OFFICE OF INSPECTOR GENERAL

Audit Report 2016-IT-B-013

2016 Audit of the Board's Information Security Program

November 10, 2016

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

Report Contributors

Khalid Hasan, Senior OIG Manager
Paul Vaclavik, OIG Manager
Chris Lambeth, Project Lead
Dan Megalo, IT Auditor
Jeff Woodward, IT Auditor
Chelsea Willis, IT Auditor
Morgan Fletcher, IT Auditor
Hau Clayton, Forensic Auditor
Peter Sheridan, Assistant Inspector General for Information Technology

Abbreviations

ATO	authorization to operate
BISP	*Board Information Security Program*
Board	Board of Governors of the Federal Reserve System
CIO	Chief Information Officer
DHS	U.S. Department of Homeland Security
Division of IT	Division of Information Technology
DLP	data loss prevention
EO 13587	Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
HSPD-12	Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*
IG	Inspector General
IR	incident response
ISCM	information security continuous monitoring
ISO	Information Security Officer
IT	information technology
NIST	National Institute of Standards and Technology
NITP	*National Insider Threat Policy*
OIG	Office of Inspector General
OMB	Office of Management and Budget

PIV	personal identity verification
SP 800-137	Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations
TIC	Trusted Internet Connections
US-CERT	United States Computer Emergency Readiness Team

Executive Summary:

2016 Audit of the Board's Information Security Program

2016-IT-B-013 November 10, 2016

Purpose

To meet our annual Federal Information Security Modernization Act of 2014 (FISMA) reporting responsibilities, we reviewed the information security program and practices of the Board of Governors of the Federal Reserve System (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 and (2) information security policies, procedures, and practices.

Background

FISMA requires each agency Inspector General (IG) to conduct an annual independent evaluation of the agency's information security program, practices, and controls for select systems. The U.S. Department of Homeland Security has issued guidance to the IGs on FISMA reporting for 2016. The guidance directs the IGs to evaluate the performance of their agencies' information security programs across eight domains that are grouped into five function areas: identify, protect, detect, respond, and recover.

Findings

Overall, we found that the Board continues to mature its information security program to ensure that it is consistent with FISMA requirements. For instance, the organization has implemented an enterprise-wide information security continuous monitoring lessons-learned process as well as strengthened its system-level vulnerability management practices. We also found that the Board's information security program contained policies and procedures that are generally consistent with the requirements for all eight information security domains listed by the U.S. Department of Homeland Security: risk management, contractor systems, configuration management, identity and access management, security and privacy training, information security continuous monitoring, incident response, and contingency planning. However, in the domain of risk management, we found that the Board can strengthen its insider threat activities by incorporating considerations for all types of sensitive information maintained by the organization into an organization-wide insider threat program. We also found that Board divisions were not consistently implementing the organization's risk management processes related to security controls assessment, security planning, and authorization.

In addition, we identified opportunities to strengthen controls in the areas of identity and access management, security and privacy training, and incident response to ensure that they are effective. Specifically, we identified opportunities for the Board to mature its information security program by (1) implementing a continuous monitoring approach for reviewing access to sensitive information maintained in the organization's enterprise-wide collaboration tool; (2) determining how best to implement multifactor authentication for all nonprivileged information system users; (3) conducting exercises to test the effectiveness of its security and privacy awareness training program; and (4) developing a plan to implement the Trusted Internet Connections Initiative and the governmentwide EINSTEIN program to better prevent, detect, and respond to information security incidents.

Finally, the Board has made progress in addressing our recommendations from last year's FISMA audit report. Our 2015 FISMA audit report included four recommendations to strengthen the Board's information security continuous monitoring, configuration management, and identity and access management. Based on the steps taken by the Board, we are closing three of our four outstanding recommendations.

Recommendations

Our report includes nine new recommendations to strengthen the Board's information security program in the areas of risk management, identity and access management, security and privacy training, and incident response. The Director of the Division of Information Technology concurs with our recommendations and stated that she has initiated actions to address them.

Summary of Recommendations, OIG Report 2016-IT-B-013

Recommendation number	Page	Recommendation	Responsible office
1	8	Work with the Chief Operating Officer to perform a risk assessment to determine which aspects of an insider threat program are applicable to other types of sensitive Board information and develop and implement an agency-wide insider threat strategy for sensitive but unclassified Board information, as appropriate.	Division of Information Technology
2	8	Strengthen oversight processes to ensure that all Board systems, as appropriate, have a current authorization to operate that is based on comprehensive selection, implementation, and assessment of security controls.	Division of Information Technology
3	10	Work with Board divisions and the Federal Reserve Banks, as appropriate, to develop and implement a continuous monitoring approach for ensuring that sensitive Board information maintained in the organization's and the Federal Reserve System's enterprise-wide collaboration environments is appropriately restricted.	Division of Information Technology
4	10	Develop and implement an identity and access management plan that includes a risk-based determination on how multifactor authentication will be implemented for nonprivileged users of the Board's internal information technology resources.	Division of Information Technology
5	12	Develop and implement a plan to periodically evaluate the effectiveness of the organization's security awareness and training program.	Division of Information Technology
6	17	Update the Board's *Incident Handling Standard* to include considerations for handling major incidents and work with appropriate parties to ensure that the escalation procedures outlined in the Federal Reserve System's incident handling guide for Board information is updated accordingly.	Division of Information Technology
7	17	Ensure that all lost laptop computers and mobile devices are reported consistent with guidance from the United States Computer Emergency Readiness Team.	Division of Information Technology
8	17	Develop and implement a plan to a. transition the Board's external network to a Trusted Internet Connections service provider. b. utilize the services offered by the U.S. Department of Homeland Security's EINSTEIN program, as appropriate.	Division of Information Technology
9	17	Define and implement performance measures to gauge the effectiveness of the Board's incident response program, including services provided by the National Incident Response Team.	Division of Information Technology

OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

November 10, 2016

MEMORANDUM

TO: Sharon Mowry
Chief Information Officer and Director, Division of Information Technology
Board of Governors of the Federal Reserve System

FROM: Peter Sheridan
Assistant Inspector General for Information Technology

SUBJECT: OIG Report 2016-IT-B-013: *2016 Audit of the Board's Information Security Program*

The Office of Inspector General has completed its 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 the agency's information security program and practices. As part of our work, we also reviewed security controls for two select agency systems; the detailed results of those reviews will be transmitted under separate, restricted cover. In addition, we will use the results of this audit to respond to specific questions in the U.S. Department of Homeland Security's *Fiscal Year 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*.

