OFFICE OF INSPECTOR GENERAL

Audit Report 2015-IT-B-019

2015 Audit of the Board's Information Security Program

November 13, 2015

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

Report Contributors

Chris Lambeth, Project Lead
Andrew Gibson, Senior IT Auditor
Kaneisha Johnson, IT Auditor
Amanda Sundstrom, IT Auditor
Chelsea Willis, IT Auditor
Khalid Hasan, Senior OIG Manager
Peter Sheridan, Assistant Inspector General for Information Technology

Abbreviations

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
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
IG	Inspector General
ISCM	information security continuous monitoring
ISO	Information Security Officer
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	plan of action and milestones
SP 800-53	Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
SP 800-137	Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*

Executive Summary:

2015 Audit of the Board's Information Security Program

2015-IT-B-019 **November 13, 2015**

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 (1) the Board's compliance with FISMA and related information security policies, procedures, standards, and guidance and (2) the effectiveness of security controls and techniques for a subset of the Board's information systems.

Background

FISMA requires federal agencies to develop, document, and implement an agency-wide information security program. FISMA also requires each Inspector General (IG) to conduct an annual independent evaluation of the agency's information security program and practices. The U.S. Department of Homeland Security (DHS) has issued guidance to IGs on FISMA reporting for 2015. The guidance directs IGs to evaluate the performance of agencies' information security programs across 10 areas. These areas are continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, and contractor systems.

Findings

Overall, we found that the Board's Chief Information Officer has developed, documented, and implemented an information security program that is generally consistent with the requirements established by FISMA and the 10 areas outlined in DHS's FISMA reporting guidance for IGs. This year, we found that the Board has taken steps to mature the organization's information security continuous monitoring (ISCM) program through the development of metrics and monitoring frequencies. We also found that the Board has strengthened its risk management processes by automating the collection and review of plans of actions and milestones, and enhanced its contractor oversight processes to better ensure that third-party systems meet FISMA and Board requirements.

While we found the Board's information security program to be consistent with requirements outlined in DHS's FISMA reporting guidance for IGs, we identified further opportunities to strengthen the program in the areas of ISCM, configuration management, and identity and access management. Specifically, we found that the Board can mature its ISCM program through greater centralization and automation in the areas of people, processes, and technology; develop and implement a process to manage database-level vulnerabilities using automated tools for a key database technology used in the organization; and improve access controls for sensitive Board information maintained in the organization's enterprise-wide collaboration tool.

Recommendations

Our report includes four recommendations to improve the Board's information security program in the areas of ISCM, configuration management, and identity and access management. In her response to our report, the Director of the Division of Information Technology concurs with our recommendations and notes that actions are underway to address them. Further, based on corrective actions taken by the Board's Information Security Officer, we are closing the open recommendations from our prior years' FISMA reports related to contractor systems, ISCM, and plan of action and milestones.

Summary of Recommendations, OIG Report No. 2015-IT-B-019

Rec. no.	Report page no.	Recommendation	Responsible office
1	6	Develop and implement an organization-wide information security continuous monitoring lessons-learned process that captures best practices in people, processes, and technologies and uses these lessons learned to make timely updates to the Board's information security continuous monitoring program.	Division of Information Technology
2	6	Strengthen the Board's software asset management processes by using automation to provide greater visibility into authorized and unauthorized software across the organization.	Division of Information Technology
3	7	Develop and implement a process, including updating supporting policies and procedures, to perform periodic database-level vulnerability scanning for the key database technology we identified.	Division of Information Technology
4	9	Implement a process to periodically monitor access control settings for sensitive Board information in the enterprise-wide collaboration tool.	Division of Information Technology

Office of Inspector General

Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

November 13, 2015

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 No. 2015-IT-B-019: *2015 Audit of the Board's Information Security Program*

The Office of Inspector General (OIG) is pleased to present its report on the 2015 audit of the information security program of the Board of Governors of the Federal Reserve System (Board). We performed this audit pursuant to requirements in the Federal Information Security Modernization Act of 2014 (FISMA), which requires each agency Inspector General to conduct an annual independent evaluation of the agency's information security program and practices.

