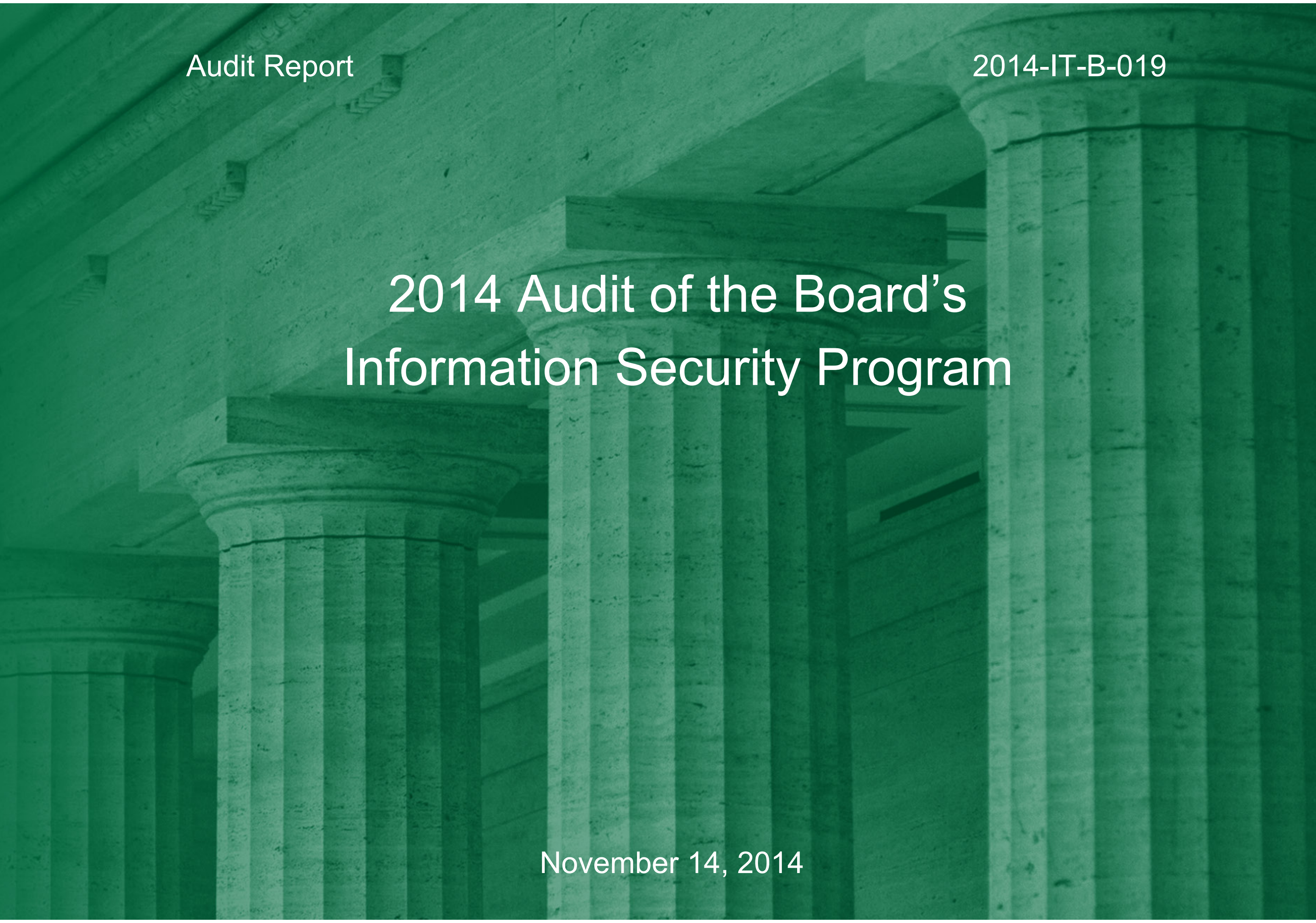
Office of Inspector General



Audit Report

2014-IT-B-019

2014 Audit of the Board's Information Security Program

November 14, 2014

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

Report Contributors

Andrew Gibson, Project Lead
Chris Lambeth, Senior IT Auditor
Adam Scheps, IT Auditor
Peter Sheridan, Senior OIG Manager for Information Technology Audits
Andrew Patchan Jr., Associate Inspector General for Information Technology

Abbreviations

Board	Board of Governors of the Federal Reserve System
CIO	Chief Information Officer
COOP	continuity of operations program
DHS	U.S. Department of Homeland Security
Division of IT	Division of Information Technology
FISMA	Federal Information Security Management Act of 2002
ISC	Information Security Compliance
ISCM	information security continuous monitoring
ISO	Information Security Officer
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POA&M	plan of action and milestones
RMF	Risk Management Framework
SP 800-37	Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*
SP 800-39	Special Publication 800-39, *Managing Information Security Risk*
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:

2014 Audit of the Board's Information Security Program

2014-IT-B-019 November 14, 2014

Purpose

To meet our annual Federal Information Security Management Act of 2002 (FISMA) reporting responsibilities, we reviewed the information security program and practices of the Board of Governors of the Federal Reserve System (Board).

