Audit Report
2018-IT-B-017
October 31, 2018

Board of Governors of the Federal Reserve System

2018 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, 2018-IT-B-017, October 31, 2018

2018 Audit of the Board's Information Security Program

Findings

The Board of Governors of the Federal Reserve System's (Board) information security program is operating at a level-4 (*managed and measurable*) maturity, which indicates an overall effective level of security. For instance, the Board has enhanced its identity and access management program by requiring multifactor authentication for access to its network for all privileged and nonprivileged users. Further, the agency has implemented an effective security training program that includes phishing exercises and associated performance metrics.

The Board also has opportunities to mature its information security program in Federal Information Security Modernization Act of 2014 (FISMA) domains across all five security functions outlined in the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective. Similar to our 2017 audit, a consistent theme we noted is that the lack of an agencywide risk management governance structure and strategy, as well as the decentralization of information technology services, results in an incomplete view of the risks affecting the Board's security posture. Although the Board has taken steps to move toward an agencywide approach to risk management governance and information technology services, several security processes, such as asset management and enterprise architecture, have not yet been implemented agencywide.

Finally, the Board has taken sufficient action to close 4 of the 13 recommendations from our prior FISMA audits that remained open at the start of this audit. The closed recommendations relate to identity and access management, incident response, and contingency planning. We are leaving open 9 recommendations in the areas of risk management, configuration management, identity and access management, and information security continuous monitoring from our 2016 and 2017 FISMA audits. We will continue to monitor the Board's progress as part of future FISMA reviews.

Recommendations

This report includes six new recommendations designed to strengthen the Board's information security program in the areas of risk management, configuration management, data protection and privacy, and security training. In her response to our draft report, the Board's Chief Information Officer concurs with our recommendations and notes actions that are underway to strengthen the Board's information security program. We will continue to monitor the Board's progress on 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 its agency's information security program, practices, and controls for select systems. U.S. Department of Homeland Security 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, 2018-IT-B-017, October 31, 2018

2018 Audit of the Board's Information Security Program

Number	Recommendation	Responsible office
1	Ensure that the Board's information security policy, procedure, standard, and process documentation is maintained to reflect changes to federal requirements and agency processes.	Division of Information Technology
2	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.	Division of Information Technology
3	Ensure that all of the Board's network devices are included in the agency's vulnerability scanning processes, as appropriate.	Division of Information Technology
4	Ensure that documentation supporting the sanitization and disposal of all agency-owned electronic media is accurate and maintained in accordance with Board policy.	Division of Information Technology
5	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. b. remove reports from the Board's report-generating technology in both production and nonproduction environments when they are no longer needed.	Division of Information Technology
6	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.	Division of Information Technology

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

MEMORANDUM

DATE: October 31, 2018

TO: Distribution List

FROM: Peter Sheridan
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2018-IT-B-017: *2018 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 a select agency system; the detailed results of that review will be transmitted under a separate, restricted cover. 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 2018 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 actions have been or will be taken to address them. We have included your response as appendix B 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, Deputy Director, Division of Information Technology
Charles Young, Deputy Associate Director, Division of Information Technology
Tina White, Senior Manager, Compliance and Internal Control, Division of Financial Management

Distribution:
Donald V. Hammond, Chief Operating Officer
Ricardo A. Aguilera, Chief Financial Officer and Director, Division of Financial Management
Sharon Mowry, Chief Information Officer and Director, Division of Information Technology
Michell Clark, Director, Management Division

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 (Board) (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 its 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. This guidance directs IGs to evaluate the effectiveness of agency information security programs across a variety of attributes grouped into eight security domains. 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* (Cybersecurity Framework) (table 1).[2]

[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] The NIST Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise.

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

Security function	Security function objective	Associated FISMA IG 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,[a] 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 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

[a] The data protection and privacy domain was added to the annual IG FISMA reporting metrics in 2018. This domain includes metrics for assessing the effectiveness of the agency's privacy program, security controls to protect personally identifiable information, enhanced network defenses, responses to data breaches, and privacy awareness training.

FISMA Maturity Model

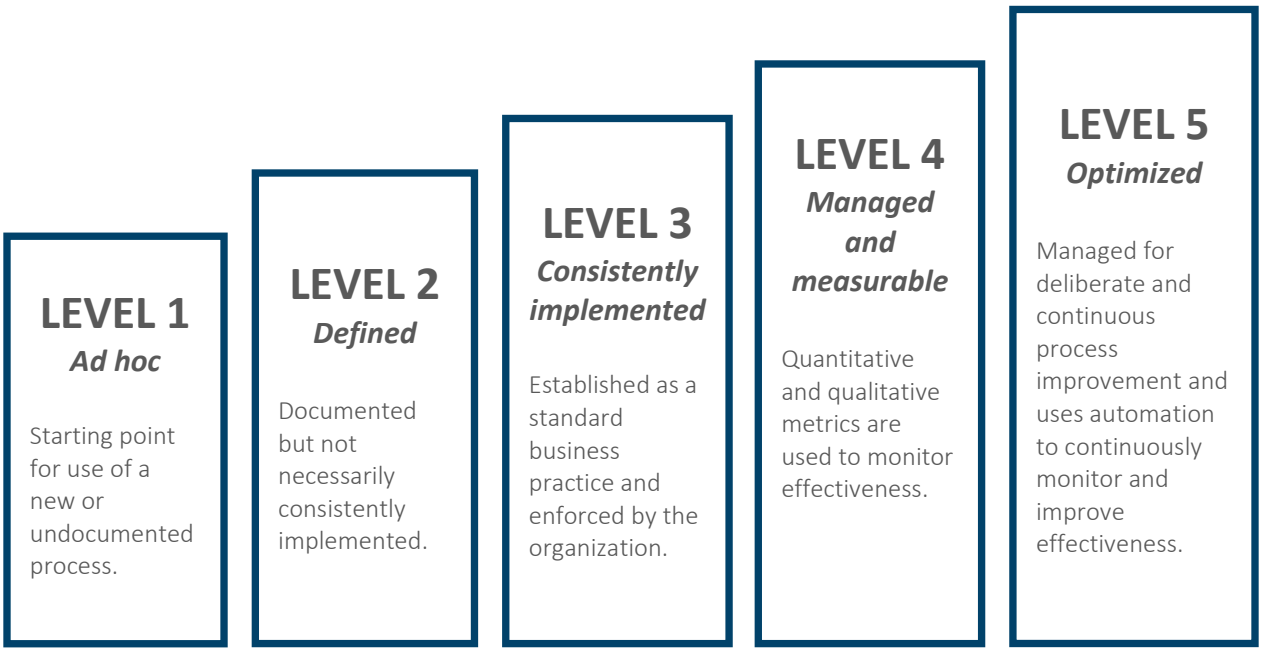
FISMA requires that IGs assess the effectiveness of information security controls that support the operations and assets of their respective agency. To that end, the Council of the Inspectors General on Integrity and Efficiency, in coordination with the Office of Management and Budget (OMB), DHS, and other key stakeholders, developed a maturity model intended to better address and report on the 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 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, level 4 (*managed and measurable*) represents an effective level of security.[3] This is the second year that all FISMA security domains will be assessed using a maturity model. Details on the scoring methodology for the maturity model are included in appendix A.