We provided a draft of our report to you for review and comment. In your response, you note that actions are underway to address our recommendations. We have included your response as appendix B to our report. We will use the results of our review of the Board's information security program and practices to respond to specific questions in the U.S. Department of Homeland Security's *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*.

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 Hammond
Raymond Romero
Charles Young
William Mitchell
J. Anthony Ogden

Contents

Introduction 1

Objectives 1
Background 1

Summary of Findings 2

Analysis of the Board's Progress in Implementing Key FISMA, OMB, and DHS Requirements 3

Information Security Continuous Monitoring 3
Configuration Management 6
Identity and Access Management 8
Status of Prior Years' Recommendations 9

Appendix A: Scope and Methodology 11

Appendix B: Management's Response 13

Introduction

Objectives

Our specific audit objectives, based on the requirements of the Federal Information Security Modernization Act of 2014 (FISMA),[1] were to evaluate (1) the Board of Governors of the Federal Reserve System's (Board) compliance with FISMA and related information security policies, procedures, standards, and guidance and (2) the effectiveness of security controls and techniques for a subset of the Board's information systems. Our scope and methodology are detailed in appendix A.

Background

FISMA provides a framework for ensuring the effectiveness of information security controls over federal operations and assets and a mechanism for the oversight of federal information security programs. FISMA requires agencies to develop, document, and implement an agency-wide information security program for the information and information systems that support the operations and assets of the agency, including those provided by another agency, a contractor, or other source. The legislation also requires each agency Inspector General (IG) to perform an annual independent evaluation of the information security program and practices of its respective agency to determine the effectiveness of such program and practices.

The U.S. Department of Homeland Security (DHS) has issued guidance to IGs on FISMA reporting for 2015.[2] The guidance directs IGs to evaluate the performance of agencies' information security programs across 10 areas. These areas are information security continuous monitoring (ISCM), configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones (POA&M), remote access management, contingency planning, and contractor systems. In 2015, DHS's FISMA reporting guidance for IGs was updated to remove the security capital planning family and to include a maturity model for IGs to use in assessing the effectiveness of agencies' ISCM programs. The purpose of the maturity model is to (1) summarize the status of agencies' ISCM programs and their maturity; (2) provide transparency to agency Chief Information Officers (CIO), top management officials, and other interested readers of IG FISMA reports about what has been accomplished and what still needs to be implemented to improve ISCM programs; and (3) help ensure consistency across the IGs in their annual FISMA reviews.

1. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-228, 128 Stat. 3073 (2014) (codified at 44 U.S.C. §§ 3551–58).

2. U.S. Department of Homeland Security, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, June 19, 2015.

Summary of Findings

Overall, we found that the Board's CIO has developed, documented, and implemented an information security program that is generally consistent with the requirements of FISMA and the 10 areas outlined in DHS's FISMA reporting guidance for IGs. This year, we found that the Board's Information Security Officer (ISO) has taken steps to mature the organization's ISCM program through the development of metrics and monitoring frequencies. We also found that the Board has strengthened its risk management processes by automating the collection and review of POA&Ms. In addition, the Board enhanced its contractor oversight processes to better ensure that third-party systems meet FISMA and Board requirements. As a result of these actions, we closed the open recommendations from our prior years' FISMA reports related to strengthening the Board's ISCM, contractor oversight, and POA&M processes.

We identified additional opportunities to strengthen the Board's information security program in the areas of ISCM, configuration management, and identity and access management through greater centralization and automation. Specifically, we found that the decentralization of information technology (IT) functions is limiting the Board's ability to mature its ISCM program. For example, the Board does not have an organization-wide approach to managing the knowledge, skills, and abilities of individuals performing ISCM activities or for using lessons learned to improve the ISCM program. Further, we found that the Board cannot readily produce an accurate inventory of all the software installed on its network or the security configurations of all its software. We also found that while the Board uses a variety of tools to identify vulnerabilities in its IT environment, the organization did not have an automated tool or process in place to perform vulnerability scanning on a key database technology that supports several systems. Finally, we identified several instances of sensitive Board information that was maintained in the organization's enterprise-wide collaboration tool and not restricted to individuals with a need to know.