Background

FISMA requires federal agencies to develop, document, and implement an agency-wide information security program. FISMA also requires each Inspector General to conduct an annual independent evaluation of its agency's information security program and practices.

As part of an agency's annual FISMA reporting, the Office of Management and Budget (OMB) requests that both the Chief Information Officer (CIO) and the Inspector General perform analysis and report on certain information security program components. As discussed in OMB Memorandum 10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, the U.S. Department of Homeland Security (DHS) exercises primary responsibility within the executive branch for the operational aspects of federal agency cybersecurity with respect to FISMA.

Findings

Overall, we found that the Board's CIO is maintaining a FISMA-compliant approach to the Board's information security program that is generally consistent with requirements established by the National Institute of Standards and Technology and OMB. The Information Security Officer continues to issue policies and procedures to transition the Board's information security program to an integrated, organization-wide program for managing information security risks.

In analyzing the status of the Board's information security program in the 11 DHS reporting metrics for 2014, we found that the Board has effective programs in place that are consistent with FISMA requirements and that include attributes identified by DHS for risk management, security configuration, remote access, identity and access management, security training, incident response and reporting, and security capital planning. We also found that the Board has programs in place that include attributes identified within the DHS reporting metrics for continuous monitoring, contractor oversight, contingency planning, and plan of action and milestones; however, we identified opportunities for improvement within those areas. Our findings related to contingency planning are being reported under separate cover.

Recommendations

Our report includes one new recommendation for improving the tracking of division-level plans of action and milestones and keeps open our 2012 recommendation on contractor systems and our 2013 recommendation on continuous monitoring.

The Director of the Division of Information Technology stated that she agrees with the recommendation and that the division will take immediate action to address the recommendation, including continuing to manually collect quarterly plan of action and milestones reports from the offices and divisions until the automated plan of action and milestones tracking process is fully implemented.

Summary of Recommendations, OIG Report No. 2014-IT-B-019

Rec. no.	Report page no.	Recommendation	Responsible office
1	10	Ensure, until the automated plan of action and milestones (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.	Division of Information Technology

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

November 14, 2014

MEMORANDUM

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

FROM: Andrew Patchan Jr. Andrew Patchan Jr.
Associate Inspector General for Information Technology

SUBJECT: OIG Report No. 2014-IT-B-019: *2014 Audit of the Board's Information Security Program*

The Office of Inspector General is pleased to present its report on the 2014 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 Management Act of 2002 (FISMA), Title III, Public Law 107-347 (December 17, 2002), 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 for review and comment. In your response, you outlined actions that have been or will be taken to address our recommendation. 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 2014 Inspector General Federal Information Security Management 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, Chief Operating Officer
Raymond Romero, Chief Privacy Officer
Charles Young, Information Security Officer
William Mitchell, Chief Financial Officer
J. Anthony Ogden, Deputy Inspector General
Matt Simber, OIG Manager for Policy, Planning, and Quality Assurance

Contents

Introduction

Objectives

Our specific audit objectives, based on the requirements of the Federal Information Security Management Act of 2002 (FISMA),[1] were to evaluate the effectiveness of the security controls and techniques for select information systems of the Board of Governors of the Federal Reserve System (Board) and to evaluate the Board's compliance with FISMA and related information security policies, procedures, standards, and guidelines. 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 to provide information security 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.

Agency information security programs must provide for, among other things, periodic risk assessments, policies and procedures based on the risk assessments, periodic testing and evaluation of the effectiveness of policies and procedures, security planning, security awareness training, and continuity of operations. FISMA also requires each agency Inspector General 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. As discussed in Office of Management and Budget (OMB) Memorandum 10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, the U.S. Department of Homeland Security (DHS) exercises primary responsibility within the executive branch for the operational aspects of federal agency cybersecurity with respect to FISMA.

[1] Title III, Public Law 107-347 (December 17, 2002).

Summary of Findings

Overall, we found that the Board's Chief Information Officer (CIO) continues to maintain a FISMA-compliant approach to the Board's information security program that is generally consistent with requirements established by the National Institute of Standards and Technology (NIST) and OMB. The Information Security Officer (ISO) continues to issue policies and procedures that include attributes identified within the DHS reporting metrics.