Our report contains recommendations designed to strengthen the Board's information security program. We provided you with a draft of our report for review and comment. In your response, you outline actions that have been or will be taken to address our recommendations. We have included your response as appendix C to our report.

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

cc: Donald V. Hammond, Chief Operating Officer
Raymond Romero, Senior Associate Director
Charles Young, Deputy Associate Director
William Mitchell, Chief Financial Officer and Director, Division of Financial Management

Contents

Introduction 1

Objectives 1
Background 1

Summary of Findings 4

Analysis of the Board's Progress in Implementing Key FISMA and DHS Information Security Program Requirements 5

Risk Management 5
Identity and Access Management 8
Security and Privacy Training 11
Information Security Continuous Monitoring 12
Incident Response 14

Status of Prior Years' Recommendations 18

Information Security Continuous Monitoring 18
Configuration Management 18
Identity and Access Management 19

Appendix A: Scope and Methodology 20

Appendix B: FISMA Scoring Methodology 21

Appendix C: Management's Response 22

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 and (2) information security policies, procedures, and practices. Our scope and methodology are detailed in appendix A.

Background

FISMA, which amended the Federal Information Security Management Act of 2002, requires agencies to develop, document, and implement an agency-wide information security program for the information and the information systems that support the operations and assets of the agency, including those provided by another agency, contractor, or other source.[1] FISMA also requires that each agency 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.

In support of FISMA's independent evaluation requirements, the U.S. Department of Homeland Security (DHS) issued guidance to the IGs on FISMA reporting for 2016.[2] This guidance directs the IGs to evaluate the effectiveness[3] of agency information security programs across a variety of attributes grouped into eight security domains: risk management, contractor systems, configuration management, identity and access management, security and privacy training, information security continuous monitoring (ISCM), incident response (IR), and contingency planning. These domains map to the five information security functions outlined in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity—identify, protect, detect, respond, and recover, as shown in table 1.

1. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-228, 128 Stat. 3073 (2014) (codified at 44 U.S.C. §§ 3551-3558).

2. U.S. Department of Homeland Security, *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, September 9, 2016.

3. National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, notes that security control effectiveness addresses 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.

Table 1: Cybersecurity Framework Security Functions Alignment With the FISMA Metric Domains

Cybersecurity framework security functions	FISMA metric domains
Identify	Risk management and contractor systems
Protect	Configuration management, identity and access management, and security and privacy training
Detect	Information security continuous monitoring
Respond	Incident response
Recover	Contingency planning

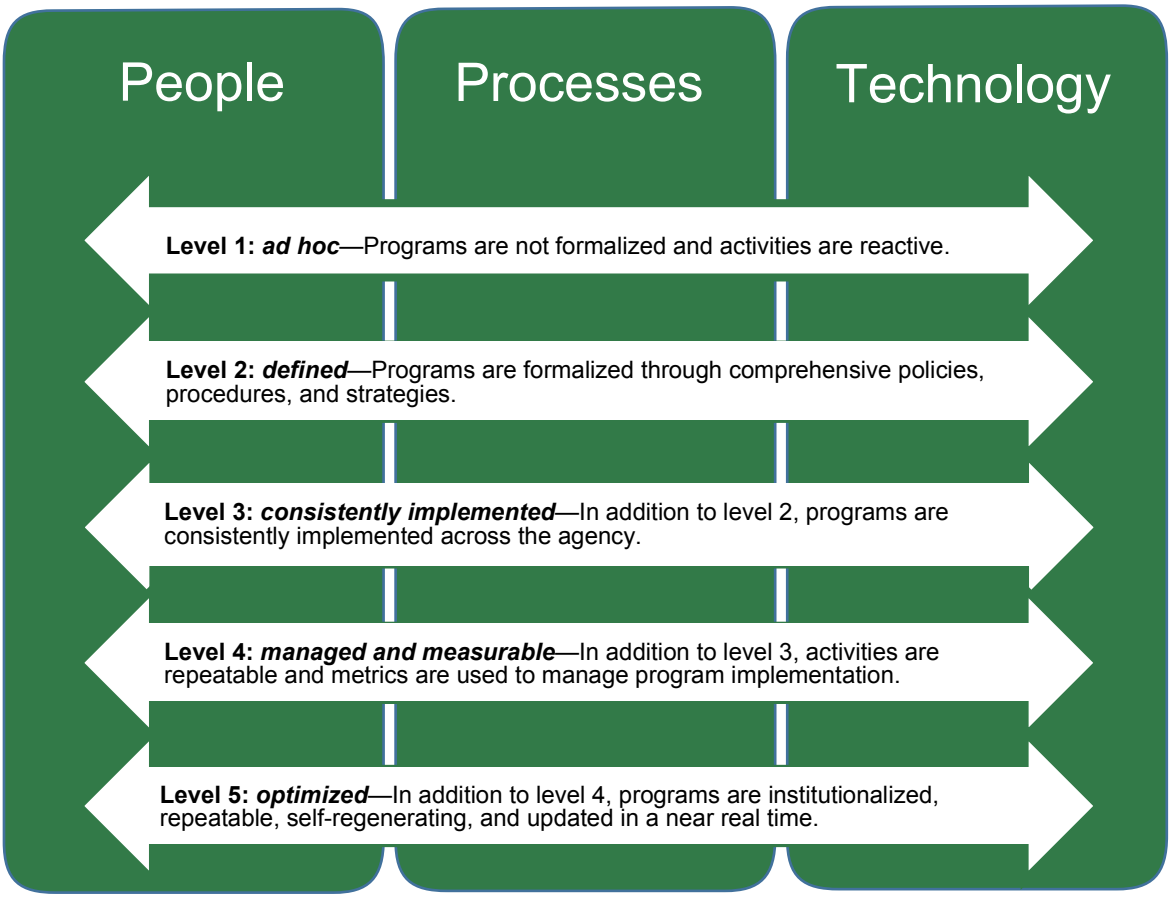
Source: DHS, *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*.

