OFFICE OF INSPECTOR GENERAL

Audit Report 2013-IT-B-019

2013 Audit of the Board's Information Security Program

November 14, 2013

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

Report Contributors

Robert McMillon, OIG Manager
Satynarayana-Setty Sriram, Senior IT Auditor
Christopher Lambeth, Senior IT Auditor
William Fumey, Senior IT Auditor
Andrew Gibson, IT Auditor
Adam Scheps, IT Auditor
Peter Sheridan, Senior OIG Manager
Andrew Patchan Jr., Associate Inspector General for Information Technology

Abbreviations

Board	Board of Governors of the Federal Reserve System
CIO	Chief Information Officer
FISMA	Federal Information Security Management Act of 2002
DHS	Department of Homeland Security
IG	Inspector General
ISCM	information security continuous monitoring
ISO	Information Security Officer
IT	information technology
NIRT	National Incident Response Team
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
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 3, *Recommended Security Controls for Federal Information Systems and Organizations*
SP 800-137	Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
US-CERT	United States Computer Emergency Readiness Team

Executive Summary:
2013 Audit of the Board's Information Security Program

2013-IT-B-019 November 14, 2013

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.

Findings

Overall, we found that the Board's Chief Information Officer 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 the Office of Management and Budget.

The Board's Information Security Officer continues to issue policies and procedures that include attributes identified within the Department of Homeland Security (DHS) reporting metrics. In our response to the 11 DHS reporting metrics for 2013, we found that the Board has effective programs in place that are consistent with FISMA requirements and that include attributes identified by DHS for plan of action and milestones, remote access management, identity and access management, contingency planning, configuration management, and security capital planning. We also found that the Board has programs in place that include attributes identified within the DHS reporting metrics for incident response and reporting, security training, and contractor systems; however, our report identifies opportunities for improvement within those areas. Our report includes a recommendation related to tracking training for individuals with significant information security responsibilities and keeps open our 2012 recommendations related to incident reporting and contractor systems.

During the past year, the Information Security Officer has continued to make progress in implementing an enterprise information technology risk management framework and a continuous monitoring program; however, additional steps are needed to fully implement programs that are consistent with FISMA requirements. Our report includes a recommendation for continuous monitoring and keeps open our 2011 recommendation related to risk management.

Recommendations

We recommend that the Chief Information Officer continue to establish a continuous monitoring program by finalizing policies and procedures, establishing metrics, and defining the frequency of monitoring. We also recommend that the Chief Information Officer monitor specialized training taken by all individuals at the Board with significant responsibilities for information security to ensure that they have been adequately trained. In her response to our draft report, the Director of the Division of Information Technology, in her capacity as Chief Information Officer, agreed with the two recommendations and stated that she intends to take immediate action to address each recommendation.

Access the full report: http://www.federalreserve.gov/oig/files/FRB_Audit_Information_Security_FISMA_Nov2013.pdf
For more information, contact the OIG at 202-973-5000 or visit http://www.federalreserve.gov/oig.

Summary of Recommendations, OIG Report No. 2013-IT-B-019

Rec. no.	Report page no.	Recommendation	Responsible office
1	8	Continue to establish a continuous monitoring program by finalizing policies and procedures, establishing metrics, and defining the frequency of monitoring.	Chief Information Officer
2	12	Monitor specialized training taken by all individuals at the Board with significant information security responsibilities to ensure that they have been adequately trained.	Chief Information Officer

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

November 14, 2013

MEMORANDUM

TO: Members of the Board
Board of Governors of the Federal Reserve System

FROM: Mark Bialek
Inspector General

SUBJECT: OIG Report No. 2013-IT-B-019: *2013 Audit of the Board's Information Security Program*

The Office of Inspector General is pleased to present its report on the 2013 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 to the Director of the Division of Information Technology, in her capacity as Chief Information Officer, for review and comment. Her response is included as appendix B. In her response, the Director agreed with the two recommendations and stated that she intends to take immediate action to address each recommendation. We will utilize the results of our review of the Board's information security program and practices to respond to specific questions in the Department of Homeland Security's *FY 2013 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.