In analyzing the status of the Board's information security program within the 11 DHS reporting metrics for 2014, we found that the Board has effective programs in place that are consistent with FISMA requirements and that include attributes identified by DHS for risk management, security configuration, remote access, identity and access management, security training, incident response and reporting, and security capital planning. We also found that the Board has programs in place that include attributes identified within the DHS reporting metrics for continuous monitoring, contractor oversight, contingency planning, and plan of action and milestones (POA&M); however, we identified opportunities for improvement within those areas. Our findings related to contingency planning are being reported under separate cover.

Our report includes one new recommendation for improving the tracking of division-level POA&Ms and keeps open our 2012 recommendation on contractor systems and our 2013 recommendation on continuous monitoring. Our 2013 FISMA audit included recommendations related to incident response and reporting, security awareness training, and risk management that we are closing based on corrective actions taken by the ISO. The following summarizes the status of our prior FISMA recommendations:

> **2011 Recommendation:** We recommended that the CIO complete and fully implement the enterprise information technology (IT) risk assessment framework across all divisions, and ensure that the automated workflow support tool is fully operational, in order to comply with updated NIST guidance on the new Risk Management Framework (RMF).
>
> **Status: Closed**
>
> **2012 Recommendation:** We recommended that the CIO develop and implement a security review process for third-party systems located outside the Federal Reserve System.
>
> **Status: Open**
>
> **2012 Recommendation:** We recommended that the CIO document the roles and responsibilities of the Board and National Incident Response Team supporting Board incidents and analyze what changes are needed to existing agreements to ensure that the respective roles and responsibilities of the National Incident Response Team and the Board are specified.
>
> **Status: Closed**

2013 Recommendation: We recommended that the CIO monitor specialized training taken by all individuals at the Board with significant information security responsibilities to ensure that they have been adequately trained.

Status: Closed

2013 Recommendation: 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.

Status: Open

We also reviewed security controls implemented for select Board information systems and IT processes, and we completed the fieldwork on several other audits of Board programs related to certain DHS metrics. Our specific findings and recommendations in these areas will be transmitted under separate cover. Appendix A lists these reviews.

Analysis of the Board’s Progress in Implementing Key FISMA, OMB, and DHS Information Security Program Requirements

Risk Management Program

The ISO has developed and finalized a new *Risk Management Program and Risk Assessment Standard* that covers the enterprise, business, and information system–level risks, and the automated workflow support tool has undergone a major upgrade. Once it is fully implemented, we believe that the Board’s risk management program will fully meet NIST guidance. As a result of the actions taken by the Board to establish its risk management program and integrate activities within the automated workflow tool, we are closing our 2011 recommendation that the CIO complete and fully implement the enterprise IT risk assessment framework across all divisions, and ensure that the automated workflow support tool is fully operational, in order to comply with updated NIST guidance on the new RMF.

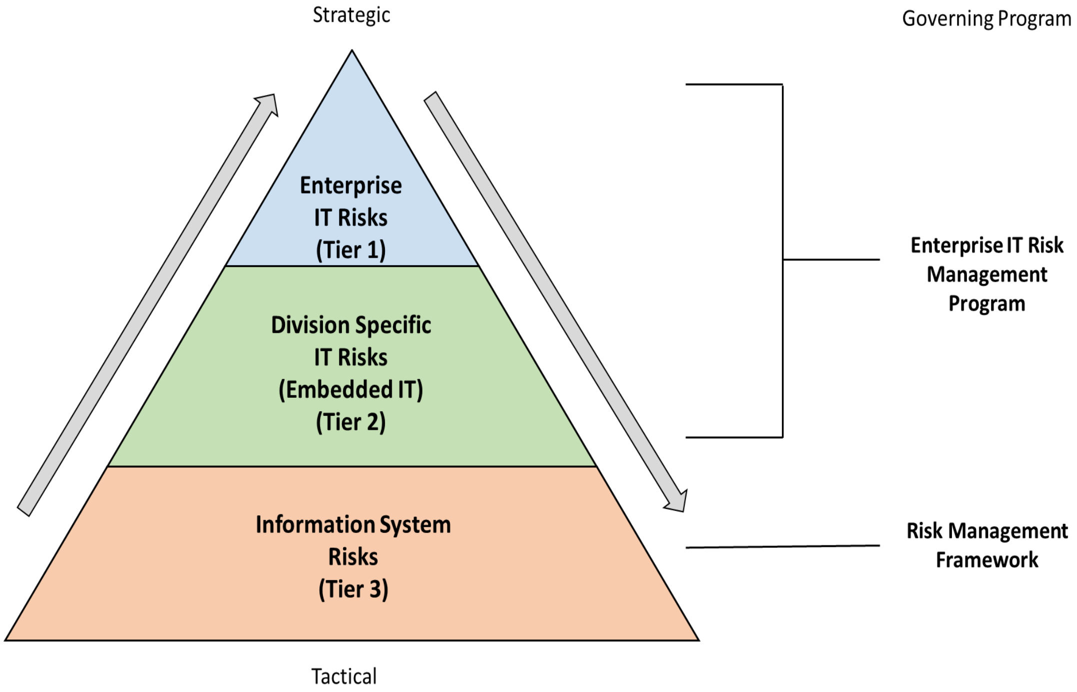
Requirement

In February 2010, NIST issued Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (SP 800-37), which transformed the traditional certification and accreditation process into the six-step RMF. The revised process emphasizes (1) building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls; (2) maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes; and (3) providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the nation arising from the operation and use of information systems.

