the Board took action to ensure that its vulnerability scanning processes include the agency's network devices to the extent practicable. However, the Board also noted that several network devices were determined to be fragile, and the agency documented its acceptance of the risk associated with their exclusion from Board scanning processes.
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.	Open	The Board has developed a list of guiding principles for ICAM and the agency's vision for the future state of the program. However, the Board is in the process of developing an ICAM strategy and transition plan for how to achieve that desired future state.
2019	4	We recommend that the CIO ensure that all components of the Board's public-facing website that require user authentication have a complete and visible warning banner, as appropriate.	Closed	The Division of IT has worked with the Board's Legal Division to revise its standard warning banner language. Further, the Board has updated the subsystems accessible from its public website to include complete and visible warning banners.
Data protection and privacy				
2018	5	We recommend that the CIO develop and implement a process to (a) ensure that access controls for the Board's report-generating technology are maintained in both production and nonproduction environments based on the principles of need to know and least privilege and (b) remove reports from the Board's report-generating technology in both production and nonproduction environments when they are no longer needed.	Closed	The Board has implemented a process to maintain appropriate access controls for its report-generating technology. Further, the Board has implemented a process to remove reports from production and nonproduction environments that have not been accessed in 365 days.

Year	Recommendation		Status	Explanation
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, Federal Resrve System officials informed us that this project is in the design phase and technical details and testing details have not yet been discussed.
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 has made substantial progress in this area, including developing draft documentation, coordinating with stakeholders across the agency, and working to automate the process. This work is 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.	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.
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 implementation of the CDM program is ongoing but has been delayed because of the COVID-19 pandemic. Board officials informed us that they plan to develop an ISCM strategy upon implementation of CDM, as well as the completion of policy updates to incorporate requirements from the planned revision of NIST SP 800-53 and the NIST Cybersecurity Framework.

Source: OIG analysis.

Appendix C: Management Response

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

DIVISION OF
INFORMATION TECHNOLOGY

October 27, 2020

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 "2020 Audit of the Board's Information Security Program" prepared as part of your office's oversight responsibilities pursuant of the Federal Information Security Modernization Act of 2014 (FISMA). The report evaluates the Board of Governors of the Federal Reserve System (Board) regarding FISMA and related information security policies, procedures, standards, and guidelines. The report also addresses the remediation of 7 of 18 recommendations from prior FISMA audits that remained open at the start of the 2020 FISMA audit. We are pleased that your assessment continues to recognize that the Board operates a comprehensive and effective information security program and recognizes the progress we continue to make to enhance the program.

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 Plans of Actions and Milestones and review our status towards addressing these 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
Chief Information Officer

cc: Mr. Peter Sheridan
Mr. Ray Romero
Mr. Charles Young

www.federalreserve.gov

Abbreviations

BDM	Division of Board Members
CDM	Continuous Diagnostics and Mitigation
CIO	chief information officer
CISO	chief information security 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
ICAM	identity, credential, and access management
ICT	information and communications technology
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
POA&M	plan of action and milestones
PTA	privacy threshold analysis
SOC	Senior Officer Committee
SP 800-39	Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
SP 800-53	Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*
SP 800-128	Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
SP 800-137	Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
SP 800-137A	Special Publication 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*

SPII	sensitive personally identifiable information
SRB	Software Review Board
TIC	Trusted Internet Connections

Report Contributors

Khalid Hasan, Senior OIG Manager for Information Technology
Paul Vaclavik, OIG Manager, Information Technology
Joshua Dieckert, Senior IT Auditor
Chelsea Nguyen, Senior IT Auditor
Martin Bardak, IT Auditor
Melissa Fortson, IT Auditor
Nick Gallegos, IT Auditor
Alexander Karst, Senior Information Systems Analyst
Fay Tang, Statistician
Monica Cook, Forensic Auditor
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

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