Information Security Continuous Monitoring

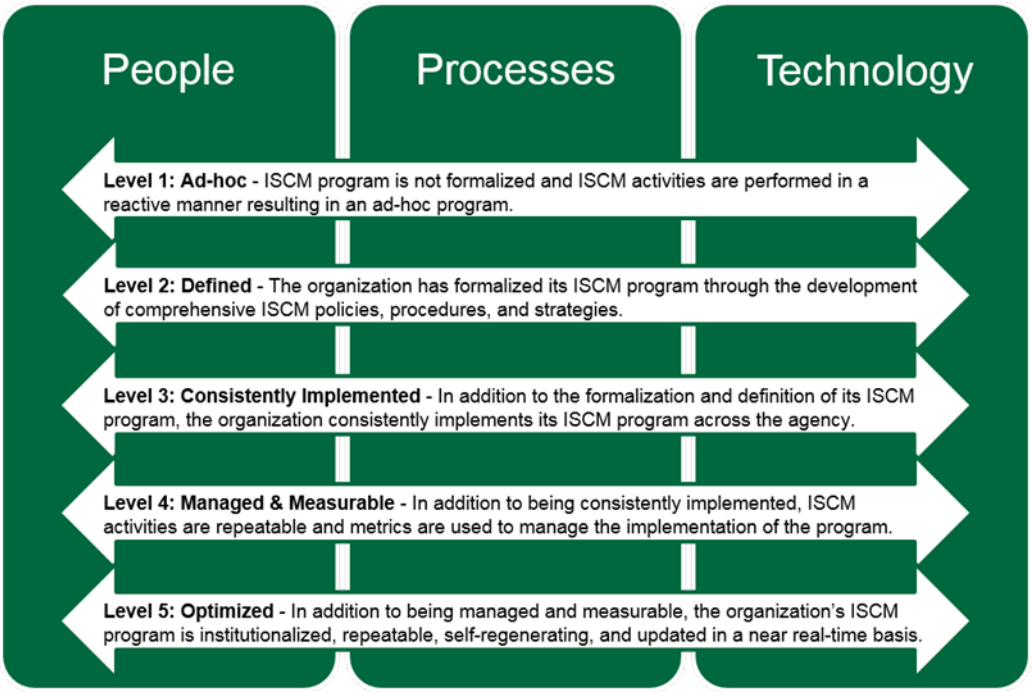
National Institute of Standards and Technology (NIST) Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (SP 800-137), defines ISCM as the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The Board's ISO has developed and implemented an ISCM program that is generally consistent with federal requirements; however, we identified opportunities to mature the Board's ISCM program through greater centralization and automation in the areas of people, processes, and technology. For instance, we found that the Board does not have an organization-wide view of the knowledge, skills, and abilities of individuals performing ISCM functions. In addition, we found that the Board's ISCM program did not include a formal process to incorporate lessons learned across the organization to drive improvements to the program. Finally, we found that the Board cannot readily produce an accurate inventory of all the software installed on its network or the security configurations of all its software. A key reason for these issues is the decentralization of IT functions at the Board. As a result of this decentralization, the Board's ISO may not have an optimal level of situational awareness and insight into the effectiveness of the people, processes, and technologies supporting ISCM.[3]

ISCM has been designated by the Office of Management and Budget (OMB) as a cross-agency priority goal, with the intent to transform the historically static security control assessment and authorization process into an integral part of a dynamic enterprise-wide risk-management process.[4] To provide a greater perspective on the overall status of agencies' ISCM programs, the Council of the Inspectors General on Integrity and Efficiency, in coordination with DHS, OMB, and other stakeholders, developed an ISCM maturity model for use by IGs as part of their fiscal year (FY) 2015 FISMA reviews. Referencing existing ISCM requirements and guidance, the maturity model includes steps to assess an agency's ISCM program through an analysis of three domains: people, processes, and technology. Figure 1 provides a summary of the five maturity levels of the ISCM maturity model.