In March 2011, NIST issued Special Publication 800-39, *Managing Information Security Risk* (SP 800-39), which provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (e.g., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation resulting from the operation and use of federal information systems. SP 800-39 provides a structured, yet flexible, approach for managing risk that is intentionally broad, with the specific details of assessing, responding to, and monitoring risk on an ongoing basis provided by other supporting NIST security standards and guidelines.

Figure 1 shows the three-tiered approach introduced by SP 800-37 and expanded on in SP 800-39. In this approach, managing information system–related security risks is a complex, multifaceted undertaking that requires the involvement of the entire organization.

Figure 1: The Three Tiers of Risk Management


Strategic
Governing Program
Enterprise IT Risks (Tier 1)
Division Specific IT Risks (Embedded IT) (Tier 2)
Enterprise IT Risk Management Program
Information System Risks (Tier 3)
Risk Management Framework
Tactical

Source: The Board's *Risk Management Program and Risk Assessment Standard*.

Tier 1, enterprise IT risks, addresses risks to the Board's enterprise IT service provider, the Division of Information Technology (Division of IT). The scope of risks in this tier include all three functional areas of the division (Infrastructure, Application Development, and Financial and Statistical Support) and focus on risks not related to a specific information system that would impact the Division of IT's ability to complete its mission of providing enterprise IT services to the Board. Tier 2, division-specific IT risks, addresses risks to the embedded IT support units within the business divisions or offices that do not relate to a specific information system. Risk management for Tiers 1 and 2 is covered by the enterprise IT risk management program; however, Tier 3, information system risks, addresses both direct and inherited risks specific to information systems.

Progress to Date

When NIST issued SP 800-37 in February 2010, the Board's ISO developed an enterprise IT risk assessment framework initiative and began implementing it within the Division of IT. Our 2011 FISMA report included a recommendation that the CIO complete and fully implement the enterprise IT risk assessment framework across all divisions, and ensure that the automated workflow support tool is fully operational, in order to comply with updated NIST guidance on the new RMF. Since our initial recommendation, the Board's processes have evolved to include more than just the enterprise IT risk assessment framework, and as a result of the actions taken by the Board to establish an RMF and integrate activities within the automated workflow tool, we are closing the 2011 recommendation.

To address Tier 1, enterprise IT risks, the Board has finalized the *Risk Management Program and Risk Assessment Standard* to address the organization-wide process for managing IT risks. Additionally, the CIO has established a Risk Management Committee, which is responsible for the development of a comprehensive governance structure and organization-wide risk management strategy. We also found that the Board has established the Division of IT risk register, which covers the enterprise IT risks because the Division of IT provides infrastructure services to the entire Board.

In our 2013 FISMA audit, we reported that the risk management program needed to be expanded to address and cover all aspects of Tier 2 risks of the Board's computing environments within all divisions' missions and business processes. To address Tier 2, division-specific IT risks, in conjunction with the *Risk Management Program and Risk Assessment Standard* document, the ISO stated that the Risk Management Committee had met with each division to develop risk registers. The *Board Risk Management Program and Risk Assessment Standard* requires that division-specific IT risks in the risk registers be updated at least quarterly.

To address Tier 3, information system risks, the Board continues to conduct annual security assessments and requires system owners to use the automated workflow support tool. The automated workflow tool underwent a major upgrade during this FISMA reporting period. We found that system owners have inputted the major systems and general support system components into the automated workflow tool, which includes security control baselines, security plans, risk assessments, and POA&Ms.

Work to Be Done

During 2014, we reviewed the Board's processes to meet FISMA's requirements for security categorization, certification and testing, security plans, and accreditation of its information systems. In addition, we reviewed how the Board's FISMA documents and review activities are compiled within the automated workflow tool. During this audit, we found that elements of the Board's information security life cycle were missing for some systems, and that the Board's *Risk Management Program and Risk Assessment Standard* relies on other *Board Information Security Program* policies and appendixes that have not been updated. We are reporting these findings under separate cover, and once fully implemented, we believe that the Board's risk management program will fully meet NIST guidance.

We plan to continue to review the implementation of the RMF in 2015 to ensure appropriate implementation of the program as well as integration with the automated workflow tool.

