Audit Report
2019-IT-B-016
October 31, 2019

Board of Governors of the Federal Reserve System

2019 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, 2019-IT-B-016, October 31, 2019

2019 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 effectively at a level-4 (*managed and measurable*) maturity. For instance, the Board has implemented its new suitability policy and assigned personnel risk designations to all Board positions. In addition, the Board has implemented automated mechanisms to more effectively support account management processes for privileged users across the organization.

The Board has opportunities to mature its information security program in Federal Information Security Modernization Act of 2014 (FISMA) domains across all five 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 defined its enterprisewide risk management strategy, risk appetite, and risk tolerance levels, which could help guide cybersecurity processes across function areas. While the Board has taken steps to move toward an enterprisewide approach to the delivery of information technology services and risk management, 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 3 of the 15 recommendations from our prior FISMA audits that remained open at the start of this audit. The closed recommendations relate to configuration management, identity and access management, and data protection and privacy. We are leaving open 12 recommendations in the areas of risk management, configuration management, identity and access management, data protection and privacy, security training, and information security continuous monitoring from our 2016, 2017, and 2018 FISMA audits. 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 6 new recommendations designed to strengthen the Board's information security program in the areas of risk management, identity and access management, and data protection and privacy. 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 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, 2019-IT-B-016, October 31, 2019

2019 Audit of the Board's Information Security Program

Number	Recommendation	Responsible office
1	Develop comprehensive enterprisewide guidance for the inventory of software and associated licenses throughout the Board.	Division of Information Technology
2	Work with all Board divisions to ensure that an accurate and complete software and license inventory is maintained.	Division of Information Technology
3	Ensure the consistent application of the Board's POA&M standard for the tracking of system- and program-level security vulnerabilities.	Division of Information Technology
4	Ensure that all components of the Board's public-facing website that require user authentication have a complete and visible warning banner, as appropriate.	Division of Information Technology
5	Work with the Federal Reserve System to ensure that the DLP replacement solution a. functions consistently across the Board's technology platforms. b. supports rulesets that limit the exfiltration weaknesses we identified, to the extent practicable.	Division of Information Technology
6	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.	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, 2019

TO: Distribution List

FROM: Peter Sheridan
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2019-IT-B-016: *2019 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 and performed vulnerability scanning and other technical tests; the detailed results of this testing will be transmitted under separate, restricted covers. 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 2019 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 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
Charles Young
Michelle Hercules
Tina White

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

Contents

Introduction 6

Objectives 6

Background 6

FISMA Maturity Model 7

Analysis of the Board's Progress in Implementing Key FISMA Information Security Program Requirements 10

Identify 11

Risk Management 11

Protect 19

Configuration Management 20

Identity and Access Management 22

Data Protection and Privacy 25

Security Training 28

Detect 30

Information Security Continuous Monitoring 30

Respond 31

Incident Response 32

Recover 33

Contingency Planning 33

Appendix A: Scope and Methodology 36

Appendix B: Management Response 37

Abbreviations 38

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. The *FY 2019 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 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.3, April 9, 2019.

[3] 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, 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 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

As noted in DHS's IG FISMA reporting metrics, one of the goals of the annual FISMA evaluation is to assess the agency's progress toward achieving outcomes that strengthen federal cybersecurity, including implementation of the administration's priorities. Two of these priorities are agency progress in implementing high-value asset (HVA) programs and supply chain management security best practices. Specifically, Office of Management and Budget (OMB) Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program,* requires all federal agencies to establish an HVA governance structure and take a strategic, enterprisewide view of cyber risk to HVAs. Additionally, the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act of 2018 (SECURE Technology Act) was passed to, in part, strengthen federal acquisition supply chain security.[4] As such, the IG FISMA reporting metrics have been updated to gauge the effectiveness of an agency's HVA program as well as its preparedness for addressing these new requirements, while recognizing that specific guidance on supply chain risk management will be issued at a later date.

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

[4] Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act, Pub. L. No. 115-390, 132 Stat. 5173 (2018).

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 to (1) summarize the status of agencies' information security programs and their maturity on a five-level scale; (2) 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) 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 IG FISMA reporting metrics, level 4 (*managed and measurable*) represents an effective level of security.[5] This is the third 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.

[5] 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.

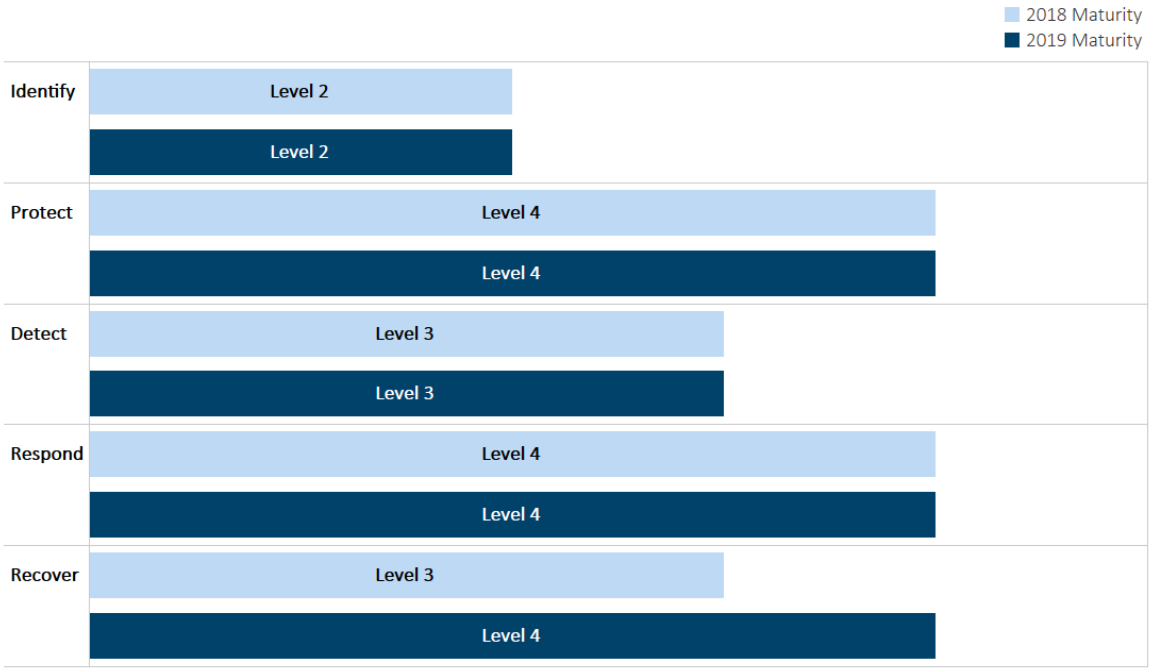
Figure 1. FISMA Maturity Model Rating Scale

Source. OIG analysis of DHS IG FISMA reporting metrics.