3 We also identified implementing a Boardwide ISCM program that complies with NIST requirements as a management challenge for the Board. See Office of Inspector General, *Major Management Challenges for the Board of Governors of the Federal Reserve System*, September 30, 2015.

4 The cross-agency priority goals were introduced in the fiscal year 2013 federal budget and focus on 14 major issues that run across several federal agencies.

Figure 1: ISCM Maturity Model



Source: Office of Inspector General analysis of DHS's FY 2015 FISMA reporting guidance for IGs.

The maturity levels of the people, processes, and technology domains indicate the overall maturity of an organization's ISCM program. Specifically, as noted in DHS's FY 2015 FISMA guidance for IGs, the "lowest common denominator" approach shall apply when determining the overall maturity level for an organization's ISCM program. Accordingly, we determined that the Board's ISCM program is operating at an overall level 2, although the Board is performing several activities at level 3.[5] The following sections highlight the actions taken by the Board's ISO to mature the Board's ISCM program, as well as additional improvements that are needed in the areas of people, processes, and technology.

People

Best practices that are referenced in the ISCM maturity model note that agencies shall ensure that adequate staff and training are in place to meet the objectives of their ISCM programs. Along these lines, agencies should identify resource and skill requirement gaps (if any) to manage and coordinate their ISCM programs.[6] The Board has defined and communicated roles and responsibilities for implementing its ISCM program. Additionally, Board officials informed us that through the Board's hiring processes, individuals who will be performing ISCM duties

5 The complete ISCM maturity model, including the various attributes that IGs are to assess for maturity in the people, processes, and technology domains, is included in DHS's FY 2015 FISMA reporting guidance for IGs, which is available at http://www.dhs.gov/publication/fy15-fisma-documents.

6. Office of Management and Budget, *Enhancing the Security of Federal Information and Information Systems*, OMB Memorandum M-14-03, November 18, 2013.

are screened for the requisite knowledge, skills, and abilities. Additional skills related to the specific tools used by the Board as part of its ISCM program are gained through training.

We found that due to the decentralization of IT functions, the Board does not have an organization-wide view of the knowledge, skills, and abilities of individuals performing ISCM activities. Specifically, the Board's ISCM program is managed by the IT security unit, which is headed by the Board's ISO in the Division of Information Technology (Division of IT). We noted that the ISO has visibility into the knowledge, skills, abilities, and training of individuals in the IT security unit who are performing ISCM functions. Some functions associated with ISCM are performed outside the IT security unit, however, and the Board's ISO does not have direct oversight of and visibility into the knowledge, skills, and abilities of the individuals performing these functions. As such, from an organization-wide perspective, the ISO cannot ensure that adequate staff and knowledge are in place to meet the objectives of the Board's ISCM program.

Processes and Technology

Best practices that are referenced in the ISCM maturity model note that agencies should define and consistently implement processes in the areas of ongoing assessment and monitoring, hardware and software asset management, common vulnerability management, reporting, and continuous improvement. DHS's FY 2015 FISMA reporting guidance for IGs emphasizes that one of the first areas in which ISCM processes should be developed is asset management. Specifically, organizations must first know about the devices and software installed on their networks before they can manage the configurations and vulnerabilities of those devices and software. Further, in support of an organization's ISCM processes, SP 800-137 notes that automation can be used to lower costs, enhance efficiency, and improve the reliability of monitoring security-related information. SP 800-137 highlights 11 automation domains, including asset management, configuration management, information management, and software assurance.