Continuous Monitoring Program

Continuous monitoring is a critical part of the risk management process. An organization's overall security architecture and accompanying security program are to be continuously monitored to ensure that organization-wide operations remain within an acceptable level of risk, despite any changes that occur. We found that the ISO has developed a *Continuous Monitoring Standard* that outlines the Board's continuous monitoring program for all information systems; however, the development of key components, such as metrics, is still a work in progress.

Requirement

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (SP 800-53), requires that the organization develop a continuous monitoring strategy and implement a continuous monitoring program that includes the establishment of metrics to be monitored, frequencies for monitoring, and assessments supporting such monitoring. It requires ongoing security control assessments and status monitoring in accordance with the organizational continuous monitoring strategy as well as correlation and analysis of security-related information generated by assessments and monitoring. Lastly, it requires (1) response actions to address results of the analysis of security-related information and (2) reporting the security status of the organization and the information system to officials.

In November 2011, NIST issued Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (SP 800-137). This document built on the monitoring concepts introduced in SP 800-37 by defining information security continuous monitoring (ISCM) and how to ensure that it is properly deployed; highlighting the criticality of ISCM in giving organization officials access to security-related information on demand; and enabling timely risk management decisions, including authorization decisions.

In June 2014, NIST issued *Supplemental Guidance on Ongoing Authorizations,* which states that when the RMF has been effectively applied across the organization and the organization has effectively implemented a robust ISCM program, organizational officials, including authorizing officials, are provided with a view of the organizational security and risk posture and each information system's contribution to that security and risk posture on demand. Thus, organizational information systems may move from a static, point-in-time authorization process to a dynamic, near-real-time ongoing authorization process.

Progress to Date

The ISO has developed a continuous monitoring standard that documents its information security capabilities across the various automation domains in SP 800-137. The continuous monitoring standard outlines the Board's continuous monitoring program for all information systems, including those used or operated by Federal Reserve Banks on the Board's behalf or under delegated authority as well as systems used or operated by contractors on the Board's behalf. The primary objective of developing a systematic approach for continuous monitoring is to ensure that the effectiveness of controls for Board information systems is monitored in a consistent, efficient, and effective manner. The Board's continuous monitoring program can be divided into two areas:

- post-system authorization security monitoring
- automated monitoring of security capabilities

We found that the ISO has implemented technical capabilities associated with foundational elements of continuous monitoring. For example, the Board has implemented various commercial-off-the-shelf tools to manage configurations. We found that network administrators continuously inform Board stakeholders about computers that are missing hard disk encryption as well as computers that are missing the configuration management client. The ISO has also established processes to manage vulnerabilities as they are being identified during the scans and report them to the divisions.

Work to Be Done

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 accordance with SP 800-137, the ISO has developed an ISCM strategy based on risk tolerance and awareness of vulnerabilities and mission or business impacts and is in the process of determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture. Going forward, the ISO will need to implement the ISCM program; collect security-related information required for metrics, assessments, and reporting; and automate collection, analysis, and reporting of data where possible.

The ISO is also developing a process to implement SP 800-137 requirements for (1) analyzing the data collected, reporting findings, and determining the appropriate response; (2) responding to findings with technical, management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection; and (3) reviewing and updating the monitoring program, adjusting the ISCM strategy, and maturing measurement capabilities to increase awareness of vulnerabilities.

Once the continuous monitoring strategy is fully implemented and the metrics are identified and communicated, the ISO will be better equipped to provide real-time monitoring to the Board's information security stakeholders as recommended by NIST guidance. As a result, our 2013 recommendation that the CIO continue to establish a continuous monitoring program by finalizing policies and procedures, establishing metrics, and defining the frequency of monitoring remains open.

Plan of Action and Milestones Program

The Board's POA&M process is a critical component of the risk management and continuous monitoring programs. The *Risk Management Program and Risk Assessment Standard* requires for each vulnerability in which the risk is not accepted that the system owner develop a remediation plan to eliminate the risk or to decrease the risk to an acceptable level. The mitigation plan must be documented in the system risk assessment and be tracked in the system's POA&M. The *Continuous Monitoring Standard* requires system owners to update POA&Ms based on the results of the continuous monitoring process. The current policy requires quarterly submission of division-level POA&Ms to the ISO for review, with scheduled completion dates identified for each POA&M item. However, we found that several divisions have missed these quarterly reporting submissions and that milestones dates are not consistently included for each identified vulnerability.

Requirement

FISMA requires that each agency develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency. The program must include a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.

Progress to Date

The ISO has developed an *Information Security Plans of Actions and Milestones Reporting Guidance for Board Divisions and Offices* that states that the Board's CIO will centrally track, maintain, and review POA&M activities at least quarterly and that the CIO is responsible for compiling performance statistics and submitting a status report to OMB annually. The guidance document further states that to meet OMB's POA&M requirements, (1) each Board division and office must maintain a POA&M to track security weaknesses, including their respective IT assets maintained outside the central IT function, and (2) each division is required to submit its POA&M quarterly to the Board ISO for review.