Maturity Model Approach for Assessing Agency Information Security Programs

With the increased focus in FISMA on security control effectiveness, in 2015, the Council of the Inspectors General on Integrity and Efficiency, in coordination with the Office of Management and Budget (OMB), DHS, NIST, and other key stakeholders, undertook an effort to develop a maturity model to evaluate the operating effectiveness of information security programs within a given agency and across agencies. In 2015, DHS's FISMA reporting guidance for IGs included a maturity model for ISCM, a key cybersecurity focus area for the federal government. In 2016, DHS' FISMA reporting guidance for IGs expanded to include a maturity model for IR, another key cybersecurity focus area.

The purpose of the maturity models is (1) to summarize the status of agencies' information security programs and their maturity on a five-level scale; (2) to provide transparency to agency Chief Information Officers, top management officials, and other interested readers of IG FISMA reports regarding what has been accomplished and what still needs to be implemented to improve the information security program; and (3) to help ensure that annual FISMA reviews are consistent across IGs. The maturity model includes steps to assess an agency's program through an analysis of three domains: people, processes, and technology. The maturity levels of each of these domains dictate the overall maturity of an organization's program. Figure 1 provides an overview of the five levels of the maturity model. A maturity ranking of level 4 represents an effective level of security within an area.

Figure 1: Maturity Model Rating Scale



Source: OIG analysis of DHS's *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*.

Summary of Findings

Overall, we found that the Board continues to mature its information security program to ensure that it is consistent with FISMA requirements. For instance, the organization has implemented an enterprise-wide ISCM lessons-learned process as well as strengthened its system-level vulnerability management practices. We also found that the Board's information security program contained policies and procedures that are generally consistent with the requirements for all eight information security domains listed by DHS: risk management, contractor systems, configuration management, identity and access management, security and privacy training, ISCM, IR, and contingency planning. In the risk management domain, however, we found that the Board can strengthen its insider threat activities by incorporating considerations for all types of sensitive information maintained by the organization into an organization-wide insider threat program. Specifically, although the Board is taking steps to develop an insider threat program for the classified information that it has access to, it has not yet determined which components of this program could apply to other sensitive information maintained by the organization.
We also found that Board divisions were not consistently implementing the organization's risk management processes related to security controls assessment, security planning, and authorization. Specifically, for two select systems that we reviewed, we found that controls had not been adequately assessed, the systems were operating with an expired authorization to operate, and the systems' security plans were not comprehensive.

In addition, we identified opportunities to strengthen controls in the areas of identity and access management, security and privacy training, and IR to ensure that they are effective. Specifically, we continued to find instances of Board sensitive information that was not appropriately restricted within the organization's enterprise-wide collaboration tool. We also found that the Board has not yet determined how best to implement multifactor authentication for all nonprivileged information system users. This year, we found that the Board had not evaluated the effectiveness of its security and privacy awareness training program. Finally, we found that the Board can strengthen its IR capabilities by transitioning to a Trusted Internet Connections (TIC) network provider and utilizing services offered through DHS's EINSTEIN program for intrusion detection and prevention.

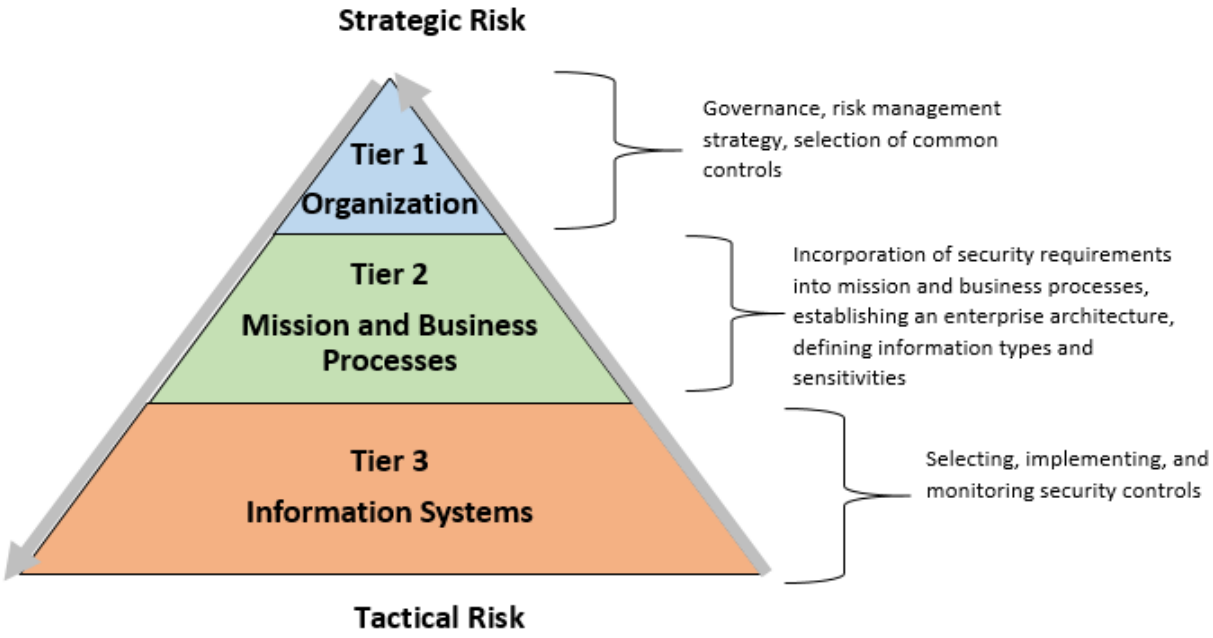
In addition, our prior year's FISMA audit report included four recommendations designed to strengthen the Board's ISCM, configuration management, and identity and access management programs. We found that the Board has taken sufficient actions to close three of the four open recommendations. We are leaving open our 2015 recommendation for the Board to strengthen its software asset management processes by using automation to provide greater visibility into authorized and unauthorized software across the organization; we will continue to monitor the Board's progress in addressing this recommendation as part of future audits.

Risk Management

Requirement

Information security risk management refers to the program and supporting processes used to manage information security risk to organizational operations, assets, individuals, and other organizations. This includes establishing the context for risk-related activities, assessing risk, responding to risks, and monitoring risks over time. NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, notes that managing risk is a complex, multifaceted activity that requires the involvement of the entire organization. As depicted in figure 2, to integrate the risk management process throughout an organization and more effectively address mission and business concerns, a three-tiered approach is best employed that addresses risk at the organization, mission/business process, and information system levels.