Figure 1. FISMA Maturity Model Rating Scale



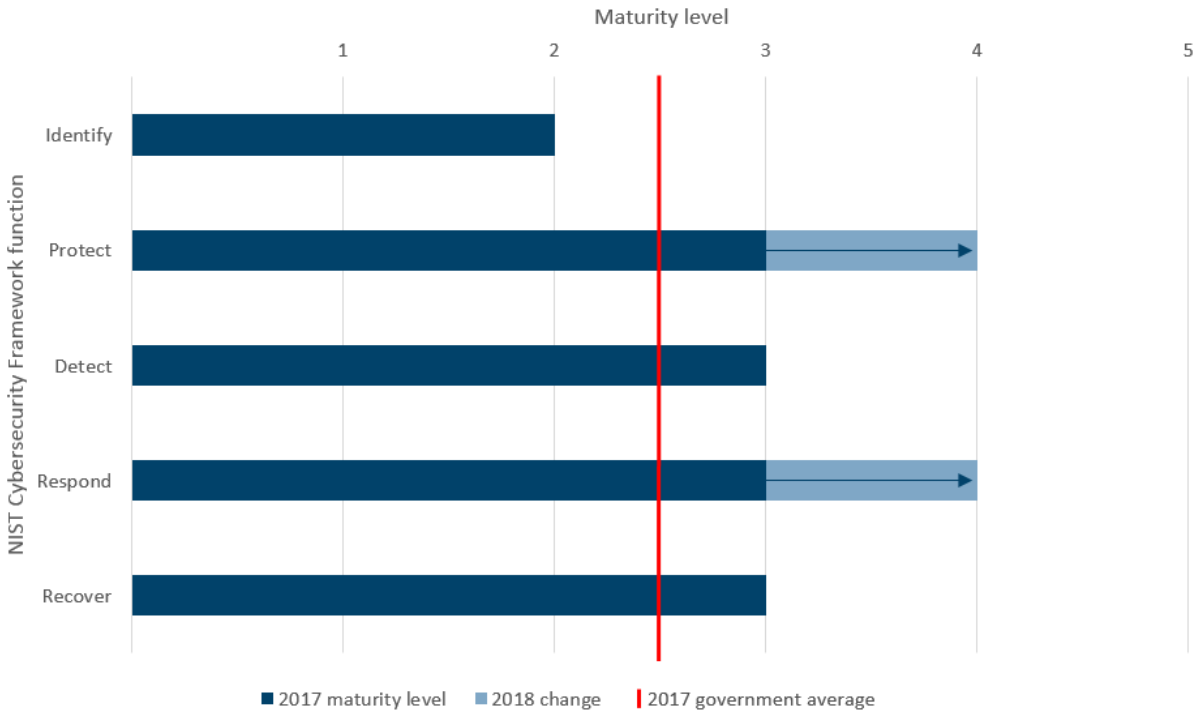
Source. OIG analysis of DHS IG FISMA reporting metrics.

[3] NIST Special Publication 800-53, Revision 4, *Security and Privacy of Controls for Federal Information Systems and Organizations*, 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.

Summary of Findings

The Board's information security program is operating at a level-4 (*managed and measurable*) maturity, which indicates an overall effective level of security (figure 2).[4] For instance, the Board has enhanced its identity and access management program by requiring multifactor authentication for access to its network for all privileged and nonprivileged users. Further, the agency has implemented an effective security training program that includes phishing exercises and associated performance metrics.

Figure 2. Maturity of the Board's Information Security Program



Source. OIG analysis.

As highlighted in table 2, the Board also has opportunities to mature its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective. Our report includes six recommendations in these areas as well as several items for management's consideration. Similar to our 2017 audit, a consistent theme we noted is that the lack of an agencywide risk management governance structure and strategy, as well as the decentralization of information technology (IT) services, results in an incomplete view of the risks affecting the security posture of the Board.[5] Although the Board has taken

[4] Appendix A of this report explains the scoring methodology used to determine the maturity of the Board's information security program.

[5] We have an ongoing evaluation of the Board's IT governance approach. The objective of the evaluation is to assess whether the Board's current organizational structure and authorities support its IT needs, specifically those associated with security, privacy, capital planning, budgeting, and acquisition.

steps to move toward an agencywide approach to risk management governance and IT services, several security processes, such as asset management and enterprise architecture, have not yet been implemented agencywide.

Table 2. Summary of Opportunities to Mature the Board's Information Security Program

Cybersecurity function area and IG FISMA reporting domain	Maturity rating	Opportunities for improvement
Identify		
Risk management	Level 2: *defined*	• Ensure that information security documentation is maintained to reflect changes to federal requirements and agency processes (2018 recommendation). • Ensure that all inventory components are maintained for all Board and third-party systems (2018 recommendation).
Protect		
Configuration management	Level 3: *consistently implemented*	• Ensure that all network devices, as appropriate, are included in the Board's vulnerability scanning processes (2018 recommendation). • Implement an identity, credential, and access management strategy as well as the organization's updated suitability policy (2017 recommendations). • Consistently maintain internal sanitization forms for the destruction of agency devices (2018 recommendation). • Enhance the security of sensitive personally identifiable information maintained in the Board's server-based report-generating software system (2018 recommendation). • Assess the knowledge, skills, and abilities of the Board's cybersecurity workforce (2018 recommendation).
Identity and access management	Level 4: *managed and measurable*	
Data protection and privacy	Level 3: *consistently implemented*	
Security training	Level 4: *managed and measurable*	
Detect		
Information security continuous monitoring (ISCM)	Level 3: *consistently implemented*	• Develop and implement an ISCM strategy that includes performance measures to gauge the effectiveness of related processes and provides agencywide security status (2017 recommendation).
Respond		
Incident response	Level 4: *managed and measurable*	• Consider methods to further integrate the Board's vulnerability management processes with its incident response function (2018 matter for management's consideration).
Recover		
Contingency planning	Level 3: *consistently implemented*	• Consider information and communications technology supply chain risks as a part of the Board's contingency program (2018 matter for management's consideration).

Source. OIG analysis.

In addition, the Board has taken sufficient action to close 4 of the 13 recommendations from our prior FISMA audits that remained open at the start of this audit. The closed recommendations relate to identity and access management, incident response, and contingency planning. We are leaving open 9 recommendations in the areas of risk management, configuration management, identity and access management, and information security continuous monitoring (ISCM) from our 2016 and 2017 FISMA audits. We will continue to monitor the Board's progress in addressing these open recommendations as part of future FISMA reviews.