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

The Board's overall information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity (figure 2).[6] Although the agency has strengthened its program since our 2018 FISMA report, it has further opportunities to mature its processes across specific FISMA domains in all five Cybersecurity Framework security functions: *identify*, *protect*, *detect*, *respond*, and *recover*. For example, the *identify* function area continues to operate at a level-2 (*defined*) maturity. 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 enterprisewide risk management 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 will positively affect the Board's maturity in other areas. In addition, the Board continues to maintain a level-3 (*consistently implemented*) maturity in the *detect* function, and since our 2018 review, the Board has strengthened its capabilities in the *recover* function.

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



Source. OIG analysis.

[6] Appendix A of this report explains the scoring methodology outlined in DHS's IG FISMA reporting metrics that was used to determine the maturity of the Board's information security program.

Identify

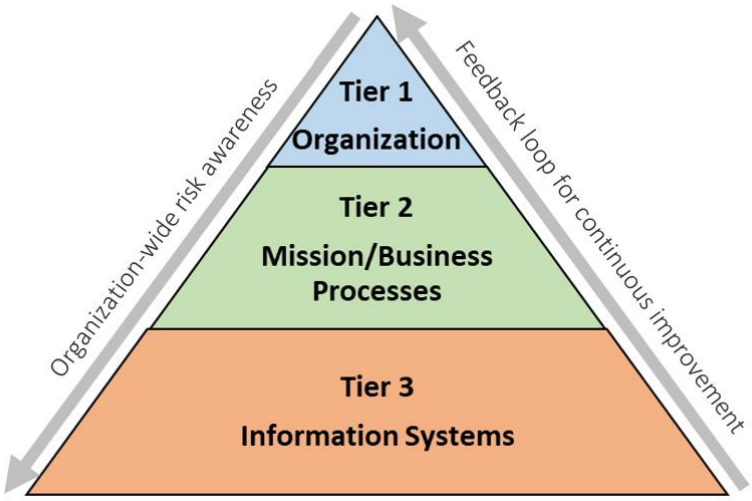
The objective of the *identify* function in the Cybersecurity Framework is to develop an organizational understanding of how to manage cybersecurity risks to agency systems, assets, data, and capabilities. The Cybersecurity Framework highlights risk management processes that organizations can implement to inform and prioritize decisions. Examples of the areas in this security function, as outlined in the IG FISMA reporting metrics, that we assessed include the Board's processes for enterprise risk management (ERM), securing HVAs, developing and implementing an enterprise architecture, asset management, and using 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. Risk management is further emphasized in OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which states that an effective ERM program promotes a common understanding for recognizing and describing potential risks that can affect an agency's mission. Such risks can include cybersecurity,[7] strategic, market, legal, and reputational.

The relationships between cybersecurity risk management and ERM are further outlined in NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* (SP 800-39), which notes that effective risk management involves integration of activities at the enterprise, mission and business process, and information system levels. As highlighted in figure 3, 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 Three Tiers of Risk Management



Source. NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.

[7] According to Executive Order, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, cybersecurity risk management refers to the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats; to maintain awareness of cyber threats; to detect anomalies and incidents adversely affecting IT and data; and to mitigate the impact of, respond to, and recover from incidents.

Tier 1 addresses risk from an organizational perspective, providing the context for all risk management activities carried out by the organization at tiers 2 and 3. NIST SP 800-39 notes that at tier 1, organizations are required to frame risk, which involves establishing the overall context for risk-based decisions. This context is established through the development of an ERM program. ERM refers to an effective agencywide approach to addressing the full spectrum of the agency's external and internal risks. Examples of ERM activities include the establishment of an enterprisewide risk management strategy and a supporting governance structure that includes the designation of a risk executive function. Additionally, ERM activities include the definition of the organization's risk appetite, risk tolerance, and risk profile.[8]

NIST SP 800-39 also notes that a key output of tier 1 risk management activities is the prioritization of mission and business functions. Specifically, more-critical mission and business functions necessitate a greater degree of risk management investments than those functions that are deemed less critical. NIST SP 800-39 further states that the determination of the relative importance of the mission and business functions, and hence the level of risk management investment, is decided at tier 1, executed at tier 2, and influences risk management activities at tier 3.

Tier 2 addresses risk from the mission and business process perspective and is informed by the risk context, decisions, and activities at tier 1. Risk management activities at tier 2 include prioritizing mission and business processes and defining the types and criticality of information needed to successfully execute the mission and business processes. These activities, along with the prioritization of mission and business functions at tier 1, can serve as a key input into the development of an HVA program. OMB Memorandum M-19-03 requires agencies to take a strategic, enterprisewide view of cyber risk and bolster protections of their HVAs to improve risk management across the government. HVAs are information and information systems that are deemed the most critical and high impact to agency and federal government operations.[9]

Another key tier 2 activity, as noted in SP 800-39, is the incorporation of information security requirements into mission and business processes, resulting in the development of an enterprise architecture. An enterprise architecture provides a disciplined and structured approach to achieving consolidation, standardization, and optimization of IT assets that are employed within organizations. One of the programs designed to assist with the consolidation, standardization, and optimization of IT assets is DHS's Continuous Diagnostics and Mitigation (CDM) program. CDM provides federal agencies with security capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential effects, and enable cybersecurity personnel to mitigate the most significant problems first. A goal of the CDM program is to provide adequate, risk-based, and cost-effective cybersecurity to

[8] 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. Although this circular is not directly applicable to the Board, other agencies, such as nonexecutive agencies, are encouraged to adopt the circular.

[9] According to OMB Memorandum M-19-03, agencies may designate federal information or information systems as HVAs when (1) the information or information system processes, stores, or transmits information that is of high value; (2) the agency that owns the asset cannot accomplish its primary mission-essential function within expected time frames without the information or information system; or (3) the information or information system serves a critical function in maintaining the security and resilience of the federal enterprise.

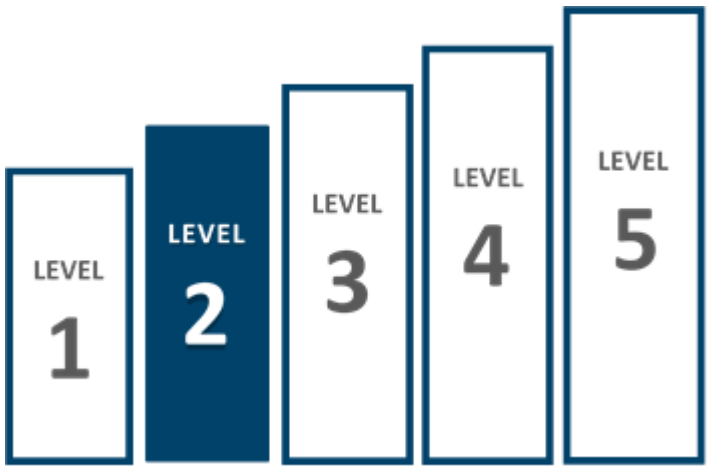
enable agencies to more efficiently allocate cybersecurity resources. CDM offers security capabilities for hardware, software, configuration setting, and vulnerability management.