Attachment
cc: Donald Hammond
Sharon Mowry
Geary Cunningham
Raymond Romero
Charles Young
William Mitchell

Contents

Introduction

Objectives

Our specific audit objectives, based on the requirements the Federal Information Security Management Act of 2002 (FISMA),[1] were to evaluate the effectiveness of 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 (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.

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 IG 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),* DHS is exercising primary responsibility within the executive branch for the operational aspects of federal agency cybersecurity with respect to FISMA.

We also review security controls implemented for the Board's information systems on an ongoing basis. During the past year, we completed security control reviews for three Board systems:

1. *Security Control Review of Contingency Planning Controls for the Information Technology General Support System*
2. *Security Control Review of the Board's National Examination Database System*
3. *Security Control Review of a Third-party Commercial Data Exchange Service Used by the Board's Division of Banking Supervision and Regulation*

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

Our reviews of information security controls for these systems identified areas in which controls need to be strengthened. Given the sensitivity of the issues involved with these reviews, the specific results were provided to management in separate restricted reports that are summarized on our publicly available website. During this year's FISMA review, we started security control reviews of the Board's travel system and a major system used by the statistics function at the Federal Reserve Banks and the Board to collect and edit over 75 periodic statistical reports from financial institutions. In addition, we started audits of the Board's contingency planning and continuity of operations, data center relocation, and IT services.

Summary of 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 (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 in the 11 DHS reporting metrics for 2013, we found that the Board has effective programs in place that are consistent with FISMA requirements and that include attributes identified by DHS for plan of action and milestones, remote access management, identity and access management, contingency planning, configuration management, and security capital planning. We also found that the Board has programs in place that include attributes identified within the DHS reporting metrics for incident response and reporting, security training, and contractor systems; however, we identified opportunities for improvement within those areas. Our report includes a recommendation for improving tracking of training for individuals with significant information security responsibilities and keeps open our 2012 recommendations related to incident reporting and contractor systems.

During the past year, the ISO has continued to make progress in implementing an enterprise information technology (IT) risk management framework and a continuous monitoring program; however, additional steps are needed to fully implement programs that are consistent with FISMA requirements. The ISO continued to enhance the risk management program and has made progress identifying enterprise IT risks, division-embedded IT risks, and information system risks; however, the ISO has not fully implemented all the objectives outlined in the Board's risk management program. Thus, our report keeps our related 2011 recommendation open. The ISO has outlined a strategy for continuous monitoring and continues to develop a program that provides details around the Board's continuous monitoring strategy. The Board has implemented a manual continuous monitoring program and has implemented tools and components of an automated continuous monitoring program. The ISO is still developing policy and procedures to fully implement the automated continuous monitoring program Board-wide. Thus, our report includes a recommendation for additional continuous monitoring actions.

Risk Management Program

During the past year, the CIO has continued to make progress in implementing an enterprise IT risk management framework; however, additional steps are needed to fully implement a program that is consistent with FISMA requirements. Our 2011 FISMA audit 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 Risk Management Framework (RMF). During the past year, the CIO has continued to enhance the risk management program and has made progress in identifying enterprise IT risks, division-embedded IT risks, and information system risks. In August 2013, the ISO issued the Board's *Risk Management Program and Risk Assessment Guide*, which describes processes for identifying enterprise IT risks, division-embedded IT risks, and information system risks. We are keeping this 2011 recommendation open as the CIO continues to implement the enhanced risk management program.

Requirement

FISMA requires organizations to develop and implement an organization-wide information security program for the information and the information systems that support the operations and assets of the organization, including those provided or managed by another organization, a contractor, or other source. NIST recently completed a fundamental transformation of the certification and accreditation process into a comprehensive, near-real-time security life-cycle process as part of an RMF. NIST's RMF is based on special publications that guide agencies through a structured process to identify the risks to the information systems, assess the risks, and take steps to reduce risks to an acceptable level.