We found that the Board has defined and communicated ISCM processes in most of the areas noted in the ISCM maturity model. However, we identified that the Board does not have an organization-wide process for consistently capturing lessons learned on the effectiveness of its ISCM processes and then using those lessons learned for making timely updates to its ISCM program. In addition, the Board's ISO does not have an optimal level of oversight into the processes and technologies being used in support of ISCM activities performed outside the Division of IT. A formal, organization-wide lessons learned process could help ensure the effective implementation of the Board's ISCM program through greater sharing of best practices and more timely and relevant updates to supporting policies and procedures.

We also found that the Board has implemented technologies in the areas of hardware and software asset management, configuration management, and vulnerability management. However, we noted that the Board does not have an organization-wide process for effective software asset management. For instance, while the Board can enumerate devices on the major operating system components of its network, we found that the organization cannot readily produce an accurate point-in-time inventory of all the authorized and unauthorized software on its network. Board officials informed us that the organization has controls in place to restrict installation of unauthorized software and remove such software, if necessary. As a result, the Board's ISO may be unable to maintain an effective level of situational awareness of the

security status of all the organization's systems and may not have the ability to quickly react to changing security situations.

As noted earlier, a key reason for these issues in 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 ISO. While these sections report ISCM information to the ISO on a periodic basis, we found that the ISO does not have visibility over the people, processes, and technologies that are employed in these sections.

Recommendations

We recommend that the CIO

1. Develop and implement an organization-wide ISCM lessons-learned process that captures best practices in people, processes, and technologies and uses these lessons learned to make timely updates to the Board's ISCM program.

2. Strengthen the Board's software asset management processes by using automation to provide greater visibility into authorized and unauthorized software across the organization.

Management's Response

The Director of the Division of IT stated that she agrees with the recommendations and has already begun taking actions to address the recommendations. These actions include continuing to enhance the Board's continuous monitoring program.

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.

Configuration Management

From an information security perspective, *configuration management* refers to establishing and maintaining the integrity of products and systems through control of the processes for initializing, changing, and monitoring their security configurations. Vulnerability scanning, which is the use of automated tools to identify security misconfigurations, outdated software, and missing patches, is one way to ensure that adequate security configurations are maintained. While the Board has implemented several vulnerability scanning tools, we found that the agency had not developed a process to perform vulnerability scanning on a key database technology that is used in support of several information systems. A main reason for this is that the *Board Information Security Program* (BISP) does not include specific requirements and guidance for database-level scanning; as a result, we noted that scanning was not being

performed. Therefore, the Board is not adequately managing the risk of key database vulnerabilities in its environment.

The Board uses automated tools to conduct periodic vulnerability scanning on its network devices, operating systems, and applications. In addition, the Board uses a specific automated tool to perform database-level scanning for the databases supporting its financial and human resource systems. However, we found that the Board had not developed a process to perform database-level vulnerability scanning for a key database technology that supports multiple systems across the agency. We performed database-level vulnerability scanning for select systems that use this database technology and found several vulnerabilities that had not been identified by the Board. As a result of these vulnerabilities, there is an increased risk to the confidentiality, integrity, and availability of Board information and systems that rely on this database technology.

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (SP 800-53), recommends that organizations scan for vulnerabilities in information systems and hosted applications, analyze the results, remediate vulnerabilities, and share information with appropriate stakeholders. Further, NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, notes that automated tools can be used to scan various information system components (e.g., Web server, database server, and network devices) running different operating systems to identify the current configuration settings and indicate where they are noncompliant with policies.

A contributing factor for this issue is the lack of clear policy and guidance. While the BISP notes that vulnerability scanning must be conducted on workstations and servers, it does not specifically mention database-level requirements. Board IT security officials also noted that ongoing database-level vulnerability scanning was conducted in the past for the database technology in question, but they were unclear why this practice had stopped. As a result, the Board is not adequately managing the risk of key database vulnerabilities in its environment.