Tier 3 addresses risk from an information system perspective and is guided by the risk context, risk decisions, and risk activities at tiers 1 and 2. Tier 3 risk management activities include the selection, implementation, assessment, authorization, and ongoing monitoring of allocated security controls for all of the organization's information systems. NIST SP 800-39 notes that the risk management activities at tier 3 reflect the organization's risk management strategy and any risk related to the cost, schedule, and performance requirements for individual information systems supporting the mission and business functions of organizations. Such requirements include specific control considerations for an organization's HVAs.

Current Security Posture

Similar to last year, we found that the Board's risk management program operates at a level-2 (*defined*) maturity (figure 4), with the agency continuing to improve and perform some activities indicative of a higher maturity level. For example, the Board has consistently implemented processes for hardware asset management and the communication of risk across the organization.

Figure 4. Risk Management, Level 2 (*Defined*)



Source. OIG analysis.

We have made several recommendations in prior FISMA reports related to risk management activities, including insider threat, third-party risk management, and policies and procedures, that remain open at this time. Specifically, our 2016 FISMA audit report includes a recommendation 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 and implement an agencywide insider threat strategy for sensitive but unclassified Board information.[10] While the Board has developed an insider threat program for its classified information, the agency has not yet determined which insider threat activities are applicable to the Board's sensitive but unclassified information. Further, as noted in the data protection and privacy section of this report, we identified an opportunity to strengthen offboarding processes that could be leveraged as part of an overall insider threat program.

In addition, our 2017 FISMA audit report includes two recommendations regarding the Board's risk management processes for third-party providers. Specifically, we recommended that the Chief Financial

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

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.[11] In 2018, we found that the Board was working to develop a new policy regarding security assurance requirements for third-party providers as well as reviewing existing third-party contracts. This year, we found that the Board was finalizing its *Vendor Management Standard* and updating the Board's standard contracting language.

Further, the Board developed an inventory of third-party providers that process, store, or transmit Board data. We found that the Board has reviewed the contracts identified through this process and accepted the risk of not making any amendments to these contracts. However, we found that the inventory of third-party providers used as part of this review was not complete. Specifically, it did not include all third-party providers we originally identified inconsistencies with as part of our 2017 FISMA audit. In addition, we noted other third-party providers that were not included in this inventory. As such, we are keeping both of these recommendations open and will continue to monitor the Board's efforts in this area as a part of future audit activities.

Further, our 2018 FISMA audit report includes a recommendation 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.[12] This year, we found that the Board has established a process to review its security policies and prioritize security policy updates for review. In addition, officials in the Division of Information Technology informed us that policy metrics and review processes have been established and that policy updates are discussed enterprisewide through the information security and privacy committee. However, the policies that we identified inconsistencies with in our 2018 FISMA audit report were still being revised. As such, we are keeping this recommendation open and will continue to monitor the Board's efforts in this area as a part of future audit activities.

Opportunities for Improvement

While the Board has taken steps to strengthen many of its risk management activities, we identified several opportunities for improvement across all three tiers of the risk management process.

Organizational Level (Tier 1)

As noted above, a key tier 1 activity is the implementation of a risk executive function and risk management strategy, including the determination of an organizational risk tolerance, as part of an overall ERM program. 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. In 2018, we found that the Board had begun to develop a strategy and governance structure for ERM but that implementation was still in progress. This year, we found that the Board continues to take steps to implement an ERM approach and governance structure as part of a phased process. As part of phase 1,

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

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

the Division of Information Technology has established an ERM committee governance structure and is communicating program status and cybersecurity risk mitigation decisions. The Board has established a Senior Officer Committee, whose responsibilities include serving as a forum for vetting Boardwide risk issues and advising the Executive Committee on risk strategy and appetite. Board officials informed us that the Senior Officer Committee also serves the purpose of a Chief Risk Officer or risk executive function. Further, the Board is updating its charter for the Senior Officer Committee to further clarify and align ERM roles and responsibilities with the new Executive Committee charter.

As part of phase 2, the Board is also working with other divisions to identify critical business processes and develop cyber risk appetites for each process. Furthermore, Board officials informed us that the Office of the Chief Operating Officer is piloting a process to implement ERM within the Board's operations divisions with a goal of broader adoption in the future. As such, while the Division of Information Technology has established an ERM governance structure and the Board is taking steps to develop and implement an organizationwide ERM strategy, we are leaving this recommendation open and will continue to monitor the Board's progress as part of our future FISMA reviews. We also believe that implementation of an ERM program could strengthen the Board's processes for managing risks with its HVAs.

Mission and Business Process Level (Tier 2)

As noted earlier, a key activity in tier 2 is developing and implementing an HVA program for the information and information systems that are deemed the most critical and high impact to agency and federal government operations. Specifically, OMB Memorandum 19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, requires agencies to take a number of steps to protect their HVAs against evolving cyber threats. These steps are outlined in table 2 and collectively represent the components of an HVA program.

Table 2. Key HVA Program Requirements

Requirement	Description
Establish enterprise HVA governance	Designate an HVA governance structure to incorporate HVA activities into broader agency activities, such as ERM, contracting processes, and contingency planning.
Improve the designation of HVAs	Identify and designate federal information or a federal information system as an HVA based on information value, support of mission-essential functions, and support of a critical function in maintaining the security and resilience of the federal civilian enterprise.
Implement data-driven prioritization	Allocate appropriate resources and ensure the effective protection of HVAs through collaboration and data-driven prioritization.
Increase the trustworthiness of HVAs	Implement systems security engineering principles for all HVAs to include security and privacy requirements.
Protect the privacy of HVAs	Ensure that privacy documentation and materials are maintained for HVAs that create, process, use, store, maintain, disseminate, disclose, or dispose of personally identifiable information.

Source. OIG analysis of OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, December 10, 2018.

While the Board has identified HVAs, it has not yet incorporated HVA security considerations into its ERM and contracting processes. Specifically, as noted earlier, the Board is developing and implementing an ERM program, and we have an open recommendation from our 2017 FISMA audit in this area. We believe that the outputs of an effective ERM program could further assist the Board in designating its HVAs and implementing data-driven prioritization. For example, an ERM program could help to identify the most critical mission and business functions, processes, and supporting systems, as well as investment priorities. As such, we suggest that the Board ensure that HVA security considerations and risk management activities are factored into the development and implementation of the agency's ERM program. Because of our open recommendations in these areas as well as evolving guidance around the security of HVAs, we will continue to monitor the Board's efforts to develop and implement an ERM program and ensure the integration of HVA activities into the program.