Figure 2: The Three Tiers of Risk Management



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

One organization-level risk that has garnered considerable attention recently within the federal government is that of insider threat. Specifically, personnel that are entrusted with sensitive agency information can pose specific types of security risks to organizations, both through intentional and inadvertent actions. For example, trusted employees of the agency may feel justified in pursuing malicious activity against the organization, or they may be exploited by outside adversaries to inflict harm against the organization. These particular types of insider threats have become increasingly common and have been the source of several recent and highly publicized data breaches across the public and private sectors.

As the Board maintains sensitive, market-moving economic and financial information, insider threats are a key risk area. For example, our 2015 FISMA audit report highlighted risks the Board faced from sensitive information in the organization's enterprise-wide collaboration tool that was not appropriately restricted. This year, as detailed in the Identity and Access Management section of this report, we continue to find similar access control weaknesses. Further, the Board has also had incidents of sensitive Federal Open Market Committee information under embargo released ahead of schedule.[4]

The importance of managing risks from insider threats led to the issuance of Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (EO 13587), as well as the *National Insider Threat Policy* (NITP).[5] EO 13587 directs executive branch agencies and departments to establish, implement, monitor, and report on the effectiveness of insider threat programs to protect classified national security information. The NITP provides implementation guidance on EO 13587 and directs agency heads to designate a senior agency official or officials who will provide management and oversight of an insider threat program, including developing a comprehensive agency insider threat policy. The policy further requires agency heads to build and maintain an insider threat analytic and response capability to gather and analyze information on insider threats gathered from information assurance, human resources, law enforcement, and other agency areas.

The Board has determined that the requirements of EO 13587 and the NITP apply only to those individuals in the organization with a security clearance and with access to classified information. NIST also notes that the guidelines contained in EO 13587 and the NITP can be employed effectively to improve the security of controlled unclassified information in non–national security systems.[6] Information on organizational level risks, such as those posed from insider threats, can be used to support risk management activities at the mission/business process and information system levels. For instance, insider threat risks can affect the selection, implementation, assessment, authorization, and ongoing monitoring of security controls.

---

4. Office of Inspector General, *The Board Should Strengthen Controls to Safeguard Embargoed Sensitive Economic Information Provided to News Organizations*, OIG Report 2016-MO-B-006, April 15, 2016.

5. EO 13587 was issued on October 7, 2011, to ensure the responsible sharing and safeguarding of classified national security information on computer networks. The order established an insider threat task force to develop a governmentwide insider threat program for deterring, detecting, and mitigating insider threats. The task force issued the NITP in November 2012, which provides minimum requirements and guidance for executive branch insider threat detection and prevention programs.

6. NIST SP 800-53 requires organizations to implement an insider threat program that includes a cross-discipline insider threat incident handling team. SP 800-53 further states that insider threat programs include security controls to detect and prevent malicious insider activity through centralized integration and analysis of both technical and nontechnical information to identify potential insider threat concerns.

Progress to Date

The Board has implemented risk management activities at the organization, business process, and information system levels. At the organization level, the Board has implemented aspects of an insider threat program, such as message classification and data loss prevention (DLP) systems, and a limited capacity digital rights management solution to monitor and detect data exfiltration and other threats. Additionally, the Board's annual security awareness training includes content regarding insider threats and highlights the importance of protecting confidential information. In accordance with EO 13587, the Board is developing an insider threat program for those with access to classified information and has drafted a strategy document and a specialized training program.

At the mission/business process level, the Board has developed a risk register process in which risks at the division level are captured and incorporated into system-level risk management activities. At the information system level, the Board has established an information system risk management framework as described in NIST Special Publication 800-30, *Guide to Conducting Risk Assessments*, and defined risk management requirements for each of the three risk management tiers. The Board's information system risk management requirements are based on a system's type, security categorization, and risk profile. The Board has also tailored security controls to its operating environment and developed policies for various risk management activities.

Work to Be Done

We found that the Board can strengthen its risk management activities related to insider threats at the organization and information system level. At the organization level, we found that although the agency is in the process of developing an insider threat program for those with access to classified information, the Board could benefit by determining which aspects of this program apply to other types of sensitive information that the organization maintains and including those program aspects. Further, at the information system level, we found that the Board does not explicitly require the consideration of insider threats as part of its risk assessment methodology. Board officials have stated that they plan to comply with EO 13587 only for those with access to classified information. Given the limited amount of classified information accessed by the Board and the sensitive nature of the nonclassified data collected by the Board to fulfill its mission, however, we believe that by strengthening ongoing insider threat risk management activities, the Board can further protect the confidentiality, integrity, and availability of the organization's data.

At the information system level, we found that the Board's risk management requirements are not consistently implemented or enforced. For example, in our testing of controls for two select Board systems, we found that the systems were operating with an expired authorization to operate (ATO) and had incomplete security plans.[7] Further, for one of these systems, we found that controls were not fully assessed as part of its last ATO performed. For the second system, we also found that the system owner was not updating security controls information in the Board's FISMA management tool or receiving an independent review of its plan of action and

7. An ATO is the official management decision to authorize operation of an information system and to explicitly accept the residual risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. An ATO typically includes completing a risk/security assessment, system security plan, and plan of action and milestones. A system security plan provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

milestones. These weaknesses resulted from inconsistent oversight of the Board's risk management program. As a result, the Board may not have a complete and accurate enterprise view of system-level risks.

Recommendation

We recommend that the Chief Information Officer (CIO)

1. Work with the Chief Operating Officer to perform a risk assessment to determine which aspects of an insider threat program are applicable to other types of sensitive Board information and develop and implement an agency-wide insider threat strategy for sensitive but unclassified Board information, as appropriate.

2. Strengthen oversight processes to ensure that all Board systems, as appropriate, have a current ATO that is based on comprehensive selection, implementation, and assessment of security controls.

Management's Response

In her response to our report, the Director of the Division of Information Technology (Division of IT) states that she agrees with the recommendations and has already initiated actions to address the recommendations. These actions include continuing to enhance the Board's risk management and continuous monitoring programs.

OIG Comment

In our opinion, the actions described by the Director are responsive to our recommendations. We plan to follow up on the Board's actions to ensure that the recommendations are fully addressed.