Recommendation

We recommend that the CIO

3. Develop and implement a process, including updating supporting policies and procedures, to perform periodic database-level vulnerability scanning for the key database technology we identified.

Management's Response

The Director of the Division of IT stated that she agrees with the recommendation and has already begun taking 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.

Identity and Access Management

Identity and access management includes the implementation of 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*. Although the BISP requires access to be based on a user's business need, we identified sensitive information maintained in the Board's enterprise-wide collaboration tool that was not restricted to individuals with a need to know. This resulted primarily from users not properly restricting access to documents they created or uploaded to the enterprise-wide collaboration tool, as well as a lack of ongoing monitoring of access control settings. As a result, there is heightened risk of unauthorized disclosure or inappropriate use of sensitive Board information.

We identified several instances of sensitive information that was maintained in the Board's enterprise-wide collaboration tool and available to all Board and Federal Reserve System employees with a network-level login.[7] We issued an early alert memorandum to Board management outlining our observations in these areas, as well as suggestions for strengthening security controls. We recognize that the Board is in the process of taking action to address our observations and suggestions.

The BISP requires access controls to be implemented for all information systems to ensure that each user is accountable for his or her actions and to protect data and equipment from malicious or accidental unauthorized access, damage, or loss. In addition, the BISP states that only authorized users can have accounts on an information system and that user authorization must be based on business requirements. Further, SP 800-53 requires least privilege to be used for systems of moderate or higher risk. *Least privilege* involves ensuring that users have access to only those resources that they need to accomplish their job functions.

We identified three key reasons that sensitive information was not appropriately restricted within the Board's enterprise-wide collaboration tool. First, users were not properly restricting access to documents they created or uploaded to the tool. Second, the Board did not provide comprehensive training to these users and other individuals responsible for ensuring the security of information in the enterprise-wide collaboration tool. Third, administrators in Board divisions were not periodically monitoring access control settings for sensitive documents stored in the tool. As a result, there is heightened risk of unauthorized disclosure and inappropriate use of sensitive Board information. We recognize that the Board has taken steps to address our concerns with access to sensitive information maintained in the enterprise-wide collaboration tool by strengthening its annual site validation and training processes.

7. The Board maintains trust relationships with the Federal Reserve Banks that enable employees and contractors of the Reserve Banks who have a network-level login to access specific Board resources, including the agency's enterprise-wide collaboration tool.

Recommendation

We recommend that the CIO work with the Board divisions and the Federal Reserve Banks, as appropriate, to

4. Implement a process to periodically monitor access control settings for sensitive Board information in the enterprise-wide collaboration tool.

Management's Response

The Director of the Division of IT stated that she agrees with the recommendation and has already begun taking 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.

Status of Prior Years' Recommendations

As part of our annual FISMA audit, we reviewed the actions taken by the Board to address outstanding recommendations from our prior years' FISMA reviews. Below is a summary of the status of the recommendations that were open at the start of our 2015 FISMA audit. Based on corrective actions taken by the Board's ISO, we are closing our prior years' recommendations related to contractor systems, ISCM, and POA&M. We will update the status of these recommendations in our upcoming *Semiannual Report to Congress*.

Contractor Systems

In our 2012 FISMA report, we recommended that the CIO develop and implement a security review process for third-party systems located outside the Federal Reserve System to ensure that these systems employ information security controls sufficient to meet the requirements of the BISP and NIST. In 2015, the ISO established a third-party review process that addresses the majority of NIST controls. The process includes questionnaires that are a part of all request for proposals, and these questionnaires are then used by the Board's ISO to determine a security risk level for third-party systems. The security risk level drives the level of assurance that is required during security reviews, as well as the frequency of monitoring activities. In addition, security assessments are required to be completed for all third-party systems. Therefore, we conclude that the Board has taken sufficient actions to address our 2012 recommendation for contractor systems.