Further, OMB Memorandum M-19-03 requires agencies to ensure that the procurement of information systems, system components, applications, or services designated as HVAs or that are intended to support HVAs include requirements to employ systems security and privacy engineering concepts and methods, security and privacy design principles, secure coding techniques, and trusted computing methods in the system development life cycle. As noted above, our 2017 FISMA audit report includes a recommendation that remains open for the Chief Financial Officer to work with the CIO to strengthen processes for integrating the Board's information security requirements into contracting processes. We believe that as the Board continues to take steps to address our 2017 recommendation, it should also determine whether additional security requirements should be referenced in contracts for HVA systems

or services. As such, we are not making an additional recommendation in this area but will continue to monitor the Board's efforts as part of future FISMA reviews.

OMB Memorandum M-19-03 also requires that agencies implement the systems security engineering principles outlined in NIST Special Publication 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, for all HVAs. The Board has developed its *System Development Methodology* and supporting application development security standards that reflect these principles. The Board's Division of Information Technology has also established an enterprise architecture and associated review processes to enforce these security engineering principles.

As part of our 2017 FISMA audit report, however, we found that the Division of Information Technology's enterprise architecture and associated review processes were not being used consistently by all divisions. Specifically, our report recommends 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. In 2018 and again this year, we found that the agency is taking steps to identify approved tools in all divisions and is working to integrate its enterprise architecture and enforce associated review processes agencywide. As such, 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.

Related to enterprise architecture, we found that two of the four Board divisions that we sampled were using ad hoc processes to maintain an inventory of their software and associated licenses. For example, one of the two divisions began using an online collaboration tool to maintain software and license information once we notified them of this issue. The other division noted that its process for software and license management requires significant manual intervention and is not centralized. We believe that a key cause for this issue is that while the *Board Information Security Program* requires divisions to maintain this information, there is no supporting enterprisewide guidance on how to do so. As a result, the Board's CIO may not have full visibility into the software used across the organization and the associated licenses. Consistent processes for software and license management could assist the Board in achieving cost savings from potential duplicative software purchases.

Board officials have informed us that they are currently implementing DHS's CDM program, which they anticipate will provide more control and standardization of asset management processes. To assist agencies in migrating to the CDM program, DHS has published a readiness and planning guide for CDM capabilities.[13] The guide notes that successful implementation of the software asset management security capability of CDM depends on software platforms and applications within the organization being inventoried. As the Board moves forward with its implementation of CDM, it is important that its inputs, including the agency's software and license inventories, are as accurate and complete as possible. We believe that enterprisewide guidance regarding software and license management, along with a complete enterprise architecture, will help ensure that divisions maintain their software and license inventories effectively and will facilitate effective implementation of the CDM program.

[13] U.S. Department of Homeland Security, *Continuous and Diagnostics Mitigation: Readiness and Planning Guide for Asset-Based CDM Security Capabilities*, January 29, 2016.

Information System Level (Tier 3)

A key activity in tier 3 is the ongoing monitoring of allocated security controls for all of the organization's information systems. Our 2018 FISMA audit report includes a recommendation that the CIO ensure that all required inventory components, including the identification of personally identifiable information (PII) as well as internal and external interconnections, are maintained for all Board and third-party systems. This year, we found that the Board continues to maintain the details of its system inventory within its two FISMA compliance tools. However, for infrastructure systems, the Board does not require the identification of PII and system interconnection components within these compliance tools. While we recognize that PII attributes may be included within application-level information maintained in the agency's FISMA compliance tools, several of the Board's infrastructure systems do not have applications associated with them. Board officials informed us that they are working on a solution to capture this information for infrastructure systems.

Further, we continue to find discrepancies in the details maintained in the Board's two FISMA compliance tools. For example, one compliance tool tracks specific information regarding information system interconnections, while the other only tracks whether any interconnections exist. This difference in information maintained affects the agency's ability to maintain a centralized inventory of all required inventory components. While we recognize that information on system interconnections and PII may be maintained outside these two tools, we believe that the centralization of these inventory components could provide more-timely insight into the types of information maintained within the agency's systems. As such, we are keeping our 2018 recommendation open and will continue to monitor the Board's progress in this area.

Another risk management activity designed to assist with the ongoing monitoring of security controls is the POA&M process. FISMA requires agencies to develop and implement a process for planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies. Consistent with FISMA and OMB guidance, the Division of Information Technology has developed a POA&M standard to facilitate the remediation of program- and system-level security vulnerabilities identified from compliance reviews, vulnerability scans, OIG audits, and continuous monitoring activities. The standard requires the Division of Information Technology to develop and maintain a comprehensive POA&M program and ensure that the POA&M process is used to manage Boardwide information system vulnerabilities. The standard also requires system owners to develop, implement, and manage system-level POA&Ms.

While the Board has developed a POA&M process, we found that several of our cybersecurity-related recommendations are not being tracked consistently. Specifically, we found that the Board was not tracking elements outlined in its POA&M standard, including resource requirements, completion dates, and remediation plans for these recommendations. In addition, recommendations we made in a 2018 information system security control audit were not being tracked in a system-level POA&M.[14] Board officials informed us that they are working on a solution that will integrate POA&M information maintained within the Board's two FISMA compliance tools. We believe that this solution could provide a more centralized view into risk at the organization and information system levels. However, we found inconsistencies in the types of POA&M information that can exported from the two tools, which may

[14] Office of Inspector General, *Security Control Review of the Board Division of Research and Statistics' General Support System,* OIG Report 2018-IT-B-015R, September 26, 2018.

affect the Board's ability to maintain centralized visibility into its POA&M process. We believe a centralized and complete view into the Board's POA&Ms will provide the agency with greater assurance that all control deficiencies and risks are being adequately prioritized and mitigated.

Recommendations

We recommend that the CIO

1. Develop comprehensive enterprisewide guidance for the inventory of software and associated licenses throughout the Board.
2. Work with all Board divisions to ensure that an accurate and complete software and license inventory is maintained.
3. Ensure the consistent application of the Board's POA&M standard for the tracking of system- and program-level security vulnerabilities.

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.

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. Table 3 summarizes the security domains that are included in this security function and the associated components that are required to be assessed by IGs.