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

The Board's overall information security program is operating effectively at a level-4 (*managed and measurable*) maturity. Although the agency has strengthened its program since our 2017 FISMA report, it has further opportunities to ensure that its information security program is effective across specific FISMA domains in all five Cybersecurity Framework security functions: *identify*, *protect*, *detect*, *respond*, and *recover*.

Identify

The objective of the *identify* function in the 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.

Risk Management

FISMA requires federal agencies to provide information security protections commensurate with their risk environment. Risk management refers to the program and supporting processes used to manage risk to organizational operations, assets, and individuals. This includes establishing the context for risk-related activities, assessing risks, responding to risks, and monitoring risks over time. NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, states that managing risk is a complex, multifaceted activity that requires the involvement of the entire organization. To accomplish this, risk management must be addressed at the enterprise, mission and business process, and information system levels.

Enterprise risk management (ERM) is an area that has seen increased emphasis in the federal government. It refers to an effective agencywide approach to addressing the full spectrum of the agency's external and internal risks. OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, provides guidance for implementing an ERM capability and governance structure that is coordinated with strategic planning and internal control processes.[6]

As part of the ERM governance structure, OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires that agencies designate a senior accountable official for risk management. This official is responsible for (1) ensuring that risk management processes are aligned with strategic, operational, and budgetary planning processes and (2) reporting to DHS and OMB on risk management decisions and the agency's

[6] Although OMB Circular A-123 is not directly applicable to the Board, other agencies, such as nonexecutive agencies, are encouraged to adopt the circular.

plan to implement the NIST Cybersecurity Framework. In addition to a governance structure, the development of an agencywide risk context is a key component of ERM. Other key components of ERM include defining risk appetite and risk tolerance levels, a risk management strategy, and a risk profile (table 3).

Table 3. Key Components of ERM

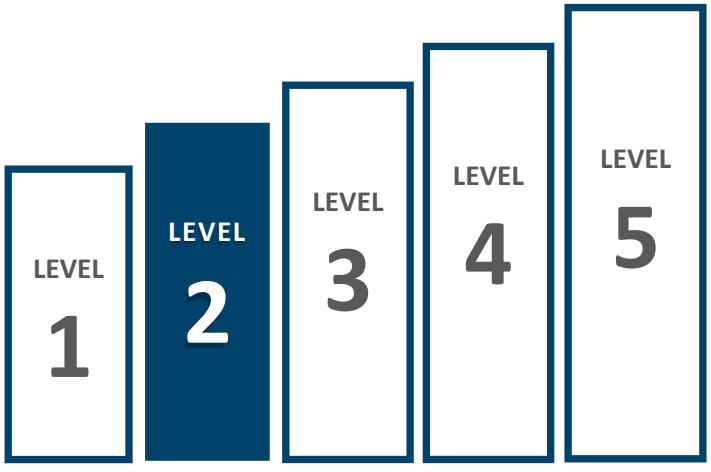
ERM component	Description
Risk context	An initial component of risk management that describes how an organization frames risk. Establishing the risk context includes defining the organization's risk appetite and tolerance levels.
Risk appetite	The broad-based amount of risk an organization is willing to accept in pursuit of its mission and vision. It is established by the organization's senior-most leadership and serves as the guidepost to set strategy and select objectives.
Risk tolerance	The acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective, or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.
Risk management strategy	Outlines how the organization intends to assess, respond to, and monitor risk.
Risk profile	Provides an analysis of the risk that an agency faces toward achieving a strategic objective and identifies appropriate options for addressing significant risks.

Source. NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*; OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.

Current Security Posture

Similar to last year, we found that the Board's risk management program continues to operate at level 2 (*defined*) (figure 3). However, the agency is performing several activities indicative of a higher maturity level. For instance, the Board has consistently implemented its tailored security control baseline as well as its processes for reviewing plans of action and milestones (POA&Ms), which are both associated with a level-3 maturity. In addition, the Board has further matured its POA&M process by incorporating

Figure 3. Risk Management, Level 2 (*Defined*)



Source. OIG analysis.

qualitative and quantitative performance measures into its process to better assess the effectiveness of associated risk management activities.

Opportunities for Improvement

Although the Board has consistently implemented processes for many of its risk management activities, we found that improvements are needed regarding the maintenance of security documentation and the agency's system inventory. We found that several of the Board's policy, procedure, standard, and process documents have not been regularly reviewed and updated. As a result, several of these documents contain information that is out of date and that does not reflect changes that have occurred throughout the Board's information security program and processes.

For example, with regard to the agency's security categorization of infrastructure systems, the Board's *Risk Management and Risk Assessment Standard* notes that infrastructure systems have a moderate default risk impact level. However, the Board's *Information Security Program and Policies*, *Information System Inventory Standard*, and *Security Categorization of Board Systems Guide* state that systems are to be assigned an overall risk impact rating based on the confidentiality, impact, and availability for the information collected by the system; these documents do not define any exceptions for infrastructure systems. Further, the Board *POA&M Standard* notes that POA&Ms should be updated at least semiannually; however, the agency's *Continuous Monitoring Standard* defines the POA&M update frequency as no less than annually and the Board's moderate information system control baseline requires POA&M updates quarterly. We believe that these inconsistencies are the result of the current time lag between changes to the Board's information security processes and the review of its policies, procedures, and standards to reflect those changes. Policies and procedures that are consistent and regularly updated will enable more-effective implementation of the Board's information security program.

Further, we found opportunities to improve the Board's process for inventorying the types of data and interconnections maintained for its information systems. The Board has moved from a manual system inventory process to one that uses its two FISMA compliance tools to maintain the details of its system inventory. Information on the interconnections and the data types for each system are contained in the system security plans maintained in these FISMA compliance tools. However, we found that the agency's infrastructure systems are not required to complete all components of the security plan, including the identification of personally identifiable information (PII) and interconnections with other systems through which PII is shared.[7] In addition, we found that not all third-party systems are included in either of the agency's FISMA compliance tools.

FISMA requires that inventories of information systems include an identification of the interfaces between each subsystem and all other systems or networks, including those not operated by or under the control of the agency. Consistent with FISMA, the Board's *Information Security Program and Policies* also notes that the agency will maintain an inventory of all information systems, including infrastructure

[7] NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, defines PII as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

components and business applications, that specifies the interfaces between systems and networks. We believe that these issues are the result of two factors. First, the Board's policy does not require infrastructure systems to complete all components of the security plan in its compliance tools. This information, however, was previously being captured in the agency's manual system inventory process. Second, the Board is in the process of verifying its inventory of third-party systems, including those operated or maintained within the Federal Reserve System. Further, Board officials informed us that the agency is in the process of implementing DHS's Continuous Diagnostics and Mitigation (CDM) program, which will help strengthen the agency's asset management and system inventory processes.[8] We believe that a complete system inventory will enable a more-effective risk-based implementation of security controls as well as provide more visibility into the types of data maintained by the agency.