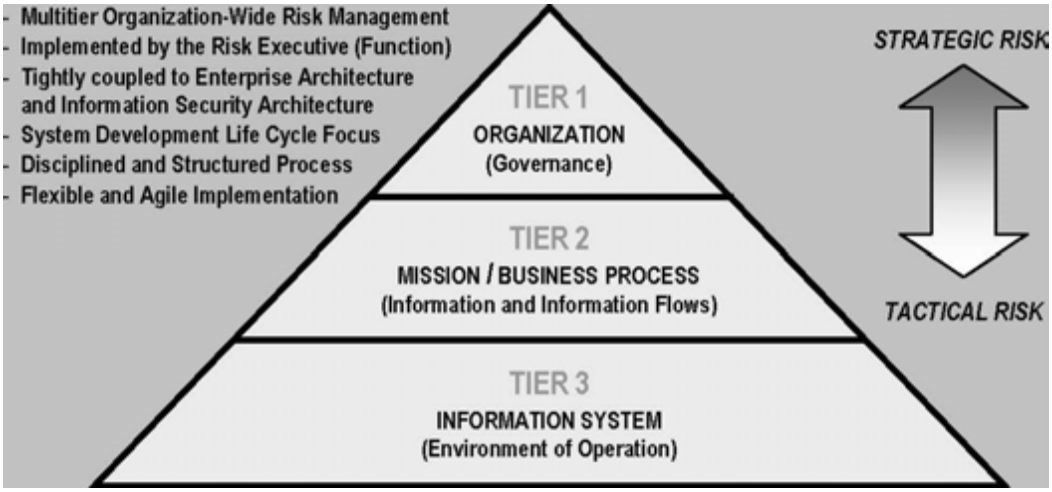
NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (SP 800-37) expands the concept of risk management and covers a strategic-to-tactical organizational approach to risk management. SP 800-37 also promotes NIST's RMF as the concept of near-real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes, with emphasis on the selection, implementation, and assessment of security controls; information systems authorization; and security control monitoring.

NIST Special Publication 800-39, *Managing Information Security Risk* (SP 800-39) states that "it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk—that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organizations." Managing information security risk, like risk management in general, is not an exact science. It brings together the best collective judgments of individuals and groups within

organizations responsible for strategic planning, oversight, management, and day-to-day operations.

Figure 1 shows the three-tiered approach introduced by SP 800-37, and expanded upon 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—senior leaders providing the strategic vision and top-level goals and objectives for the organization (Tier 1); mid-level leaders planning and managing projects for the mission and business processes (Tier 2); and individuals on the front lines developing, implementing, and operating the systems supporting the organization's core missions and business processes (Tier 3).

Figure 1: NIST's Three-Tiered Approach to Risk Management



Source: NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2011.

Progress to Date

In following up on the status of the CIO's corrective actions in response to our outstanding 2011 recommendation on risk management, we found that the ISO had not fully implemented all objectives outlined in the Board's enhanced risk management program. In August 2013, the ISO produced a new draft risk management document, *Risk Management Program and Risk Assessment Guide*, to enhance the original risk assessment framework initiative.

A key feature of the Board's risk management program is the development of risk registers. The ISO has developed a Tier 1 risk register, which is shared with the divisions and offices. The ISO stated that this register is updated on a quarterly basis. The ISO has begun working with the divisions and offices to assist them in developing division-specific IT risk registers and in identifying additional Board-wide risks that should be included in the Tier 1 risk register.

Our 2011 recommendation also included actions to implement the automated workflow support tool. In 2013, the ISO made progress in implementing portions of the automated workflow support tool. For example, the ISO established a repository for many information security components for applications and general support systems, such as control baselines, system security plans, system risk assessments, and security assessment results.

Work to Be Done

The ISO has implemented the risk assessment framework initiative within the Division of Information Technology, as well as a new automated workflow support tool; however, additional actions need to be finalized before the risk program is fully in place and operable.