Table 3. *Protect* Function Security Domains and Selected Components

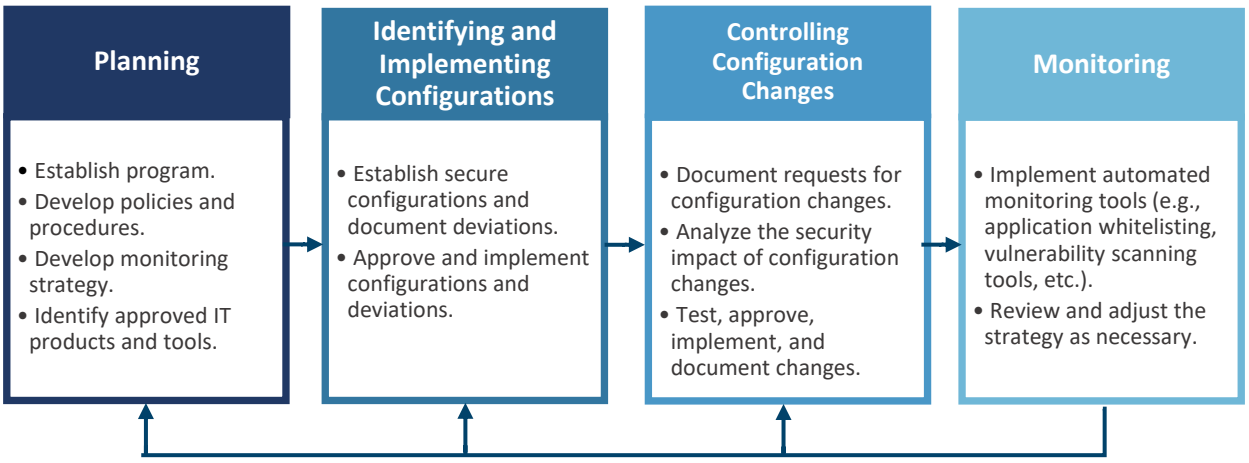
Security domains	Examples of components assessed by IGs
Configuration management	Configuration management plans, configuration settings, flaw remediation, and change control
Identity and access management	Identity credential and access management strategy, access agreements, least privilege, and separation 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 2019 Inspector General Federal Information Security Modernization Act of 2014 (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. 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 5).

Figure 5. Security-Focused Configuration Management Phases



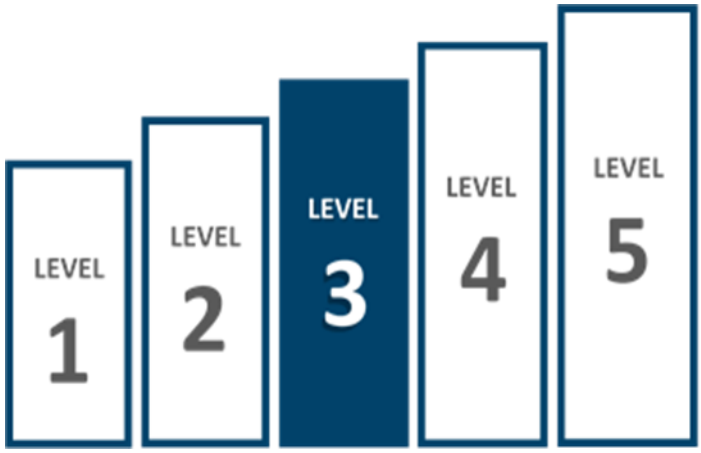
Source. NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*.

A key phase in 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 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[15] 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.

Current Security Posture

This year, we found that the Board's configuration management program continues to operate at a level-3 (*consistently implemented*) maturity (figure 6). For instance, the Board has consistently implemented its configuration change control activities, including the consideration of the security effects of proposed changes, the documentation of change control decisions, and the retention of records for approved configuration changes.

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



Source. OIG analysis.

Further, our 2016 FISMA report included a recommendation that the CIO develop and implement a plan to transition the Board's external network to a Trusted Internet Connections service provider as well as use services offered by DHS's EINSTEIN program, as appropriate.[16] This year, we found that the Board is taking steps to implement its plan to transition the Board's network to a Trusted Internet Connections service provider, performing testing to ensure that sufficient protections are in place. The Board's transition plan also includes steps to use the services offered through DHS's EINSTEIN program. As such, we are closing this recommendation.

Opportunities for Improvement

Similar to last year, we found opportunities to improve the Board's vulnerability scanning processes by ensuring that all network devices are being assessed. Specifically, our 2018 FISMA report includes a recommendation that the CIO ensure that all of the Board's network devices are included in the agency's vulnerability scanning processes.[17] This year, we found that the Board is still determining the best way to scan certain network devices to limit any effect on the availability of those devices. As such, we are

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

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

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

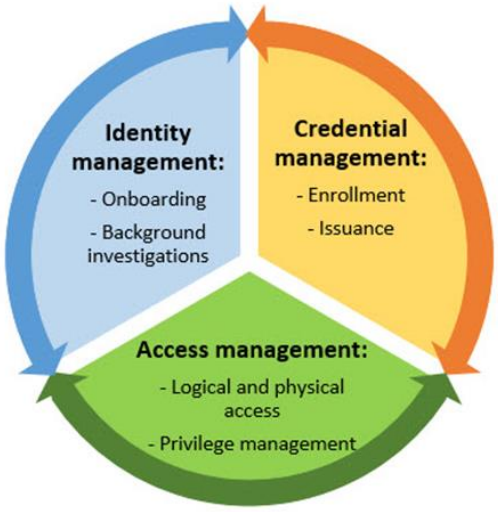
leaving this recommendation open and will continue to monitor the Board's efforts as a part of future audit activities. Further, we identified additional network devices that were not being periodically scanned. Once we notified Board officials of these additional devices, they took immediate steps to address the issue.

In addition, for two key agency systems, while database-level vulnerability scanning was being performed, it was not conducted with the privileges necessary to review all security configurations. Conducting such database-level vulnerability scanning could provide the Board with additional information regarding any potential security misconfigurations. We also performed vulnerability scanning at the operating system, network, and database levels for select Board systems. Our specific results will be transmitted under a separate, restricted cover.

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 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 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. Underscoring the importance of ICAM strategies, recent OMB guidance notes that, in line with the federal government's approach to modernization, it is essential that agencies' ICAM strategies and solutions shift toward a model informed by risk management perspectives and the federal resources accessed.[18]

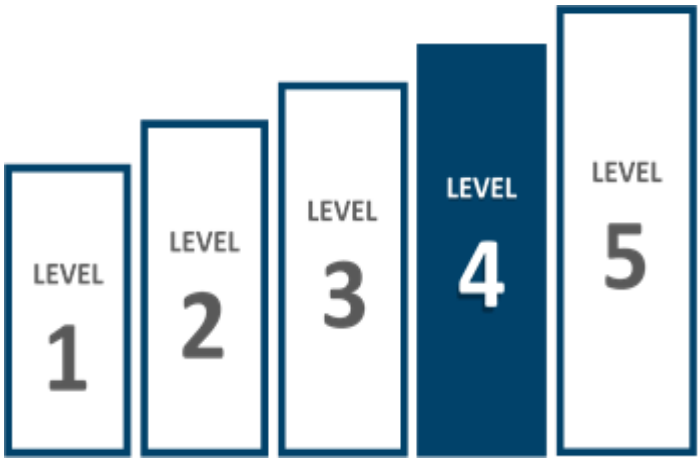
[18] Office of Management and Budget, Memorandum M-19-17, *Enabling Mission Delivery Through Improved Identity, Credential, and Access Management,* May 21, 2019.