In addition to these issues, we made several recommendations in prior FISMA reports related to the Board's risk management activities. Specifically, in our 2016 FISMA audit report, we recommended 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 the types of information maintained by the Board.[9] In 2017, a draft strategy was created, but it was not finalized because the Board was prioritizing updates to its suitability program and processes. This year, the Board finished drafting its suitability policy and completed its insider threat policy for classified information. However, at the time of our review, we found that the agency has not yet determined which insider threat activities are applicable to the sensitive but unclassified information maintained by the Board. Therefore, we are leaving this recommendation open and will continue to monitor the Board's progress in this area as part of our future audit activities.

Our 2017 FISMA audit report includes a recommendation that the COO ensure that (1) an optimal governance structure for ERM is implemented that includes considerations for a Chief Risk Officer or equivalent function and (2) an ERM strategy is used to maintain a risk profile for the Board.[10] This year, we found that although the Board has begun to develop a strategy and governance structure for ERM, the implementation of this framework, including the development of the agency's risk profile, is still in progress. Therefore, we are leaving this recommendation open and will continue to monitor the Board's progress in this area as part of our future audit activities.

Our 2017 FISMA audit report also includes two recommendations regarding the Board's risk management processes for third-party providers. Specifically, we recommended that the Chief Financial Officer work with the CIO (1) to ensure that the agency's standard contracting language includes the Board's security assurance requirements for third parties, as necessary, and (2) 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. This year, Board officials informed us that they are working to develop a policy regarding security assurance requirements for third-party providers

[8] Provided by DHS, the CDM program is designed to provide federal agencies with capabilities and tools to identify cybersecurity risks on an ongoing basis and prioritize these risks based on potential impacts. CDM offers commercial off-the-shelf tools to support technical modernization as threats change, as well as provide an agency dashboard and customized reports to alert network managers of their most critical cybersecurity risks.

[9] Office of Inspector General, *2016 Audit of the Board's Information Security Program*, OIG Report 2016-IT-B-013, November 10, 2016.

[10] Office of Inspector General, *2017 Audit of the Board's Information Security Program*, OIG Report 2017-IT-B-018, October 31, 2017.

as well as reviewing existing third-party contracts. In addition, POA&Ms are being developed for contracts that require updates; however, this process had not yet been completed at the time of our review. As such, we are leaving these two recommendations open and will follow up on the Board's progress in these areas as a part of future audit activities.

Recommendations

We recommend that the CIO

1. Ensure that the Board's information security policy, procedure, standard, and process documentation is maintained to reflect changes to federal requirements and agency processes.
2. 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.

Management's Response

In her response to our draft report, 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.

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.

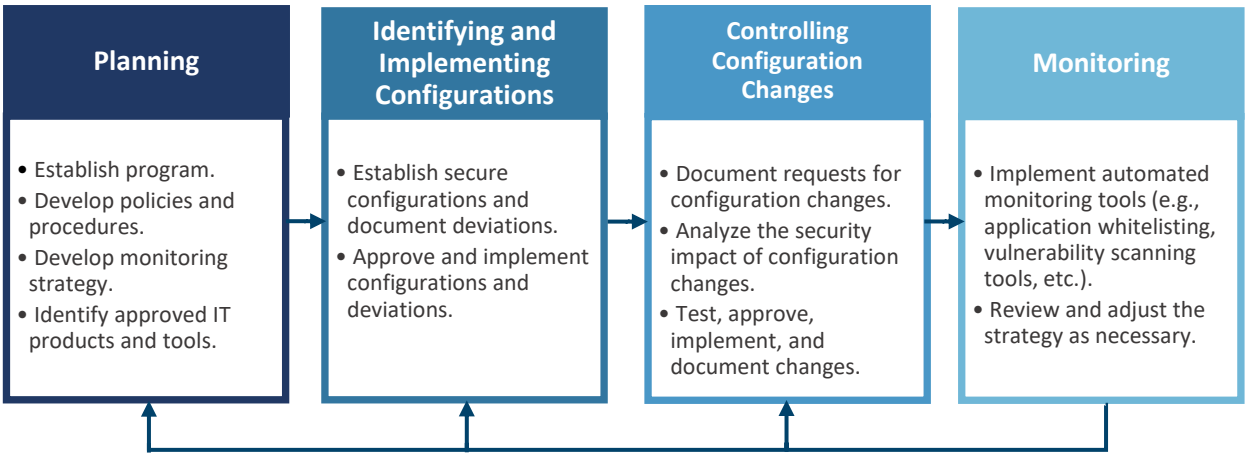
Protect

The objective of the *protect* function in the Cybersecurity Framework is to develop and implement safeguards to secure information systems. This function supports the ability to prevent, limit, or contain the impact of a cybersecurity event through applicable configuration management, identity and access management, data protection and privacy, and security training processes.

Configuration Management

FISMA requires agencies to develop 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. Security-focused 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 4).

Figure 4. Security-Focused Configuration Management Phases



Source. NIST SP 800-128.

A key component of security-focused configuration management is monitoring, which involves validating that information systems are adhering to organizational policies, procedures, and approved secure configuration baselines. SP 800-128 notes that organizations are encouraged to perform scanning activities to discover network components not recorded in the inventory as well as identify potential disparities between the approved configuration baselines and the actual configuration for an information system. Vulnerability scanners are commonly used in organizations to identify known vulnerabilities on hosts and networks and on commonly used operating systems and applications. These scanning tools can proactively identify vulnerabilities, provide a fast and easy way to measure exposure, identify out-of-date software versions, validate compliance with an organizational security policy, and generate alerts and reports about identified vulnerabilities. Further, SP 800-128 states that organizations should review configuration changes for consistency with an organizational enterprise architecture.

Current Security Posture

Last year, we found that that the Board's configuration management program was operating at level 3 (*consistently implemented*). For 2018, although we determined that the agency has taken several steps to mature its processes in this area, we found that the Board's configuration management program continues to operate at level 3 (*consistently implemented*), with the agency performing several, but not all, recommended activities indicative of higher maturity levels (figure 5). For instance, the Board employs network access controls and application whitelisting to detect unauthorized hardware and

Figure 5. Configuration Management, Level 3 (*Consistently Implemented*)

Source. OIG analysis.

software on the network. We also found that the Board tracks performance metrics to measure the effectiveness of its change control processes, which is associated with a level-4 maturity. Further, the agency uses several configuration management tools to automatically enforce and redeploy configuration settings at regular intervals.

Opportunities for Improvement

We found opportunities to improve the Board's vulnerability scanning processes by ensuring that all network devices are being assessed.[11] Although the Board performs vulnerability scanning on various technologies and devices within its environment, agency officials informed us that they have chosen not to scan certain devices to limit any impact on the availability of the devices. However, we believe that the performance of periodic vulnerability scans of all of the Board's network devices will provide the organization with greater assurance that these devices are securely configured.