Identity and Access Management

Requirement

Identity and access management includes implementing a set of capabilities to ensure that users authenticate to information technology (IT) resources and have access to only those resources that are required for their job function, a concept referred to as *need to know*. 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. Further, due to security vulnerabilities that may have been exploited with recent cybersecurity breaches affecting the federal government, OMB has placed added emphasis on agencies adopting multifactor authentication for users of IT resources.[8] Multifactor

8. To improve federal cybersecurity and protect systems against evolving threats, in June 2016, OMB launched a 30-day Cybersecurity Sprint. As part of this effort, OMB directed agencies to dramatically accelerate their use of multi-factor authentication, especially for privileged users.

authentication involves using two or more factors to achieve authentication, such as (1) something you know (for example, a password or PIN); (2) something you have (for example, a personal identity verification card or token); or (3) something you are (for example, a biometric).

Agency adoption of multifactor authentication is required by Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors* (HSPD-12). Issued in 2004, HSPD-12 requires federal agencies to use personal identity verification (PIV) cards for both physical and logical access. For example, use of a PIV card in conjunction with a username and password would provide two-factor authentication to an information system. Subsequent federal guidance has clarified that agencies may implement PIV cards or a solution that provides an equivalent level of security to meet HSPD-12 requirements.

The Board has issued a number of policy and procedural documents that provide guidance on implementing identity and access controls. For instance, the *Board Information Security Program* (BISP) requires that access controls be implemented for all information systems to ensure that users are accountable for their actions and to protect data and equipment from malicious or accidental unauthorized access, damage, or loss. Further, the BISP requires the use of PIV cards for employees and contractors for physical access as well as the use of multifactor authentication for remote access.

Progress to Date

The Board has taken steps to strengthen access controls over sensitive information maintained by the organization. For example, our 2015 FISMA audit report included a recommendation for the CIO to implement a process to periodically monitor access control settings for sensitive information in the Board's enterprise-wide collaboration tool.[9] In response, the Board's Division of IT developed an access validation process and offered training to ensure that proper access controls are established. As such, we are closing our 2015 recommendation. As noted below, however, we continued to find multiple instances of sensitive Board information, including personally identifiable information, stored in the Board's enterprise-wide collaboration tool, which is not restricted to employees with a need to know.

We also found that the Board has been using PIV cards for physical access control and identification purposes for its employees and contractors for several years and also utilizes two-factor token-based authentication for remote access to its network. As highlighted in our report on the Board's information security management practices pursuant to the Cybersecurity Act of 2015, we also found that the Board has implemented PIV cards for privileged users for the organization's Active Directory operating environment.[10] This environment provides authentication services for the agency's network and several systems.

9. Office of Inspector General, *2015 Audit of the Board's Information Security Program*, OIG Report 2015-IT-B-019, November 13, 2015.

10. Office of Inspector General, *OIG Report on the Board's Information Security Management Practices Pursuant to Section 406 of the Cybersecurity Act of 2015*, August 12, 2016.

Work to Be Done

As noted above, we continue to identify instances of sensitive Board information, including personally identifiable information, which is not restricted to individuals with a need to know within the Board's internal enterprise-wide collaboration tool. We also identified similar access control issues with sensitive Board information that is maintained in the Federal Reserve System's collaboration tool. Although the Board has taken steps to strengthen access controls, it has not implemented a continuous monitoring approach that could timely identify instances in which access controls are not appropriately set for sensitive Board information that is maintained in the organization's and the Federal Reserve System's enterprise-wide collaboration tools. As such, there is heightened risk of unauthorized disclosure and inappropriate use of sensitive Board information.

We found that the Board has not implemented the use of PIV cards or another multifactor authentication solution for nonprivileged users of its internal IT resources due to technical difficulties and higher-priority projects. As a result, there is heightened risk of unauthorized access to internal systems. Further, we found that the encryption algorithms supported by the remote-access tokens do not meet federal requirements for cryptographic modules.[11] Board officials notified us that the organization is aware of this issue and that the resulting risk is limited, as the organization does not utilize the tokens for cryptographic functions, such as digital signatures. Further, Board officials notified us that they are working on a plan to implement updated tokens that meet federal requirements. We will continue to monitor the Board's progress in updating its remote access tokens as part of our future FISMA reviews.

Recommendations

We recommend that the CIO

3. Work with Board divisions and the Federal Reserve Banks, as appropriate, to develop and implement a continuous monitoring approach for ensuring that sensitive Board information maintained in the organization's and the Federal Reserve System's enterprise-wide collaboration environments is appropriately restricted.

4. Develop and implement an identity and access management plan that includes a risk-based determination on how multifactor authentication will be implemented for nonprivileged users of the Board's internal IT resources.

Management's Response

In her response to our report, the Director of the Division of IT states that she agrees with the recommendations and has already initiated actions to address the recommendations.

11. Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001.

OIG Comment

In our opinion, the actions described by the Director are responsive to our recommendations. We plan to follow up on the Board's actions to ensure that the recommendations are fully addressed.

Security and Privacy Training

Requirement

An important control for raising awareness of information security roles and responsibilities is security and privacy training. FISMA requires agencies to provide security awareness training to all information system users and provide role-based security training to individuals with significant security responsibilities. The primary difference between security awareness training and role-based training is that the former is geared toward educating all users about overall information security policies, while the latter is geared toward teaching the information security skills needed to perform specific IT functions.

In accordance with FISMA requirements, the BISP notes that all Board employees and contractors with access to Board information systems must receive security awareness training before being permitted access to the organization's network and on an annual basis. The BISP also requires that role-based training be provided for individuals with significant security responsibilities and that records of awareness and role-based training be maintained.

Best practices for developing and implementing a security training program are outlined in NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*. Special Publication 800-50 highlights the important role that training plays in ensuring the effective implementation of an agency's information security program. Further, NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role and Performance Based Model*, establishes a model and requirements for IT system roles and responsibilities. Special Publication 800-16 notes that agencies are expected to find training gaps and establish priorities and strategies for filling them.

Progress to Date

Information security training at the Board is delivered via several online modules. For example, the Board's annual security awareness training module is delivered through an online portal. It focuses on key information security reminders and reviews the organization's information security policies. The Board has also defined and documented the roles, knowledge base, and required and recommended training for personnel with significant security and privacy responsibilities. In October 2016, the Board also developed a specialized security awareness training module for individuals with technical responsibilities.[12]

12. The Board's role-based training for technical staff was implemented after the conclusion of our fieldwork. As such, we did not assess the effectiveness of the training. We will continue to monitor the actions taken by the Board to mature its security awareness and training program as part of our future FISMA audits.