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

Similar to last year, 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 requires multifactor authentication for access to its network for both privileged and nonprivileged users. Additionally, the Board has implemented its personal identity verification card–based solution for remote access. Further, the agency centrally manages annual access agreements for its users.

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



Source. OIG analysis.

The Board has also taken steps to strengthen its personnel screening processes. As part of our 2017 FISMA audit report, we made two recommendations regarding the Board's suitability policy. Specifically, we recommended that the COO work with Board divisions to update the agency's suitability policy to include requirements for assigning risk and sensitivity designations and associated investigative requirements to Board positions. Further, we recommended that the Director of the Management Division ensure that the agency's updated suitability policy is implemented and that investigations are conducted in accordance with the new policy.[19] In our 2018 report, we found that the Board had updated its suitability policy accordingly, and we closed that recommendation. This year, we found that the Board had implemented its updated suitability policy and assigned risk designations to all positions. Further, we found that the updated suitability policy increased the minimum background investigation level required and that investigations were conducted in accordance with this new requirement. As such, we are closing our 2017 recommendation.

Further, our 2017 FISMA audit report includes 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

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

between the two. Although the Board has implemented several ICAM processes effectively, including mandating the use of personal identity verification credentials for privileged and nonprivileged users, these activities were not guided by an enterprisewide ICAM strategy. Board officials have made progress in developing an ICAM strategy, but our review found that the strategy did not include all required elements. Specifically, it did not include an assessment of the current state of activities or a plan to bridge gaps between the current and target state. Therefore, we are leaving our recommendation open and will continue to monitor the Board's progress in this area as part of our future audit activities.

Opportunities for Improvement

This year, we identified an additional opportunity for the Board to improve its identity and access management program to ensure that it remains effective. Specifically, we found that two subsystems of the Board's public-facing website that require users to authenticate did not include the appropriate warning banner. Specifically, one subsystem accessible from the Board's public website had a warning banner that was not clearly visible, while another had a generic warning banner that did not include all required elements. We believe this issue exists because of inconsistent implementation of the warning banner requirements by system owners. Further, the Board's continuous monitoring process does not include reviews of system-level warning banners.

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* requires that information systems display a warning banner prior to logon to ensure that all users are aware of the type of system they are accessing and the applicable security and privacy conditions. Specifically, the warning banner should include notification (1) of access to a U.S. government information system; (2) that the information system may be monitored, recorded, and subject to audit; (3) that unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and (4) that use of the information system indicates consent to monitoring and recording. We believe that complete and visible warning banners on all portions of the Board's public website that require authentication will ensure that users are fully aware of and acknowledge the conditions that apply to their use of the system.

During our audit, we also identified weaknesses in security controls applied to sensitive Board information maintained within several of the Federal Reserve System's internal collaboration tools. Specifically, we identified multiple instances in which sensitive Board information was accessible to individuals who did not have a need to know. Upon notification of these issues, Board and System officials took immediate steps to either restrict access to this sensitive information to those with a need to know or remove the sensitive information from their respective collaboration environments if the information was no longer required for business purposes.[20] As such, we are not making any formal recommendations in this area and will continue to monitor the Board's efforts to strengthen access control as part of our future audit activities.

[20] On July 25, 2019, we issued a restricted memorandum detailing our observations concerning security controls for sensitive Board information maintained in the Federal Reserve System's collaboration tools.

Recommendation

We recommend that the CIO

4. Ensure that all components of the Board's public-facing website that require user authentication have a complete and visible warning banner, as appropriate.

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.

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. 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.[21] 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, 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).

[21] NIST has developed a risk management framework to provide a structured and flexible process for managing security and privacy risk for federal information and information systems that includes security categorization, control selection, implementation and assessment, authorization, and continuous monitoring. NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*, describes the Risk Management Framework and provides guidelines for applying it to information systems and organizations.

Current Security Posture

Similar to last year, 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 policies and procedures for the protection of the PII that is collected, used, maintained, shared, or disposed of by the agency. This includes encrypting data at rest within the Board's database management systems. The Board has also consistently implemented its data breach response plan for any incidents involving sensitive PII in its possession or under its control. Further, the Board has implemented agencywide privacy awareness training that all users are required to complete annually.

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

Source. OIG analysis.

In 2018, we identified an opportunity for the Board to strengthen its media sanitization processes.[22] These processes are designed to remove information from the media such that it cannot be retrieved or reconstructed, thus preventing the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Specifically, our 2018 FISMA audit report includes a recommendation for the CIO to ensure that documentation supporting the sanitization and disposal of all agency-owned electronic media is accurate and maintained in accordance with Board policy.[23] This year, we found that the Board has implemented new procedures regarding the sanitization and disposal of all hardware assets containing agency-owned information. These procedures include requirements that records of sanitized media are maintained, readily available, and reconcilable. We sampled electronic media sanitization records and found that the Board is maintaining documentation in accordance with its policies and procedures. As such, we are closing this recommendation.

Last year we also identified opportunities to strengthen controls for sensitive Board information, including PII, maintained in a report-generating technology used by the agency. Specifically, our 2018 FISMA audit report includes a recommendation for the CIO to develop and implement a process to (1) 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 (2) remove reports from the Board's report-generating technology in both production and nonproduction environments when they are no longer needed.[24] This year, we found that the Board has

[22] Information system media includes both digital and nondigital media subject to disposal or reuse. Examples include media found in scanners, copiers, printers, laptops, desktops, and mobile devices.

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

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

implemented new processes and automated scripts to ensure that access controls for the report-generating technology are based on the principles of need to know and least privilege. However, the agency has not yet implemented a process to remove reports from the report-generating environment when they are no longer needed. 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.

Opportunities for Improvement

We identified opportunities for the Board to mature its data protection and privacy program in two main areas. First, the Board leverages a commercially available data loss protection (DLP) solution managed by the Federal Reserve System. We found that the DLP solution was not fully effective in ensuring that sensitive agency data were protected from inadvertent or malicious exfiltration.[25] We believe that the primary causes of this issue were that the rulesets used by the tool did not function consistently across technologies and were not sufficiently tailored to account for the exfiltration avenues we identified. As a result, there is increased risk of undetected exfiltration of sensitive Board information.

Second, the Board has not implemented an organizationwide process to review logs from the DLP solution to identify suspicious events from employees leaving the agency. Specifically, while one Board division is performing this level of review of DLP logs, this process is not standardized across the agency.[26] Logs from the DLP solution contain key information that could assist the Board in identifying unauthorized transfer of, or access to, sensitive data when employees leave the agency. We believe this review is of heightened importance because of past occurrences of Federal Reserve System employees taking sensitive information with them when they leave their jobs.