In addition to vulnerability scanning, security-focused configuration management activities also include the consistent use of approved IT products and tools through the implementation of an enterprise architecture. Our 2017 FISMA report recommended that the CIO ensure that the Board's enterprise architecture includes technologies managed by all divisions, and that the CIO work with the COO to enforce associated review processes agencywide. Although we found that the agency has taken steps to identify approved IT tools in all divisions, the Board is still working to integrate its enterprise architecture and review processes for each domain into one agencywide approach. Therefore, we are leaving this recommendation open at this time and will continue to monitor the Board's progress in this area as part of our future audit activities.

In addition, our 2016 FISMA report recommended that the CIO develop and implement a plan to transition the Board's external network to a Trusted Internet Connections service provider and use the services offered by DHS's EINSTEIN program, as appropriate.[12] Although the Board has taken steps to meet the goals of the Trusted Internet Connections initiative with the implementation of EINSTEIN 3 Accelerated, the agency is still in the process of transitioning its external network to a Trusted Internet Connections service provider. Therefore, we are leaving this recommendation open at this time and will continue to monitor the Board's progress in this area as part of our future audit activities.

Recommendation

We recommend that the CIO

3. Ensure that all of the Board's network devices are included in the agency's vulnerability scanning processes, as appropriate.

[11] We provided details on the specific devices that are referenced to Board officials in a separate communication.

[12] 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. DHS's EINSTEIN 3 Accelerated program, like its predecessors EINSTEIN 1 and EINSTEIN 2, provides further enhancements to participating agencies' capabilities to perform cybersecurity analysis, situational awareness, and security response. The EINSTEIN 3 Accelerated program accomplishes this by using major internet service providers that provide intrusion prevention security services for federal civilian agencies using widely available commercial technology to both detect cyberattacks targeting federal civilian government networks and actively prevent potential compromises.

Management's Response

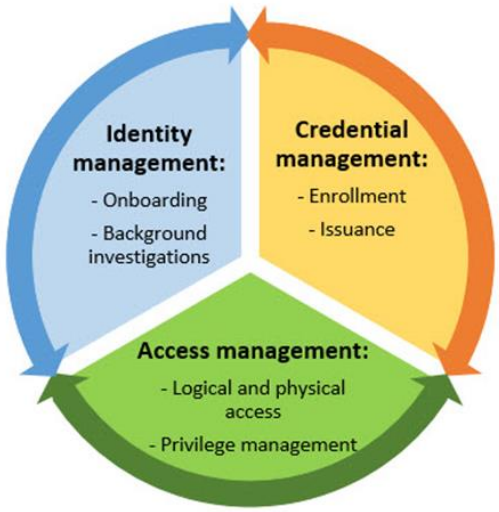
In her response to our draft report, the CIO concurs with our recommendation and notes that a POA&M will be established to detail the steps the Board will take to address our recommendation.

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.

Identity and Access Management

Figure 6. ICAM Conceptual Design



Source. CIO Council, *Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance.*

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 6).

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 Roadmap and Implementation Guidance* to provide the government with a common framework and implementation guidance to plan and execute ICAM programs. 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.

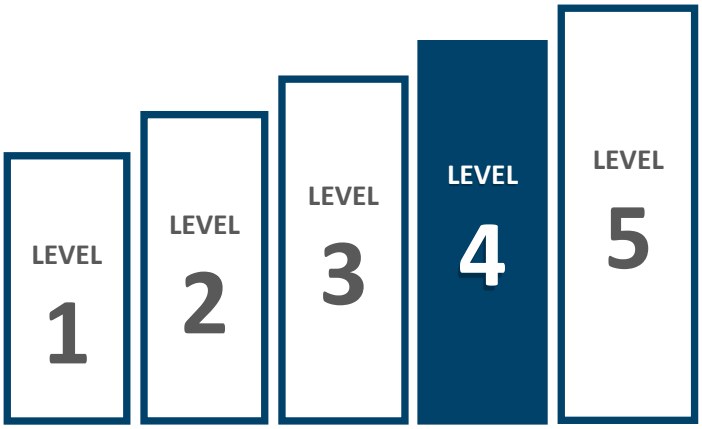
The Board's information security policies and procedures cover multiple ICAM functions throughout the life cycle of a user's digital identity. For example, the Board conducts background investigations to determine an individual's suitability to be employed in certain positions or to obtain access to certain types of information. The scope of a background investigation depends on the nature of an individual's work and the degree to which that work affects the security and effectiveness of Board operations. Further, users with access to the Board's network and data are required to read, understand, and agree to the agency's permissible use policy and rules of behavior as a part of their annual security awareness

training. Individuals who are granted access to classified information are required to sign a nondisclosure agreement.

Current Security Posture

In 2017, the Board's ICAM program was operating at level 3 (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level. This year, the Board is operating effectively at level 4 (*managed and measurable*), having matured multiple aspects of its ICAM program since last year (figure 7). For instance, as noted below, the Board requires multifactor authentication for access to its network. Further, the agency is in the final stages of piloting its personal identity verification (PIV) card–based solution for remote access and is working toward integrating this solution with its enterprise single-sign-on capability for agency systems.

Figure 7. Identity and Access Management, Level 4 (*Managed and Measurable*)



Source. OIG analysis.

As part of our 2016 FISMA audit report, we recommended that the CIO develop and implement an identity and access management plan that includes a risk-based determination for how multifactor authentication will be implemented for nonprivileged users. Last year, we noted that the Board had made multifactor authentication available as an option for nonprivileged users; however, the policy could not be fully implemented due to compatibility issues with some systems. This year, however, we found that the agency has completed its rollout of multifactor authentication for nonprivileged users to every division across the Board. As such, we are closing this recommendation.

In addition, our 2017 FISMA audit report included two recommendations regarding the Board's suitability policy. Specifically, we recommended that the COO work with the agency's divisions to update the suitability policy to include requirements for assigning risk and sensitivity designations and associated investigative requirements to Board positions. Further, we recommended that the Management Division ensure that the updated suitability policy is implemented and that investigations are conducted in accordance with the new policy. This year, we found that the Board has finalized its update to the suitability policy, which now includes risk and sensitivity designations assigned to each position within the agency. Therefore, we are closing the recommendation regarding the policy update. However, Board officials informed us that personnel screening in accordance with the new policy will not begin until 2019. As such, we are keeping open the recommendation regarding the performance of personnel screening investigations.

Opportunities for Improvement

The Board has taken several steps to mature its ICAM program. However, for a select system that we reviewed, we found inconsistencies in the implementation of the principle of least privilege. We found

several instances in which system users were provisioned roles with identical sets of privileges. For example, we identified multiple system roles that provided the same system capabilities to both regular and administrative user accounts. This condition may impact the ability to trace specific actions back to users and make it difficult to effectively manage user permissions. Board officials attribute this condition to the system's mirroring of group membership in Active Directory.