Although the ISO has made progress in addressing the NIST guidance regarding organizational risk management that was published in 2010 and 2011, an enterprise IT risk assessment framework, as shown in figure 1, still needs to be fully implemented Board-wide. The majority of the Board's computing environment may be managed by the Division of Information Technology; however, the *Risk Management Program and Risk Assessment Guide* needs to be expanded to address and cover all aspects of Tier 2 of the Board's computing environments within all divisions' missions and business processes.

Going forward, the ISO should complete the risk assessment process with the divisions and offices and their embedded IT groups to identify any additional risks. The ISO plans for every division to have an initial risk register completed by the end of the first quarter 2014. We will continue to follow up on the CIO's actions to implement our outstanding recommendation from 2011.

Continuous Monitoring Program

The ISO has outlined a strategy for continuous monitoring and continues to develop a program to fully implement the Board's continuous monitoring strategy. The Board has implemented a manual continuous monitoring program and has implemented automated monitoring tools; however, the ISO is still developing policies, procedures, metrics, and other components of an enterprise-wide continuous monitoring program. To fully implement an automated continuous monitoring program, the CIO should finalize policies and procedures, establish metrics, and define the frequency of monitoring.

Requirement

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (SP 800-53) requires that agencies establish a continuous monitoring strategy and implement a continuous monitoring program that includes a configuration management process for the information system and its constituent components, a determination of the security impact of changes to the information system and environment of operation, ongoing security control assessments in accordance with the organizational continuous monitoring strategy, and a reporting of the security state of the information system to appropriate organizational officials.

In September 2011, NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (SP 800-137) was issued, providing additional guidance on the implementation of a continuous monitoring program. According to SP 800-137, the process of implementing an ISCM program includes the following steps:

- Define the ISCM strategy based on risk tolerance, awareness of vulnerabilities, and mission/business impacts.
- Establish an ISCM program determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.
- Implement the ISCM program and collect security-related information required for metrics, assessments, and reporting. Automate collection, analysis, and reporting of data where possible.
- Analyze the data collected and report findings, determining the appropriate response.
- Respond to findings with technical, management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.
- Review and update the monitoring program, adjusting the ISCM strategy and maturing measurement capabilities to increase awareness of vulnerabilities.

SP 800-137 states that organization-wide monitoring cannot be achieved through either manual or automated processes alone. Where manual processes are used, the processes are repeatable and verifiable to enable consistent implementation, and automated processes can make continuous monitoring more cost effective. Figure 2 documents the continuous monitoring automation domains.

Figure 2: Continuous Monitoring Automation Domains

Source: NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011.

Progress to Date

The ISO outlined a strategic plan for the Board to implement NIST guidance on continuous monitoring in 2011 and updated the plan in August 2012 to include additional continuous monitoring automation tools and to provide more detailed implementation status information. In August 2013, the ISO evolved his continuous monitoring strategy into an *Information Security Continuous Monitoring Program* document, which consists of three primary activities that discuss the Board's continuous monitoring automation, manual processes, and key metrics. The Board's continuous monitoring program consists of many tools and processes that predate the issuance of SP 800-137. The ISO has mapped the existing automated tools and processes to the

automation domains recommended by SP 800-137 (figure 2). The program also describes the manual processes in place at the Board.

Work to Be Done

While the ISO has established a strategy and the program has been initially documented, there are several elements of the continuous monitoring program that need to be developed and finalized before the ISO has a fully implemented organization-wide ISCM program. These elements include finalizing policies and procedures, establishing metrics, and defining the frequency of monitoring.

The program document indicates that the ISO is working with the managers of the continuous monitoring tools and in consultation with an executive risk committee within the Division of Information Technology to develop continuous monitoring metrics as appropriate. The initial set of metrics is anticipated to be developed by the end of the fourth quarter 2013.