The *FY19 CIO Reporting Metrics* highlights the importance of using technology, such as a DLP solution, to detect potential unauthorized exfiltration of information. In addition, NIST SP 800-122 notes that organizations can employ automated tools, such as DLP technologies, to monitor PII internally or at network boundaries for unusual or suspicious transfers or events. Further, with respect to a review of DLP logs, NIST Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide* (SP 800-61), notes that incidents may not be discovered until days, weeks, or months later. Audit logs can be reviewed and analyzed as often as needed to provide important information to organizations to facilitate risk-based decisionmaking.

Board officials informed us that the Federal Reserve System is in the process of evaluating new DLP solutions that will provide additional functionality and strengthen data exfiltration controls. The Board is working with the Federal Reserve System as part of this evaluation and plans to use the solution chosen. We believe that, as part of this process, the Board should work with the Federal Reserve System to ensure that the solution chosen addresses the weaknesses we identified, to the extent practicable.

[25] Because of the sensitive nature of these issues, the details will be transmitted under a separate, restricted cover.

[26] In addition, we found that the Federal Reserve System has defined a policy requiring managers to request and review logs from the DLP solution when an employee leaves the organization.

Recommendations

We recommend that the CIO

5. Work with the Federal Reserve System to ensure that the DLP replacement solution
    a. functions consistently across the Board's technology platforms.
    b. supports rulesets that limit the exfiltration weaknesses we identified, to the extent practicable.
6. 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.

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.

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.

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 Federal Cybersecurity Workforce Assessment Act of 2015 requires federal agencies to conduct and report to Congress a baseline assessment of their existing workforce.[27] To assist in implementing these requirements, NIST published the *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework* (NICE 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. Further, the framework organizes individuals with security

[27] Federal Cybersecurity Workforce Assessment Act of 2015, Title III of Pub. L. No. 114-113, 129 Stat. 2242, 2975 (2015) (codified at 5 U.S.C. § 301 note).

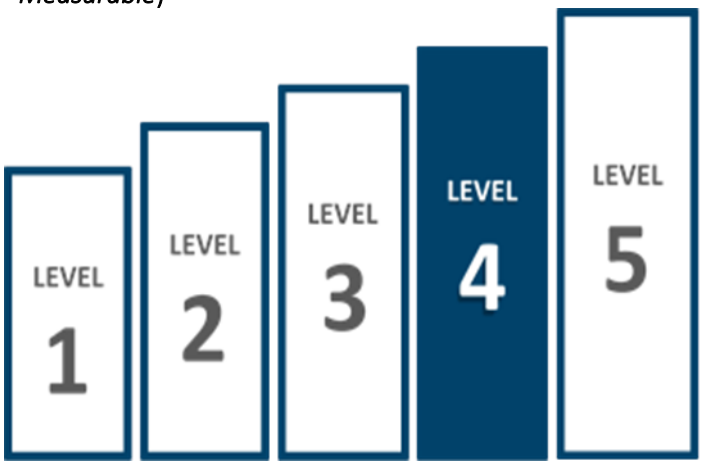
responsibilities into seven general categories: analyze, collect and operate, investigate, operate and maintain, oversee and govern, protect and defend, and securely provision.

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 receive 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 to 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 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. 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.

Opportunities for Improvement

Although the Board is operating an effective security training program, we have identified opportunities to improve role-based training processes and activities. Specifically, our 2018 FISMA audit report includes a recommendation that the CIO develop and implement a process to assess the knowledge, skills, and abilities of Board staff with security responsibilities and to establish plans to close identified gaps.[28] Our report also notes that the NICE Framework provides guidance to perform such an assessment. This year, we found that while the Board offers specialized security training for those with significant roles and responsibilities,[29] the agency has not defined its process for conducting an assessment on the knowledge, skills, and abilities of its workforce. Board officials informed us that they are planning to leverage recent work done by the Federal Reserve System in this area. We also believe that the completion of this assessment will enable the Board to improve its role-based training program. For example, the Office of

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

[29] The *Information Security Training Standard* designates authorizing officials, system owners, and system administrators as individuals having significant security responsibilities.

Personnel Management offers a governmentwide web-based training solution for individuals with significant security responsibilities, in alignment with the role-based categories defined within the NICE Framework. Further, the outputs of this skills assessment could be used to perform more-targeted phishing exercises. As such, 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.

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, maintain knowledge of threats, and ensure security control effectiveness. Examples of the assessment areas in this security function, as outlined in the IG FISMA reporting metrics, that we assessed include the Board's progress in developing and implementing an information security continuous monitoring (ISCM) strategy, performing ongoing system authorizations, and using ISCM-related performance measures.

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.

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

Source. OIG analysis.

Current Security Posture

Similar to last year, 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 captures metrics on IT security operations. These metrics include activities related to incident response functions, phishing exercises, user activity, web traffic, and data loss prevention.

Opportunities for Improvement

We found that the Board can mature its ISCM program through the use of further automation. For example, the Board maintains data regarding its system security plans, system authorizations, and other ISCM-related functions in two FISMA compliance tools. In a 2014 report, we recommended that security documentation for all Board-owned and -operated systems be centralized into one tool.[30] This year, we found that the Board continues to maintain two FISMA compliance tools, which hinders the agency's ability to deliver persistent situational awareness and assess security risks across the organization in a timely manner. For example, the Board is working to develop dashboards and metrics related to information system POA&Ms. However, in order to gather the information, the Board must export it from its two FISMA compliance tools. The fields captured in the two tools are not consistent, which requires manual intervention to consolidate into a centralized dashboard. As such, we are leaving this recommendation open and will monitor the Board's status in this area as part of our future FISMA reviews.

Further, our 2017 FISMA audit report includes a recommendation for the CIO to develop, implement, and regularly update an ISCM strategy that includes performance measures to gauge the effectiveness of related processes and that provides agencywide security status.[31] In 2018, Board officials informed us that completing an ISCM strategy would depend on the agency's implementation of the CDM program, which was scheduled to begin in 2019. This year, we found that the implementation of the CDM program is ongoing and that the Board plans to develop an ISCM strategy after the implementation of the CDM program is complete. Because we have an open recommendation regarding the implementation of an ISCM strategy, we are not making another recommendation in this area and will continue to monitor the Board's progress 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. Examples of the assessment areas in this security function, as outlined in the IG FISMA reporting metrics, that we assessed include the Board's incident detection, analysis, handling, and reporting processes.

[30] Office of Inspector General, *Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board's Information Security Life Cycle*, OIG Report 2014-IT-B-021, December 18, 2014.

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

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 SP 800-61, 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.