In 2016, we assessed select security controls for the Board's Active Directory environment and made recommendations related to this issue.[13] As such, we are not making additional recommendations in this report and will continue to follow up on the Board's actions in this area as part of future audits. Further, given the number of Board systems that inherit access controls from Active Directory, we believe these issues may be applicable to other systems throughout the agency.

Our 2017 FISMA audit report included a recommendation that the CIO develop and implement an agencywide ICAM strategy. Elements of an ICAM strategy include an assessment of the current state of activities as presently performed, a vision for the desired target state, and a plan to bridge any gaps between the two. Although the Board has improved the effectiveness and automation associated with several ICAM processes, including mandating the use of PIV credentials for nonprivileged users, these activities were not guided by an enterprisewide ICAM strategy. Board officials informed us that they are waiting to complete their ICAM strategy until OMB publishes new ICAM requirements, which are anticipated for release later this year. This new ICAM guidance will include requirements around the implementation of effective governance, the modernization of ICAM capabilities, and potential shared solutions and services. Therefore, we are leaving this recommendation open and will continue to monitor the Board's progress in this area as part of our future audit activities.

Data Protection and Privacy

Data protection and privacy refers to a collection of activities focused on the security objective of confidentiality, preserving authorized restrictions on information access, and disclosure to protect personal privacy and proprietary information.[14] In today's digital world, effectively managing the risk to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their PII increasingly depends on the safeguards employed for the information systems that process, store, and transmit the information. As such, OMB Circular A-130, *Managing Information as a Strategic Resource*, requires 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. Executive Order 13719, *Establishment of the Federal Privacy Council*, requires agency heads to designate a senior agency official for privacy who has agencywide responsibility and accountability for the agency's privacy program.

NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (SP 800-122), 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. Further, SP 800-122 recommends measures to protect PII and other sensitive information, including operational safeguards (for example,

[13] Office of Inspector General, *Security Control Review of the Board's Active Directory Implementation*, OIG Report 2016-IT-B-008, May 11, 2016.

[14] The data protection and privacy domain was added to the annual IG FISMA reporting metrics in 2018.

policies, procedures, and awareness training); privacy-specific safeguards (for example, minimizing the use, collection, and retention of PII); and security controls (for example, access control to PII, media sanitization, and the protection of data at rest or in transit).

Current Security Posture

The Board's data protection and privacy program is operating at level 3 (*consistently implemented*) (figure 8). In 2017, the Board began to develop an agencywide privacy program in accordance with guidance from OMB and NIST. This year, we found that the Board has made significant progress in defining and communicating its privacy program, including roles and responsibilities, resources, and the optimal governance structure with which to effectively implement the program. The Board has also developed policies and procedures for the protection of the PII that is collected, used, maintained, shared, or disposed of by the agency, including through its information systems. These policies and procedures include controls for the encryption of data at rest and in transit, as well as the limitation of data transfer to removable media. Further, the Board uses a data loss prevention solution to monitor the transfer of sensitive information outside the agency's network.[15] The Board has also defined a process for sanitizing and disposing of all agency hardware assets containing agency information and has implemented a data breach response plan that identifies the Board's data breach response team, documents the processes and procedures for data breach notification, and outlines the necessary actions to be taken in the event of a data breach.

Figure 8. Data Protection and Privacy, Level 3 (*Consistently Implemented*)

Source. OIG analysis.

Opportunities for Improvement

Although the Board has made progress in the development and implementation of an agencywide privacy program, we identified two areas where improvements are needed to better protect the agency's sensitive privacy data and ensure that the program is effective. These areas are (1) the maintenance of electronic media sanitization records and (2) the access controls in place for one of the Board's report-generating tools.

[15] *Data loss prevention* refers to a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. Data loss prevention solutions are designed to prevent end users from accidentally or maliciously sharing data that could put the organization at risk.

During our audit, we identified opportunities to strengthen the Board's media sanitization processes of agency-owned electronic media.[16] Specifically, although the Board uses a third-party vendor to sanitize its electronic media, it was unable to produce documentation confirming the disposal of 57 of the 471 items (12.1 percent) listed in the vendor's invoice and inventory report.[17] The Board has developed a *Media Disposal Procedure* that outlines the steps to be taken to properly sanitize and dispose of the agency's media. These steps include the completion of an internal Information Sanitization Form that list the assets to be destroyed, the verification and preparation of assets to match those listed on the completed form, the oversight of media destruction by the vendor, and the retention of the form on an agency shared drive. Board officials informed us that although the agency oversees the vendor's destruction of digital media, the agency does not reconcile its internal documentation with the vendor's invoice and inventory report after the job has been completed. We believe that a process to verify that the Board's internal Sanitization Forms align with the invoice and inventory reports provided by the vendor will provide greater assurance that all of the organization's digital media is appropriately sanitized and destroyed.

Finally, for a report-generating technology used by the Board, we found that access controls were not implemented in accordance with the principles of need to know and least privilege. As a result, sensitive PII and other information was available in both production and nonproduction environments to those without a need for the data. We believe that this condition exists for two key reasons. First, the Board was not monitoring the access control settings to the folders and reports contained in this report-generating technology. Second, the Board did not have a consistent process to remove database folders and reports that were no longer needed. SP 800-122 notes that organizations should regularly review holdings of previously collected PII to determine whether the data are still relevant and necessary for meeting the organization's business purpose and mission. If the PII is no longer relevant or necessary, the data should be properly destroyed. Finally, the Board was using production data from these reports in a nonproduction environment without ensuring that the required access controls were implemented.

To accomplish its mission, the Board maintains sensitive PII on foreign nationals, and as such, there may be non-U.S. regulations that may impact the protection of this information. One such regulation is the European Union's General Data Protection Regulation, which includes protections for personal data of EU citizens regardless of where the processing of the data takes place or where the business that is processing the data is located. As such, we believe that the Board should consider the effect of these regulations as it matures its privacy program.

Recommendations

We recommend that the CIO

4. Ensure that documentation supporting the sanitization and disposal of all agency-owned electronic media is accurate and maintained in accordance with Board policy.

[16] NIST Special Publication 800-88, Revision 1, *Guidelines for Media Sanitization*, defines *media sanitization* as the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. *Media* refers to either hard-copy or electronic representations of information, such as paper, hard drives, and flash drives.

[17] The 471 devices includes all Board-owned electronic media sanitized in May 2018.

5. 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.

    b. remove reports from the Board's report-generating technology in both production and nonproduction environments when they are no longer needed.

Management's Response

In her response to our draft report, 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.

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.