Information Security Continuous Monitoring

In our 2013 FISMA report, we recommended that the CIO continue to establish a continuous monitoring program by finalizing policies and procedures, establishing metrics, and defining the frequency of monitoring. In 2014, we found that the Board's ISO had finalized the *Continuous Monitoring Standard* but had yet to establish metrics and define the frequency of monitoring activities. As a result, this recommendation was carried forward. In 2015, we found that the ISO developed initial metrics and established frequencies for continuous monitoring activities. Therefore, we conclude that the Board has taken sufficient actions to address our 2013 recommendation for continuous monitoring.

Plan of Actions and Milestones

In our 2014 FISMA report, we recommended that the CIO ensure, until the automated POA&M tracking process has been implemented, that all division POA&Ms are collected and reviewed on a quarterly basis for inclusion in Boardwide performance reporting, including reviewing POA&M items to ensure that milestone dates are consistently included. In 2015, Division of IT officials informed us that all division POA&Ms are now managed in the Board's online FISMA management tool, where they are reviewed on a biannual basis. This process also enables the Board's ISO to perform an on-demand review of POA&Ms if particular issues arise. In addition, the Board's *Information Security Plans of Actions and Milestones Reporting Guidance for Board Divisions and Offices* was updated in October 2015 to remove the quarterly POA&M review requirement. The update now states that the CIO must centrally track, maintain, and review POA&M activities at least biannually. Therefore, we conclude that the Board has taken sufficient actions to address our 2014 recommendation for POA&Ms.

Appendix A
Scope and Methodology

To accomplish our audit objectives, we reviewed the effectiveness of the Board's information security program across the 10 areas outlined in DHS's 2015 FISMA reporting guidance for IGs. These areas are ISCM, configuration management, identity and access management, incident response and reporting, risk management, security training, POA&M, remote access management, 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 audit the security controls implemented for the Board's IT systems and processes on an ongoing basis. We incorporated the results of these reviews, as appropriate, into our 2015 FISMA audit, including our response to specific questions in DHS's 2015 FISMA reporting guidance for IGs. During the past fiscal year, we issued the following reports:

- *The Board Can Better Coordinate Its Contingency Planning and Continuity of Operations Program*, OIG Report No. 2014-IT-B-018, October 30, 2014
- *Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board's Information Security Life Cycle*, OIG Report No. 2015-IT-B-021, December 18, 2014
- *Audit of the Planned Physical and Environmental Controls for the Board's Data Center Relocation*, OIG Report No. 2015-IT-B-001, January 30, 2015
- *Security Control Review of the Board's Consolidated Supervision Comparative Analysis, Planning and Execution System*, OIG Report No. 2015-IT-B-015, September 2, 2015
- *The Board Continues to Follow a Structured Approach to Planning and Executing the Relocation of the Data Center*, OIG Report No. 2015-IT-B-017, September 16, 2015

Additionally, during 2015, we completed fieldwork on our *Security Control Review of the Board's Active Directory Implementation* and used the results to answer specific questions in DHS's 2015 FISMA reporting guidance for IGs. We also performed reviews of the status of open audit recommendations for the following OIG information security–related audits:

- *Security Control Review of a Third-party Commercial Data Exchange Service Used by the Board's Division of Banking Supervision and Regulation*, OIG Report No. 2013-IT-B-010, August 6, 2013
- *Security Control Review of the Board's National Examination Database System*, OIG Report No. 2013-IT-B-009, July 19, 2013
- *Security Control Review of the Federal Reserve Bank of Richmond's Lotus Notes Systems Supporting the Board's Division of Banking Supervision and Regulation*, August 8, 2012

We conducted our fieldwork from July 2015 to October 2015. 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 obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B
Management's Response

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

DIVISION OF
INFORMATION TECHNOLOGY

November 10, 2015

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 "2015 Audit of the Board's Information Security Program" prepared as part of your office's oversight responsibilities pursuant to the Federal Information Security Management Act of 2002 (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 all recommendations made by the Inspector General FISMA reports in prior years. 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 Continuous Monitoring Program. 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