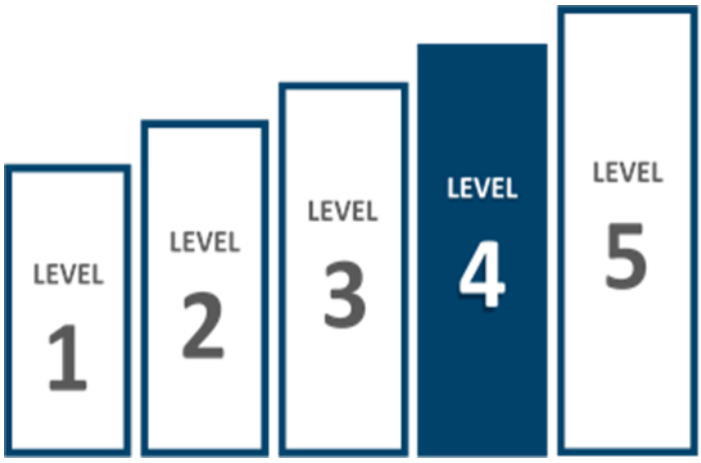
Source. NIST Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide.*

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 incident response and security intelligence services.

Current Security Posture

Similar to last year, 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 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 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.

Opportunities for Improvement

Although the Board's incident response program is operating effectively, we identified an opportunity for improvement through greater integration of the agency's incident response program with its vulnerability management processes. Specifically, the Board is in the process of implementing the tools offered through the CDM program. These tools could provide greater visibility into the security configurations and posture of agency systems, thus enabling the Board to strengthen its incident response capabilities. For instance, tools offered through the CDM program could strengthen the Board's processes for analyzing the enterprisewide impact of potential security incidents and vulnerabilities. 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 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. Examples of the assessment areas in this security function, as outlined in the IG FISMA reporting metrics, that we assessed include the Board's processes for developing and testing information system contingency plans, as well as 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. 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. The information obtained from an agency's business impact analysis can serve as important inputs to an organization's ERM and HVA programs. For example, system-level priorities from the business impact analysis can inform the risk-based allocation of resources to an agency's HVAs.

A key component of an effective contingency planning program is the consideration of risk from an organization's ICT supply chain. NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (SP 800-161), 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 alternative delivery routes for critical system components.[32] 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 the procurement of IT and to establish criteria for determining what types of products pose supply chain security risks to the federal government.[33] 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.[34] 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.

[32] 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, 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.

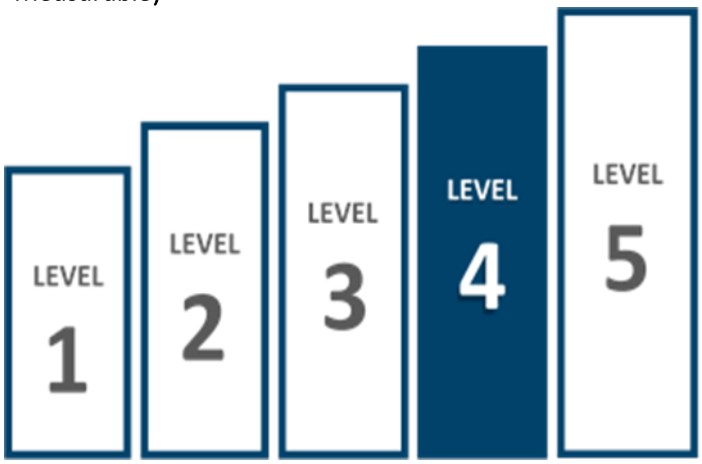
[33] At the conclusion of our fieldwork, the Federal Acquisition Security Council had not yet issued guidance related to mitigation of ICT supply chain risks.

[34] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1, April 16, 2018.

Current Security Posture

In 2018, the Board's contingency planning program was operating effectively at a level-3 (*consistently implemented*) maturity. This year, we found that the agency's contingency planning program is operating effectively at a level-4 (*managed and measurable*) maturity (figure 13).[35] Specifically, the Board has consistently implemented its processes, strategies, and technologies for performing information system backups and ensuring that its alternative processing and storage sites are configured with information security safeguards equivalent to those of the primary site. Further, the Board is measuring the effectiveness of its contingency planning testing activities. Additionally, for select systems that we reviewed, we noted that information system contingency plans are developed and implemented to include both organizational and system-level considerations regarding activation, testing, recovery, and reconstitution.

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



Source. OIG analysis.

Opportunities for Improvement

We found that the Board has opportunities to mature its contingency planning program through the consideration and management of ICT supply chain risks. SP 800-161 notes that many techniques used for contingency planning, such as alternative 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. While we recognize that SP 800-161 applies to high-risk systems, given the additional governmentwide focus on supply chain risk management, we believe that the Board should determine the applicability of ICT supply chain risks to its environment. As the Federal Acquisition Security Council works to develop additional criteria regarding the supply chain security risks to the federal government, the Board has an opportunity to further enhance its contingency planning program through the consideration of these risks. While we are not making a recommendation in this area at this time, we will continue to monitor the Board's efforts, including its response to guidance issued by the Federal Acquisition Security Council, as part of our future FISMA reviews.

[35] The FY 2019 IG FISMA reporting metrics included minor updates in the contingency planning domain. Specifically, a level-4 (*managed and measurable*) indicator was added within the contingency planning metrics.

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 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, including one of the agency's HVAs
- assessed Boardwide software and license management policies and sampled related processes for four Board divisions, including an analysis of software purchases against agency standards
- conducted specific testing of the effectiveness of the rulesets applied for the DLP tool used by the Board
- performed data analytics using a commercially available tool to support our testing in a number of 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 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 March 2019 to September 2019. 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 Response

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

DIVISION OF
INFORMATION TECHNOLOGY

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

Dear Mark:

We have reviewed your report entitled "2019 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 addresses the successful remediation of three of fifteen recommendations from prior FISMA audits and continues to recognize that the Board operates a comprehensive and effective information security program that has been continually enhanced.

We agree with the recommendations offered in your report. We have already made progress in addressing many of the recommendations. We will provide you with our 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 Operating Officer

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

www.federalreserve.gov

Abbreviations

Board	Board of Governors of the Federal Reserve System
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
COO	Chief Operating Officer
DHS	U.S. Department of Homeland Security
DLP	data loss protection
ERM	enterprise risk management
FISMA	Federal Information Security Modernization Act of 2014
HVA	high-value asset
ICAM	identity, credential, and access management
ICT	information and communications technology
IG	Inspector General
ISCM	information security continuous monitoring
IT	information technology
NICE Framework	*National Initiative for Cybersecurity Education Cybersecurity Workforce Framework*
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	personally identifiable information
POA&M	plan of action and milestones
SECURE Technology Act	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act of 2018
SP 800-61	Special Publication 800-61, *Computer Security Incident Handling Guide*
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
Martin Bardak, IT Auditor
Morgan Fletcher, IT Auditor
Nick Gallegos, IT Auditor
Chelsea Nguyen, IT Auditor
Alex Karst, Senior Information Systems Analyst
Fay Tang, Statistician
Ashley Azike, 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