The ISO is in the process of implementing an automated POA&M process that will allow real-time reporting. Currently, POA&Ms for individual information systems are housed within two databases and are reviewed annually during the system's security assessment review by Information Security Compliance (ISC) staff members. During this review, completed POA&M items are certified as resolved, remediation plans are reviewed, and POA&Ms are reviewed for completeness. Division-level POA&Ms are submitted in hard copy to the ISC.

ISC staff members also request division-level POA&Ms on a quarterly basis. The ISC staff members use the Division of IT's quarterly POA&M to compile an Information Security Performance Report, which includes a section with metrics on POA&M items for the Division of IT's systems.

Work to Be Done

While the ISO implements the automated POA&M tracking process, divisions are required to submit quarterly POA&M updates to the ISO for review. We found that three divisions did not meet this requirement in the June 2014 submission period. When divisions miss the submission deadline, ISC staff members send a reminder e-mail. However, ISC staff members only collect and store the POA&M reports and do not analyze or develop metrics using those divisions' POA&Ms. Without a review of the division-specific POA&Ms, the ISC staff members may not be reporting the complete universe of issues to Board stakeholders. Further, without inclusion of POA&M metrics from the divisions, the Information Security Performance Report's metrics do not provide a full view of the agency's information security.

The ISC staff members compile an Information Security Performance Report including POA&M metrics, but as this report only covers POA&M items owned by the Division of IT, it does not include all division POA&Ms. Without consistent collection and evaluation of all division POA&Ms, and without consistent inclusion of milestone dates for POA&M items, agency-wide systemic issues may not be identified and timely resolved. Further, without inclusion of all division POA&M items in the performance reports, the metrics included do not provide a view of information security for the agency as a whole.

We also found that, while the POA&M template includes a field for milestone dates and many system POA&Ms contain this information, there were several instances in the Board's automated workflow tool where this information was not documented. Further, this information also was not documented in the internal compliance management system of the Board's Division of Banking Supervision and Regulation. The *Information Security Plans of Actions and Milestones Reporting Guidance for Board Divisions and Offices* includes, as part of the POA&M template, that divisions are required to include scheduled completion dates to identify the expected date of completion of each task. Without this information, the Board is unable to evaluate timeliness of remedial action to address deficiencies.

Recommendation

We recommend that the CIO

1. 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.

Management's Response

The Director of the Division of IT stated that she agrees with the recommendation and that the Division of IT will take immediate action to address the recommendation, including continuing to manually collect quarterly POA&M reports from the offices and divisions until the automated POA&M tracking process is fully implemented.

OIG Comment

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

Contractor Oversight Program

The Board's third-party systems are covered by the risk management and continuous monitoring programs. The *Risk Management Program and Risk Assessment Standard* states that information system risks (Tier 3) apply to all information systems hosted at the Board. Information systems hosted at a third party, including the Federal Reserve Banks, are covered in the *Third Party Risk Management Program*. The *Continuous Monitoring Standard* outlines the Board's continuous monitoring program for all information systems, including those used or operated by Federal Reserve Banks on behalf of, or under delegated authority from, the Board as well as systems used or operated by contractors on the Board's behalf. However, the *Third Party Risk Management Program* has not been finalized.

Requirement

FISMA requires agencies to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, a contractor, or other source. The *Board Information Security Program* requires third parties, including Federal Reserve Banks, other agencies, and commercial providers, to employ appropriate security controls to protect Board-provided information and services. The level of controls provided by third parties must be comparable to NIST standards.

Progress to Date

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 *Board Information Security Program* and NIST standards. Since then, a project team has been formed and has developed a high-level concept of the way in which security reviews for these systems will be performed. To mitigate risks while developing the program, the ISO plans to conduct full assessments onsite for all new third-party systems. The ISO conducted two compliance reviews in 2013 of third-party systems. To date, the ISO has established a Third-Party Risk Questionnaire that will be used by divisions as new third-party systems are implemented at the Board.

Work to Be Done

In 2014, we reviewed a third-party system. We noted that the system had not undergone a risk assessment, and we identified several inconsistencies between the Board's security requirements and the third party's security requirements, which resulted in several deficiencies.

The majority of the Board's third-party systems are located within the Federal Reserve Banks. The Federal Reserve Banks are transitioning to an information security program that is based on standards and policies developed by NIST. During our follow-up reviews, we found that the program at the Federal Reserve Banks remains a work in progress.