SP 800-137 states that at the mission/business processes tier, the organization establishes the minimum frequency with which each security control or metric is to be assessed or monitored. Frequencies are established across all organizational systems and common controls. The ISO is working on developing the frequencies for continuous monitoring that need to be established. Going forward, the ISO should establish detailed policies and procedures for both the metrics and the frequency of testing for the various continuous monitoring tools.

Although not all tools planned for continuous monitoring are under the direct control of the ISO, the underlying procedures for running the tools are in place. However, the procedures do not connect the various tools to the *Information Security Continuous Monitoring Program* document. Making this connection may be an integral part of establishing the frequency and metrics for the continuous monitoring program to be complete.

SP 800-137 states that the organization-wide ISCM strategy and associated policy should be developed at the organizational tier with general procedures for implementation at the mission or business tier (figure 1). We will continue to monitor the ISO's progress in completing the implementation of the organization-wide continuous monitoring program.

Recommendation

We recommend that the CIO

1. Continue to establish a continuous monitoring program by finalizing policies and procedures, establishing metrics, and defining the frequency of monitoring.

Management's Response

The Director of the Division of IT, in her capacity as the CIO, stated that she agreed with the recommendation and that she intends to take immediate action to address the recommendation.

This action includes continuing to implement and mature the Board's continuous monitoring program.

OIG Comment

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

Incident Response and Reporting

Our 2012 FISMA audit report included a recommendation that the CIO document the roles and responsibilities of the Board and the Federal Reserve System's National Incident response Team (NIRT) staffs supporting Board incidents and analyze what changes are needed to existing agreements to ensure that the respective roles and responsibilities of NIRT and the Board are specified. During the past year, the ISO updated the roles and responsibilities for both the Information System Manager and NIRT staff in the Board's *Information Security Incident Handling Guide, Appendix I*; however, the existing agreement that includes NIRT has not been updated since 2007.

Requirement

Federal law requires federal agencies to report incidents to the United States Computer Emergency Readiness Team (US-CERT) office within DHS. SP 800-53 established eight information security controls that are recommended for implementing incident response controls. These controls cover operational aspects of incident handling, such as training, testing, monitoring, and reporting. NIST Special Publication 800-61, Revision 2*, Computer Security Incident Handling Guide*, states that an incident response capability should include the following actions: (1) creating an incident response policy and plan; (2) developing procedures for performing incident handling and reporting; (3) setting guidelines for communicating with outside parties regarding incidents; (4) selecting a team structure and staffing model; (5) establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies); (6) determining what services the incident response team should provide; and (7) staffing and training the incident response team.

Progress to Date

Prioritizing the handling of individual incidents is a critical decision point in the incident response process. The Board has issued internal guidance, *Information Security Incident Handling Guide*, to assist users in appropriately handling security incidents and to identify the general roles and responsibilities of the incident response team. This past year, the ISO updated the roles and responsibilities in the guide for internal staff and NIRT.

The ISO continues to send monthly security log information to US-CERT and reports security incidents within established time frames. In addition, the ISO has implemented

automated tools for intrusion detection, centralized log file analysis, and network analyzers for prevention of denial-of-service attacks. The Board's mandatory security awareness training for all staff includes references to incident-handling guidance and end-user roles and responsibilities. The ISO continues to post security-related articles, information about security incidents, and advisories on the Board's internal website.

Work to Be Done

The Board's help desk team is the primary liaison for coordinating, categorizing, escalating, and documenting all incoming user requests, including security-related incidents. The Information Security Unit within the Board's Division of Information Technology is responsible for handling information security–related incidents. The Information Security Unit uses NIRT, a service of the Federal Reserve System, for incidents that are deemed to have higher impact. NIRT offers eight information security services to the Board and Federal Reserve Banks. A NIRT representative stated that the primary services provided to the Board include security monitoring, forensic services, and alerts.