Work to Be Done

We found that the Board can strengthen its security and privacy training program by developing and implementing a process to evaluate its effectiveness. For example, although the Board has conducted social engineering and phishing exercises in the past to measure the effectiveness of its security and privacy training programs, it had not done so in 2016. Board officials notified us that these exercises were not conducted due to resource constraints. As such, the Board may not have complete information with which to make improvements to its security and privacy training program.

An organization's people are often one of the weakest links when it comes to effectively implementing security best practices and guarding against cyberattacks. An organization-wide process to evaluate the effectiveness of Board's security and privacy training program can provide the Board with additional information on user behavior and areas in which additional focus in security awareness may be needed.

Recommendation

We recommend that the CIO

5. Develop and implement a plan to periodically evaluate the effectiveness of the organization's security awareness and training program.

Management's Response

In her response to our report, the Director of the Division of IT states that she agrees with the recommendation and has already initiated actions to address the recommendation.

OIG Comment

In our opinion, the actions described by the Director are responsive to our recommendation. We plan to follow up on the Board's actions to ensure that the recommendation is fully addressed.

Information Security Continuous Monitoring

Requirement

ISCM refers to the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. FISMA emphasizes the importance of continuously monitoring information system security by requiring agencies to conduct assessments of security controls at a risk-based frequency. 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). Given the importance of ISCM in ensuring the security of federal information systems, OMB

designated ISCM as a cybersecurity cross-agency priority for fiscal year (FY) 2015 through FY 2017.

As previously noted, ISCM was the first domain chosen to be assessed under a maturity model approach in DHS's FISMA reporting guidance for IGs because it is a critical governmentwide focus area. Within the maturity model, there are five levels of maturity, of which level 4 (*managed and measurable*) represents an effective program. As outlined in appendix B, DHS has provided a scoring methodology for IGs to utilize in determining the maturity of their agency's ISCM program.

Progress to Date and Work to Be Done

Last year, we found that that the Board's ISCM program was operating at a level 2 (*defined*), with the agency performing several, but not all, recommended activities indicative of higher maturity levels. To mature the Board's information security program, last year we recommended that the CIO (1) develop and implement an organization-wide ISCM lessons-learned process and (2) utilize automation to provider greater visibility into authorized and unauthorized software across the organization.[13]

This year, we found that while the Board has taken several steps to improve the effectiveness of its ISCM program, it continues to operate at a level 2 (*defined*) maturity level. For example, the Board implemented a quarterly ISCM lessons-learned process that is designed to share best practices around management of people, processes, and technologies supporting ISCM activities. As such, we are closing our related 2015 audit recommendation. As detailed below, however, the Board has not implemented an effective process that provides near-real-time visibility into the authorized and unauthorized software across the organization. As such, we are keeping open our related 2015 audit recommendation in this area and will continue to monitor the Board's progress as part of our future FISMA audits.

As described in the following sections, we identified opportunities to mature the Board's ISCM program through greater centralization and automation in the areas of people, processes, and technology. These improvement opportunities largely are a result of the decentralization of IT functions at the Board. Specifically, there are sections within the Board's IT network that are managed outside the direct purview of the Board's Information Security Officer (ISO). Although these sections report ISCM information to the ISO on a periodic basis, we found that the ISO does not have an effective level of visibility into the people, processes, and technologies that are employed in these sections. By taking steps to mature its ISCM program, the Board can have greater visibility into the security posture of all of the organization's systems and more comprehensive information with which to make risk-based decisions.

People

We found that the Board's ISCM program continues to operate at an overall level 2 (*defined*) maturity within the people domain of the ISCM maturity model. Specifically, the Board has fully defined ISCM roles and responsibilities, documented and communicated ISCM policies and procedures across the organization, and hired skilled individuals to perform ISCM duties

13. Office of Inspector General, *2015 Audit of the Board's Information Security Program*, OIG Report 2015-IT-B-019, November 13, 2015.

within the Division of IT. However, we found that the Board has not implemented a consistent approach across the organization for evaluating the skills of individuals with significant security responsibilities and then using that information to provide additional training content to close any identified gaps. We also found that the Board had not provided technical role-based security training in 2015. While this training was provided in late October 2016, we believe that such training should be available on a periodic basis and updated based on changes to the Board's ISCM program and threat environment.

Processes

We found that the Board's ISCM program continues to operate at an overall level 3 (*consistently implemented*) maturity within the processes domain of the ISCM maturity model. Specifically, we found that the Board performs ongoing security control assessments, assesses its systems for technical vulnerabilities using various automated tools, and has begun conducting lessons-learned with stakeholders to facilitate ongoing improvements in the Board's ISCM program. As noted within the Risk Management section of our report, however, for two select systems we found that the Board's processes for security control assessments were not consistently implemented. We also found that the Board was in the process of refining the dashboard used to capture its defined qualitative and quantitative performance measures along with the frequency with which it plans to review such metrics to measure the effectiveness of its ISCM processes.

Technology

We found that the Board's ISCM program continues to operate at an overall level 3 (*consistently implemented*) maturity within the technology domain of the ISCM maturity model. Specifically, the Board has consistently implemented a suite of tools that cover the majority of the automation areas outlined in NIST SP 800-137,[14] including the implementation of a DLP system to monitor and detect data exfiltration and to help prevent intentional and unintentional data leaks. As noted above, however, the Board has not implemented an automated solution that provides near-real-time visibility into the authorized and unauthorized software on its network. Although the Board can enumerate this information for the major operating systems on its network, it cannot readily produce this information for all types of software used across the organization's divisions. Further, we found that although the Board has implemented a security information and event management tool, key information produced by ISCM sources and tools, such as audit logs, is not fully integrated with the tool.