Security Training

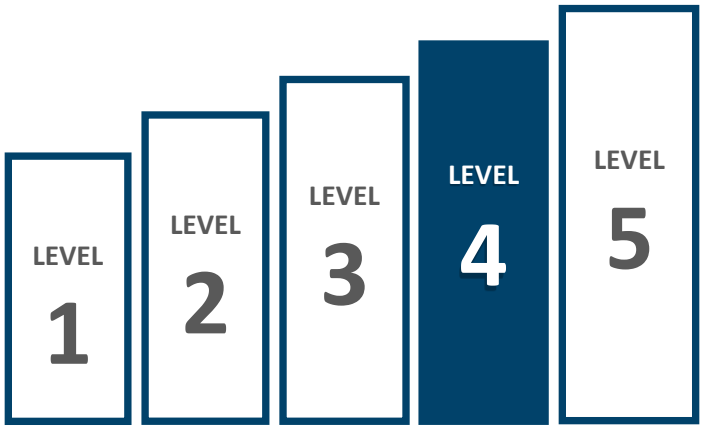
FISMA requires agencies to develop an information security program that provides security awareness training to personnel, including contractors, who support the operations and assets of the organization, as well as role-based training for individuals with significant information security responsibilities. 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. As such, a robust, enterprisewide security awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them.

In accordance with FISMA requirements, the Board's information security program notes that all employees and contractors with access to agency information systems must receive security awareness training before being permitted access to the Board 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 be maintained.

Current Security Posture

Similar to last year, we found that the Board's security awareness training program continues to operate effectively at level 4 (*managed and measurable*) (figure 9). 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, and security incident reporting. Further, the agency conducts regular phishing exercises, targeting all of the agency's users and tracking metrics on the effectiveness of the exercise through the use of a tool to report suspicious emails. Board officials routinely report the results of their phishing exercises to the agency's Information Security and Privacy Committee and track repeated user failures to gauge the effectiveness of the exercises and provide additional training, as necessary.

Figure 9. Security Training, Level 4 (*Managed and Measurable*)



Source. OIG analysis.

Opportunities for Improvement

Although the Board provides specialized security training to Board staff with significant security responsibilities, it has not established an agencywide process for assessing the knowledge, skills, and abilities of its personnel who hold cybersecurity-related positions. The Federal Cybersecurity Workforce Assessment Act of 2015 requires federal agencies to conduct and report to Congress a baseline assessment of their existing workforce. To help implement these requirements, NIST published the *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework* in August 2017. The framework provides a resource to support a workforce capable of meeting an organization's cybersecurity needs, providing guidance for leaders to better understand, inventory, and track strengths and gaps in their cybersecurity workforce's knowledge, skills, and abilities.

Board officials informed us that the agency is prioritizing other aspects of its information security program, such as its ERM framework and its implementation of the CDM program. Further, not all individuals performing cybersecurity responsibilities report to the CIO or to the Information Security Officer due to the decentralized nature of the agency's IT security workforce. However, we believe that regularly performing assessments of its cybersecurity workforce will allow the Board to more easily identify critical knowledge gaps for individuals with significant security responsibilities and provide additional security awareness and training as needed.

Recommendation

We recommend that the CIO

6. 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.

Management's Response

In her response to our draft report, 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.

Detect

The objective of the *detect* function in the 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, knowledge of threats, and security control effectiveness.

Information Security Continuous Monitoring

ISCM refers to the process of maintaining 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 for Federal Information Systems and Organizations* (SP 800-137). 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, 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 notes 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.

Current Security Posture

Figure 10. ISCM, Level 3 (*Consistently Implemented*)

Source. OIG analysis.

Similar to last year, we found for 2018 that the Board's ISCM program is operating at level 3 (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level (figure 10). For instance, the Board has developed and 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 captures metrics on IT security operations. These metrics include activities related to incident response functions, phishing exercises, user activity and travel violations, web traffic, and data loss prevention.

Opportunities for Improvement

Although we found that the Board is manually capturing several ISCM-related operational metrics, it has opportunities to mature its ISCM program through further automation. Similar to the agency's inventory of systems noted above, the Board maintains data regarding its system authorizations and other ISCM-related functions in two FISMA compliance tools. One of these tools has the capability to aggregate system data to provide performance measures and dashboards; however, the decentralization of this data into two tools hinders the Board's ability to deliver persistent situational awareness and assess security risks across the organization.

We believe that this situation is due to two key contributing factors. First, as noted in the risk management section above, the Board has not yet implemented its ERM strategy or defined an organizational risk tolerance and risk appetite level. As noted earlier, 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. This year, we found that the Board is in the process of establishing an ERM strategy and supporting governance structure. Second, the Board has not yet developed an agencywide ISCM strategy that defines specific metrics to gauge the security status of the enterprise. In our 2017 FISMA report, we recommended 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. This year, Board officials informed us that completing an ISCM strategy will depend on the agency's implementation of the CDM program. Board officials informed us that they are actively working with DHS regarding the agency's implementation of the CDM program, which is currently slated to begin in 2019. Therefore, we are leaving this recommendation open at this time, and we will continue to monitor the Board's progress in this area as part of our future audit activities.

Respond

The objective of the *respond* function in the 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.

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 main phases: preparation; detection and analysis; containment, eradication, and recovery; and postincident activity (table 4). It further notes 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.

Table 4. 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.

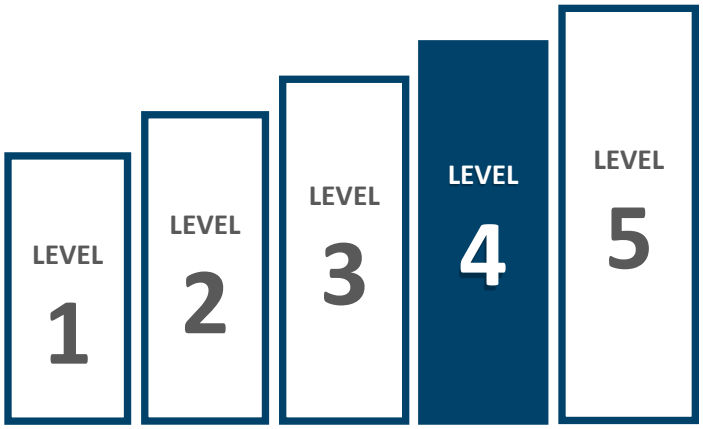
Source. NIST Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide.*

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 Security Posture

In 2017, the Board's incident response program was operating at level 3 (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level. This year, however, we found that the Board is operating effectively at level 4 (*managed and measurable*), having matured several aspects of its incident response program since last year (figure 11). For instance, the Board has implemented incident response metrics that are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders. In addition, the Board consistently shares information on incident activities with internal stakeholders and ensures that security incidents are reported timely to our office; the U.S. Computer Emergency Readiness Team; law enforcement; and, for major incidents, Congress.

Figure 11. Incident Response, Level 4 (*Managed and Measurable*)



Source. OIG analysis.