While the ISO has worked closely with the Federal Reserve Banks and has taken steps to address the risks associated with third-party systems by performing full reviews of all new third-party systems, until a risk-based security review procedure for third-party systems has been established, our recommendation will remain open. The ISO should continue to build on the high-level concept for security reviews of third-party systems that has been developed. By fully developing and implementing this security review process, the Board will be better able to ensure that all third-party systems use information security controls that meet the requirements of the *Board Information Security Program* and NIST standards. We will continue to follow up on the CIO's actions to implement our outstanding recommendation.

Contingency Planning Program

Contingency planning is a critical component of risk management and continuous monitoring programs. The *Risk Management Program and Risk Assessment Standard* defines risk categorizations that will need to be identified and assessed, including business interruption/disaster risk. The *Continuous Monitoring Standard* involves managing and responding to various inputs, such as results of a contingency plan test.

The Management Division is primarily responsible for the coordination and administration of the Board's contingency planning and continuity of operations program (COOP) and contingency site. During the 2014 FISMA reporting period, we concluded an audit that separately evaluated the Board's COOP to ensure that the Board's contingency planning and COOP provide a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. In our audit report *The Board Can Better Coordinate Its Contingency Planning and Continuity of Operations Program*, we discuss the need for the Board to develop strategies to implement all the necessary aspects of the Board's COOP.

Requirement

FISMA requires that agency information security programs include plans and procedures to ensure continuity of operations for information systems that support the agency's operations and assets. NIST Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, states that information system contingency planning is a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption, including sustaining continuity of operations within 12 hours and for up to 30 days, from an alternate site. SP 800-53 also establishes contingency planning controls that are essential for recovery and reconstitution of an information system in contingency scenarios. These controls cover information system operational aspects such as policy, planning, training, testing, alternate storage site, alternate processing site, telecommunication services, backup, recovery, and reconstitution.

Progress to Date

Overall, we found that the Board has established and is maintaining a contingency program for the IT general support systems that is generally consistent with NIST and OMB FISMA requirements. The Board has invested resources in the areas of hardware, mainframe computing, network bandwidth, equipment, and other logistical necessities to sustain operations at the contingency site. In addition, the Board continues to conduct semiannual contingency tests of its mission-critical applications.

During the past year, we separately evaluated the Board's contingency planning and COOP to ensure that they provide a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. Overall, we found that the Board has developed a strategy and has taken actions to ensure the continuous operation of critical missions and essential functions in any emergency. The Board has developed a COOP that implements an emergency management policy, identifies emergency management responsibilities, and specifies procedures for the development and implementation of timely emergency responses. The Board also has dedicated COOP personnel and has secured a well-equipped alternate work site.

Work to Be Done

During our audit of the Board's COOP, we found that the Division of IT does provide the ability for divisions to conduct contingency testing for systems and applications biannually. However, we identified two issues related to the Board's contingency plan testing:

- Four divisions did not participate in either contingency plan test this past year.
- Not all after-action reports are developed or submitted to a central unit responsible for governance over the contingency plan testing program.

We recommended that the Director of the Management Division develop strategies to implement across the Board's divisions all the necessary aspects of the Board's COOP. We also recommended that the Director develop a Test, Training, and Exercise program; a reconstitution plan; and a devolution plan for the Board's COOP. Recommendations identified in the COOP report address these issues, and as such, we are not making formal recommendations in this report.

Appendix A
Scope and Methodology

To accomplish our audit objectives, we reviewed the effectiveness of the Board's information security program across 11 areas outlined in DHS's 2014 FISMA reporting guidance for Inspectors General. These areas include continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, security training, POA&M, remote access management, contingency planning, contractor systems, and security capital planning. To assess the Board's information security program in these areas, we interviewed Board management and staff members; analyzed security policies, procedures, and documentation; and observed and tested specific security processes and controls.

We also reviewed security controls implemented for the Board's information systems and IT processes on an ongoing basis. During the past year, we issued the following reports:

- *Audit of the Board's Data Center Relocation*
- *Opportunities Exist to Achieve Operational Efficiencies in the Board's Management of Information Technology Services*
- *Security Control Review of the Board's* E^2 *Solutions Travel Management System*
- *The Board Can Better Coordinate Its Contingency Planning and Continuity of Operations Program*

Given the sensitivity of the issues involved with these reviews, the specific results were provided to management in separate reports, some of which are restricted.