Incident Response

Requirement

Several of the outputs of an effective ISCM program can provide key indicators of an agency's ability to detect, prevent, and respond to computer security incidents in a timely manner. As

14. The 11 automation areas outlined in SP 800-137 are patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management.

computer security incidents affecting the federal government have continued to increase in number and impact, implementing an effective IR and reporting capability has become a critical component of agency information security programs. FISMA requires agencies to develop and implement procedures for detecting, reporting, and responding to security incidents, including mitigating the risks of such incidents before substantial damage is done. FISMA also requires agencies to notify and consult with the United States Computer Emergency Readiness Team (US-CERT). Specifically, agencies are required to notify US-CERT of all computer security incidents involving a federal government information system with a confirmed impact to confidentiality, integrity, or availability within one hour. Further, FISMA requires agencies to report major incidents to Congress within seven days after the date on which there is a reasonable basis to conclude that such incidents have occurred.[15]

DHS's 2016 FISMA reporting guidance for IGs includes a maturity model for the IGs to utilize to determine the effectiveness of agency IR programs. The maturity model incorporates several best practices for incident detection, analysis, and reporting. For instance, the maturity model includes steps to determine agency progress in implementing OMB's TIC Initiative, which aims to optimize and standardize the security of individual external network connections in use by federal agencies, including connections to the Internet. The TIC Initiative was announced in 2007 and requires federal agencies to, among other things, ensure that all external network connections are routed through an OMB-approved TIC provider. These TIC providers are required to provide specific incident detection, prevention, and response capabilities for agencies based on evolving technologies and threats.

Another best practice referenced in the IR maturity model is agency use of DHS's EINSTEIN program, which enhances the ability of participating agencies to provide effective information security protections for their information and information systems. Specifically, DHS's EINSTEIN program detects and blocks cyberattacks from compromising federal agencies and provides DHS with situational awareness by using threat information detected in one agency to protect the rest of the government. DHS's EINSTEIN program is implemented through a combination of commercial-off-the-shelf hardware and software, government-developed software, and commercially available and managed security services.

Progress to Date and Work to Be Done

We found that the Board's IR program is operating at level 1 (*ad hoc*), with the organization performing several activities indicative of a higher maturity level. For instance, the Board has developed policies and procedures for IR activities and also has implemented technologies and processes for identification and tracking of incidents. We identified opportunities to mature the Board's IR program, however, through improvements in policy and implementation of the TIC Initiative and EINSTEIN program. We detail these improvement opportunities within the maturity model domains of people, processes, and technology below.

15. In determining whether an incident is major, OMB has directed agencies to consider whether the incident (1) involves information that is classified, controlled unclassified information proprietary, controlled unclassified information privacy, or controlled unclassified information other; (2) is not recoverable, not recoverable within a specified amount of time, or is recoverable only with supplemental resources; and (3) has a high or medium functional impact to the mission of an agency; or (4) involves the exfiltration, modification, deletion, or unauthorized access or lack of availability to information or systems within certain parameters to include either (a) a specific threshold of number of records or users affected or (b) any record of special importance.

People

We found that the people domain of the Board's IR program is operating at level 1 (*ad hoc*). Specifically, the Board is in the process of updating its *Security Incident Handling Guide* to reflect FISMA requirements for the handling and reporting of major incidents. Further, the Board relies on specific IR and monitoring services provided by the National Incident Response Team, which is a Federal Reserve System provider of IR services. We found that the Federal Reserve System's incident handling standard, while referencing Board policies and procedures, has not been updated to reflect escalation requirements for major incidents that may occur at Federal Reserve Banks that maintain Board information. We believe that the amount of coordination required among the various entities across the Board and the Federal Reserve System has contributed to delays in updating the incident handling standards. As a result, there is increased risk that a major incident may not be handled and reported in a timely manner.

As noted in the ISCM section above, we found that the Board has not implemented a consistent approach across the organization for evaluating the skills of individuals with significant security responsibilities and then using that information to provide additional training content to close any identified gaps. We also found that the Board had not provided role-based technical security training in 2015. While this training was provided in late October 2016, we believe that such training should be available on a periodic basis and updated based on changes to the Board's IR program and threat environment.

Processes

We found that the processes domain of the Board's IR program is operating at level 1 (*ad hoc*), with several, but not all, processes performed at a level 2 (*defined*) maturity. For example, we found that the Board is collecting and analyzing incident data from a number of sources to protect the agency's network. We found, however, that the Board is not reporting lost agency-issued laptops or mobile devices to US-CERT. Board officials informed us that this is because the information stored on the equipment is required to be encrypted. As a result, the resulting risk of data loss may be minimized. However, US-CERT still requires lost encrypted mobile devices to be reported, as these lost laptops represent a loss of availability. As a result, the Board is not benefitting from the IR resources and services that US-CERT may be able to provide.

Similar to the processes domain within ISCM, we also found that the Board has not defined qualitative or quantitative performance measures to gauge the effectiveness of its IR program. Board officials informed us that this has not been completed in part because the information required for effective performance measurement is maintained by several parties. As a result, the Board may not have adequate information with which to make value-added improvements to its IR program.

Technology

We found that the technology domain of the Board's IR program is operating at level 1 (*ad hoc*). The Board utilizes an automated solution for its IR tracking activities and has multiple tools in place for detecting intrusions or threats, including a DLP system. The Board also utilizes the services and technology offered by the National Incident Response Team to monitor

its network and web traffic. However, the Board has not transitioned to a TIC, and as such, it is not participating in DHS's EINSTEIN program. Participation in the TIC Initiative is necessary to ensure that all external connections are monitored by DHS's intrusion detection sensors, which are a key component of the EINSTEIN program. The Board's transition to a TIC and use of DHS's EINSTEIN program have been delayed due to specific privacy concerns with use of the EINSTEIN program, which has recently been resolved in a memorandum of agreement with DHS. As a result, the Board is not benefiting from the capabilities that that a TIC provider and the EINSTEIN program can offer with respect to better detecting, preventing, and responding to external attacks.

Recommendations

We recommend that the CIO

6. Update the Board's *Incident Handling Standard* to include considerations for handling major incidents and work with appropriate parties to ensure that the escalation procedures outlined in the Federal Reserve System's incident handling guide for Board information is updated accordingly.

7. Ensure that all lost laptop computers and mobile devices are reported consistent with guidance from US-CERT.

8. Develop and implement a plan to

    a. transition the Board's external network to a TIC service provider.

    b. utilize the services offered by the DHS EINSTEIN program, as appropriate.

9. Define and implement performance measures to gauge the effectiveness of the Board's IR program, to including services provided by the National Incident Response Team.

Management's Response

In her response to our report, the Director of the Division of IT states that she agrees with the recommendations and has already initiated actions to address the recommendations.

OIG Comment

In our opinion, the actions described by the Director are responsive to our recommendations. We plan to follow up on the Board's actions to ensure that the recommendations are fully addressed.