As part of our 2016 audit report, we recommended that the CIO update the Board's *Information Security Incident Handling Standard* to include considerations for handling major incidents and work with the appropriate parties to ensure that the escalation procedures outlined in the Federal Reserve System's incident handling guide for Board information is updated accordingly. In 2017, Board officials informed us that an update to the agency's *Incident Handling Standard* was still underway, along with the Board's *Data Breach Notification Policy*. This year, we found that the Board's *Incident Response Program* has been updated to include considerations for handling major incidents. Further, we found that escalation procedures in the Federal Reserve System's incident handling guide align with the updates made to the Board's incident response policies and procedures. As such, we are closing this recommendation.

Opportunities for Improvement

We identified further improvements the Board could make to mature its incident response program, and we offer these for management's consideration. For example, although the Board is consistently implementing and analyzing precursors and indicators that are generated by several supporting technologies that have been implemented in the organization, Board officials informed us that the agency does not have file integrity checking capability in place at this time.

Further, the Board has implemented several processes for incident handling, which include the development of incident containment strategies for various types of incidents, incident eradication processes, and processes to remediate vulnerabilities and recover system operations. However, the Board has not yet developed a process to fully integrate its vulnerability management function with its incident response functions. As such, the agency is not yet able to ensure that related vulnerabilities identified on one system can be quickly mitigated on other systems.

Recover

The objective of the *recover* function in the 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 impact of a cybersecurity event.

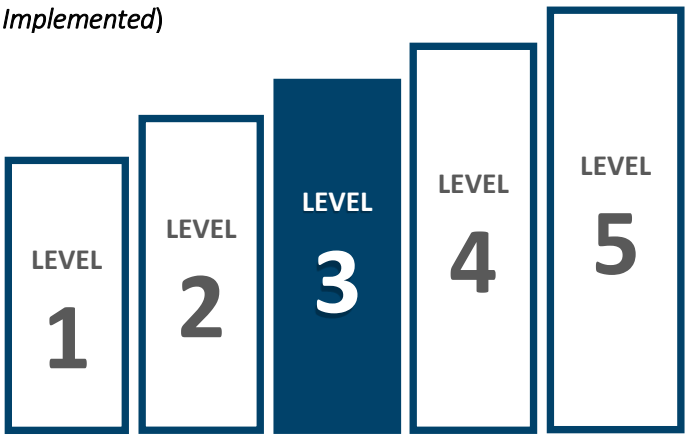
Contingency Planning

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. 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 factors that could affect mission-essential functions.

Current Security Posture

In 2017, the Board's contingency program was operating at level 3 (*consistently implemented*). Although this year we found that the Board continues to operate at level 3 (*consistently implemented*), we believe that the agency's contingency planning program is effective, with activities being performed at levels of higher maturity (figure 12).[18] For example, we found that the Board has consistently implemented its processes, strategies, and technologies for consistently performing information system backups and ensuring that its alternate processing and storage sites are configured with information security safeguards equivalent to those of the primary site. Further, for a select system that we reviewed, we noted that data are continuously

Figure 12. Contingency Planning, Level 3 (*Consistently Implemented*)



Source. OIG analysis.

[18] The FY 2018 IG FISMA reporting metrics made some minor changes to the maturity indicators for several FISMA metrics as compared to those for 2017. Most notably, several metrics were altered to remove the level-4 (*managed and measurable*) maturity indicator and incorporate them into other FISMA metrics. As such, IGs are provided flexibility in determining the level of effectiveness for these metrics.

replicated between the system's production and backup environments, providing a full, readily available copy of system data at either facility in the event that the contingency plan requires activation.

In our 2017 audit report, we recommended that the CIO ensure that the results of the Board's business impact analysis are used to make updates to the contingency planning program, as appropriate. This year, we found that all Board divisions have completed a business process analysis that highlights the processes, work flows, activities, systems, data, and facilities of their respective functions. These business process analyses were rolled up into an agencywide business impact analysis, which has been used as an input to determine the Board's risk mitigation strategy as well as the agency's high-value assets.[19] Therefore, we are closing this recommendation.

Opportunities for Improvement

Although the Board has implemented contingency planning procedures, along with tests and exercises to assess those procedures, the agency has opportunities to mature its contingency planning program through the consideration and management of information and communications technology (ICT) supply chain risks. NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (SP 800-161), states that the ICT supply chain concerns associated with contingency planning include planning for alternative suppliers of system components, alternative suppliers of systems and services, denial-of-service attacks to the supply chain, and alternate delivery routes for critical system components.[20] Further, SP 800-161 notes that many techniques used for contingency planning, such as alternate processing sites, have their own ICT supply chains and risks. Organizations should ensure that they understand and manage ICT supply chain risks and dependencies related to the contingency planning activities as necessary.

The importance of supply chain risk management is highlighted by its inclusion and enhanced focus in the recent update to the NIST Cybersecurity Framework. As such, we believe that management should consider which components of ICT supply chain concerns and risks should be addressed as a part of the Board's contingency planning program. Further, the use of performance metrics on the Board's information system recovery activities, including activities coordinated with ICT supply chain partners, would benefit the agency's process of continuous improvement for its contingency planning program.

[19] According to OMB M-17-09, *Management of Federal High Value Assets*, *high-value assets* are defined as those assets, federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could significantly affect U.S. national security interests, foreign relations, or economy or the public confidence, civil liberties, or public health and safety of the American people.

[20] The guidance and controls in this 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, 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.

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 2018 Inspector General Federal Information Security Modernization Act of 2014 (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 interviewed Board management and staff; analyzed security policies, procedures, and documentation; reviewed vulnerability scans performed for a select database technology; and observed and tested specific security processes and controls. We also assessed the implementation of select security controls for a select agency system.

To rate the maturity of the Board's information security program and functional areas, we used the scoring methodology defined in DHS's FY 2018 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 May 2018 to September 2018. 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: Management's Response

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

DIVISION OF
INFORMATION TECHNOLOGY

October 24, 2018

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 "2018 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) with FISMA and related information security and privacy policies, procedures, and standards and guidelines. The report also addresses the successful completion of remediation of four of thirteen recommendations from the past years' FISMA audits that 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 (POA&Ms) shortly 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. Donald Hammond

www.federalreserve.gov

Mr. Ray Romero
Mr. Charles Young
Mr. Ricardo Aguilera
Mr. Michell Clark
Mr. Khalid Hasan
Ms. Michelle Hercules

Abbreviations

Board	Board of Governors of the Federal Reserve System
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
COO	Chief Operating Officer
Cybersecurity Framework	*Framework for Improving Critical Infrastructure Cybersecurity*
DHS	U.S. Department of Homeland Security
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
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	personally identifiable information
PIV	personal identity verification
POA&M	plan of action and milestones
SP 800-122	Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*
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 for Federal Information Systems and Organizations*
SP 800-161	Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*

Report Contributors

Khalid Hasan, Senior OIG Manager
Paul Vaclavik, OIG Manager
Joshua Dieckert, Senior IT Auditor
Morgan Fletcher, IT Auditor
Nick Gallegos, IT Auditor
Chelsea Nguyen, IT Auditor
John Aderotoye, IT Audit Intern
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