Additionally, during this FISMA cycle we completed the fieldwork on several other audits of Board processes that relate to certain DHS FISMA metric areas:

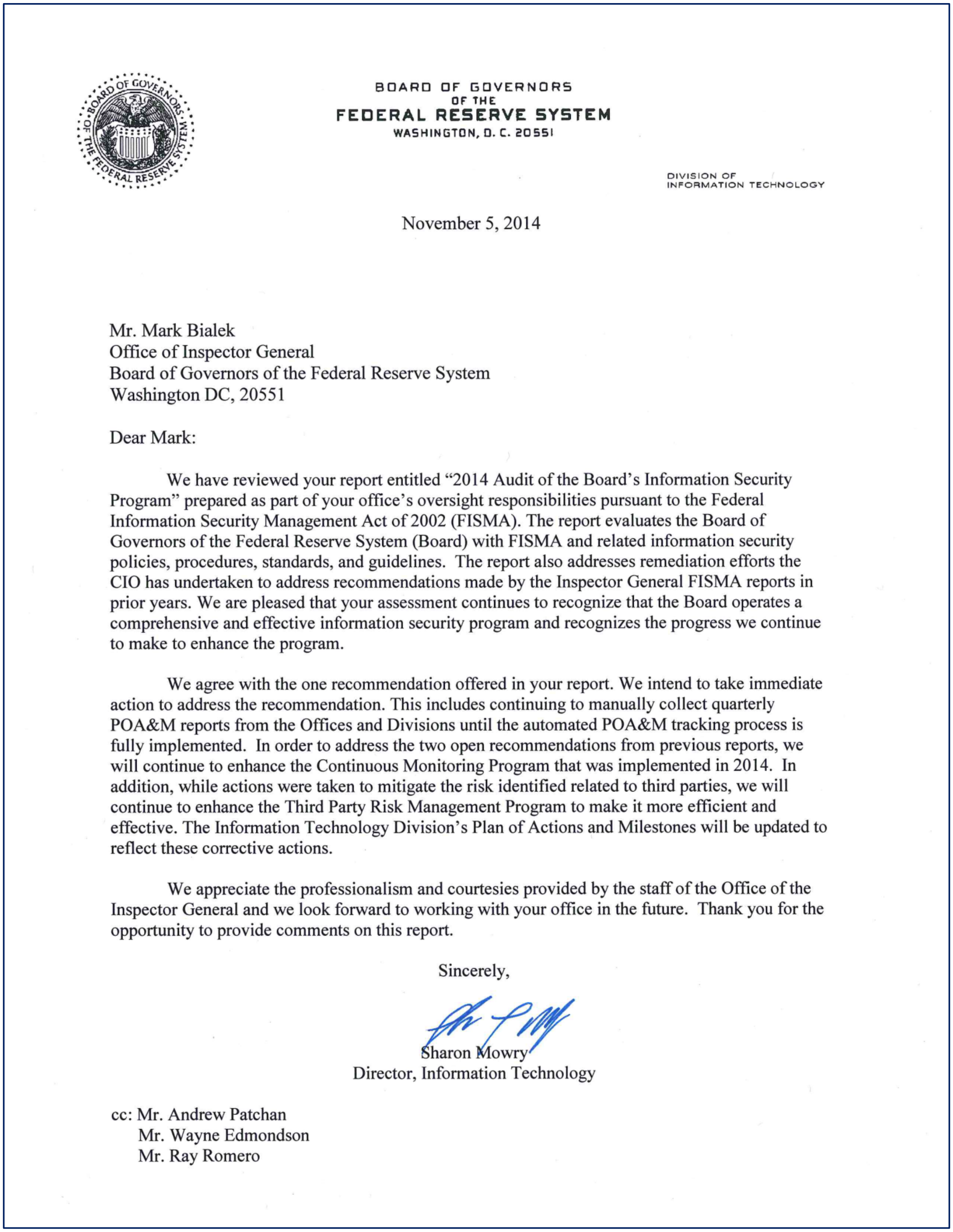
- *Audit of the Board's Data Center Relocation*
- *Audit of the Board's Information System Security Life Cycle Process*
- *Audit of the Board's STAR Modernization Project*

In addition to the FISMA requirements, we performed follow-up reviews of open audit recommendations from prior OIG information security–related audits and application control reviews. These follow-up reviews help us evaluate the Board's compliance with FISMA and related information security policies and procedures and report to DHS and OMB.

- *Security Control Review of Aon Hewitt Employee Benefits System*
- *Security Control Review of the Visitor Registration System*
- *Security Control Review of Contingency Planning Controls for the Information Technology General Support Systems*

We conducted our fieldwork for this audit from June 2014 to September 2014. 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 5, 2014

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 "2014 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 remediation efforts the CIO has undertaken to address 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 one recommendation offered in your report. We intend to take immediate action to address the recommendation. This includes continuing to manually collect quarterly POA&M reports from the Offices and Divisions until the automated POA&M tracking process is fully implemented. In order to address the two open recommendations from previous reports, we will continue to enhance the Continuous Monitoring Program that was implemented in 2014. In addition, while actions were taken to mitigate the risk identified related to third parties, we will continue to enhance the Third Party Risk Management Program to make it more efficient and effective. 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. Andrew Patchan
Mr. Wayne Edmondson
Mr. Ray Romero

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