Status of Prior Years' Recommendations

As part of our annual FISMA audit, we reviewed the actions taken by the Board to address the outstanding recommendations from our prior years' FISMA reviews. Below is a summary of the status of the four recommendations that were open at the start of our 2016 FISMA audit. Based on corrective actions taken by the Board, we are closing three prior recommendations related to ISCM, configuration management, and identity and access management. One recommendation related to strengthening the Board's software asset management process will remain open. We will update the status of these recommendations in our upcoming *Semiannual Report to Congress* and continue to monitor the Board's progress in addressing the one open recommendation as a part of future FISMA reviews.

Information Security Continuous Monitoring

In our 2015 FISMA report, we recommended that the CIO develop and implement an enterprise-wide ISCM lessons-learned process that captures best practices in the domains of people, processes, and technologies and use these lessons-learned to make timely updates to the Board's ISCM program. This year, we found that the Board is conducting lessons-learned discussions at the program level. Specifically, the Board's ISO is holding regularly scheduled meetings with ISCM stakeholders throughout the agency. These meetings are designed to discuss the state of the organization's ISCM program, including strengths of the program, areas for improvement, and how the Division of IT can provide further support to Board divisions. As such, we conclude that sufficient actions have been taken to close this recommendation.

Our 2015 FISMA report also included a recommendation for the CIO to strengthen the Board's software asset management processes by using automation to provide greater visibility into authorized and unauthorized software across the organization. This year, we found that although Board officials with ISCM responsibilities have the capability of producing a point-in-time inventory of their hardware and software, the process is still not automated. Specifically, the Board can enumerate the software applications that are components of its major operating systems, but it does not have the means to timely produce an inventory of all software applications installed on the organization's network or the security status of those applications. Therefore, we are leaving this recommendation open, and we will continue to monitor the Board's progress in this area as part of our future audit activities.

Configuration Management

As a part of our 2015 FISMA audit, we recommended that the CIO develop and implement a process, including updating supporting policies and procedures, to perform periodic database-level vulnerability scanning for a key database technology. This year, we found that the Board has developed a process to perform database-level vulnerability scans, procured additional software licenses for scanning purposes, and performed scanning of the key database

technology. As such, we conclude that sufficient actions have been taken to close this recommendation.

Identity and Access Management

In our 2015 FISMA report, we recommended that the CIO implement a process to periodically monitor access control settings for sensitive Board information in the enterprise-wide collaboration tool. This year, we found that the Division of IT implemented a weekly access validation process whereby reports are provided to Board divisions informing them of which groups and users have access to individual sites within the tool. Board divisions are also encouraged to provide an annual assessment form to the Division of IT that indicates that permissions and access lists have been reviewed. The Division of IT has also offered training to administrators of the enterprise-wide collaboration tool on access control settings. As such, we conclude that sufficient actions have been taken to close this recommendation.

Appendix A
Scope and Methodology

Our specific audit objectives, based on the requirements of FISMA, were to evaluate the effectiveness of the Board's (1) security controls and techniques 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 eight areas outlined in DHS's *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*. These areas are ISCM, configuration management, identity and access management, IR, risk management, security and privacy training, contingency planning, and contractor systems.

To assess the Board's information security program in these areas, we interviewed Board management and staff; analyzed security policies, procedures, and documentation; and observed and tested specific security processes and controls. We also assessed the implementation of select security controls for two agency systems and performed vulnerability scanning at the network and operating system levels on select IT devices. We used the results of our review of the Board's information security program and testing of controls for two agency systems to evaluate the implementation of specific attributes outlined in DHS's 2016 FISMA reporting guidance for IGs.

We performed our fieldwork from July 2016 to October 2016. 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
FISMA Scoring Methodology

This appendix contains the scoring methodology contained in DHS's *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*. IGs are required to use this methodology to determine the maturity level of their respective agency's information security programs. Specifically, based on the IGs' assessments, agencies are allotted points for each cybersecurity framework function area based on their achievement of various levels of maturity. For each framework function, a total of 20 points is possible. Last year, when determining the overall maturity for an agency's program, a lowest common denominator approach was used, meaning an agency could only meet a particular level of maturity if they met all ISCM security metrics defined for that level. The FY 2016 IG FISMA reporting metrics continue the effort begun in 2015; however, the lowest common denominator scoring approach has been removed. The scoring methodology for each maturity level is provided in table 2 below.

Table B-1: Maturity Level Scoring Methodology

Maturity level	Scoring description	Scoring distribution
Level 1: *ad hoc*	Automatically receives points regardless of achievements.	3 points
Level 2: *defined*	For the identify, protect, and recover function areas, met at least half the metrics designated at level 2 (*defined*). For the detect and respond function areas, met all metrics designated at level 1 (*ad hoc*) and at least half those designated at level 2 (*defined*).	4 points
Level 3: *consistently implemented*	For all function areas, met all metrics designated at level 2 (*defined*) and at least half those designated at level 3 (consistently implemented).	6 points
Level 4: *managed and measurable*	For all function areas, met all metrics designated at level 3 (*consistently implemented*) and at least half those designated at level 4 (*managed and measurable*).	5 points
Level 5: *optimized*	For all function areas, met all metrics designated at level 4 (*managed and measurable*) and level 5 (*optimized*).	2 points

Source: OIG analysis of DHS's *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*.

Appendix C
Management's Response

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D.C. 20551

DIVISION OF
INFORMATION TECHNOLOGY

November 8, 2016

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 "2016 Audit of the Board's Information Security Program" prepared as part of your office's oversight responsibilities pursuant to 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 policies, procedures, standards, and guidelines. The report also addresses the successful completion of remediation of 3 of 4 recommendations made by the Inspector General in the "2015 Audit of the Board's Information Security Program." We are pleased that your assessment continues to recognize that the Board operates a comprehensive and effective information security program and recognizes the progress we continue to make to enhance the program.

We agree with the recommendations offered in your report. We have already initiated actions to address the recommendations. This includes continuing to enhance the Board's Risk Management and Continuous Monitoring Programs. The Information Technology Division's Plan of Actions and Milestones will be updated to reflect these corrective actions.

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
Director, Information Technology

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

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

HOTLINE

1-800-827-3340

OIGHotline@frb.gov

Report Fraud, Waste, and Abuse

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, e-mail, fax, or telephone.

Office of Inspector General, c/o Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW, Mail Stop K-300, Washington, DC 20551
Attention: OIG Hotline

Fax: 202-973-5044

Questions about what to report?

Visit the OIG website at www.federalreserve.gov/oig
or
www.consumerfinance.gov/oig