This past year, the ISO partially addressed our 2012 recommendation by documenting the roles and responsibilities of Board and NIRT staffs in the Board's *Information Security Incident Handling Guide, Appendix I*. However, the Board has a 2007 service-level agreement on the Federal Reserve National IT Services website that lists IT services, such as NIRT incident response services. This agreement states that it is to be updated annually; additionally, this agreement was authorized by a Board officer in a position that has since been eliminated. We continue to believe that the CIO should continue to work with Federal Reserve National IT Services to either update or remove this agreement.

Under either circumstance, the CIO is responsible for analyzing how the Board is provided necessary assurances that (1) Board incidents reported to NIRT receive full attention as necessary, (2) incidents are handled in a timely manner, (3) agreed-upon coordination among the different technical and business staff is established, and (4) other expected services/outcomes are covered.

Security Awareness and Training

The CIO's office has changed its practice of collecting information from IT leadership within the various divisions regarding training received by individuals with significant information security responsibilities. A security training module for technical staff has been released, which provides specialized security training to employees with administrator accounts at the Board. However, Appendix K to the *Board Information Security Program* documents 11 categories of staff that the Board deemed as having significant information security responsibilities and the associated minimum required training for each category. By not monitoring training for all individuals with significant information security responsibilities, the CIO lacks assurance that all such information security staff is sufficiently trained.

Requirement

FISMA requires that an agency's information security program includes security awareness training to inform all personnel, including contractors and other users of information systems that support the agency's operations and assets, of the information security risks associated with their activities, as well as their responsibilities for complying with agency policies and procedures. FISMA also requires that the CIO train and oversee personnel with significant responsibilities for information security. NIST and OMB require that the program include (1) security awareness training for the entire staff, (2) training content based on the organization and roles, and (3) tracking of employees with significant information security responsibilities who require specialized training.

Progress to Date

The Information Security Compliance group, within the Division of Information Technology, retains responsibility for information security training for Board staff. To meet this mission, the group maintains a security awareness training page within the division's internal website. This site contains policies and training materials offered to Board staff and contractors, as well as newsletters providing further information and notifications on information security.

Information security training at the Board continues to be delivered via several online modules. The basic annual security awareness training module is required for all Board employees, contractors, and interns on an annual basis. The security training for technical staff is required annually for all Board employees with administrator accounts. Lastly, security training for authorizing officials and system owners and managers is annual but optional. The Information Security Compliance group tracks staff completion of these modules.

Work to Be Done

In the past, the CIO tracked the training of individuals with significant security responsibilities of the various divisions. Beginning in 2012, however, the CIO released a security training module for technical staff to provide specialized security training. To that end, the CIO has mandated that all Board users with administrator accounts complete the online module annually. With the implementation of this module, training for all staff with significant information security responsibilities is no longer tracked.

Appendix K states that the ISO is responsible for ensuring that each division and office identifies individuals with significant information security responsibilities and ensuring that these individuals receive adequate training. The appendix documents 11 categories of staff that the Board has deemed as having significant security responsibilities and specifies the security-related training requirements for each category; however, the module does not provide for training to meet all of these requirements. Appendix K is in compliance with the CIO's FISMA metrics, which state, "Those with significant security responsibilities include all users who have one or more privileged network user account and all other users who have managerial or operational responsibilities that allow them to increase or decrease cybersecurity." However, without oversight and monitoring of training for all individuals with significant security responsibilities, the CIO's office lacks assurance that all information security staff is sufficiently trained.

Recommendation

We recommend that the CIO

2. Monitor specialized training taken by all individuals at the Board with significant information security responsibilities to ensure that they have been adequately trained.

Management's Response

The Director of the Division of IT, in her capacity as the CIO, stated that she agreed with the recommendation and that she intends to take immediate action to address the recommendation. This action includes reviewing the Board's security training program for individuals with significant security responsibilities to ensure that it adequately addresses the Board's information security training requirements.

OIG Comment

In our opinion, the action described by the Director is 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

In our *2012 Audit of the Board's Information Security Program*, we identified the need for the Board to develop and implement a security review process for third-party systems located outside the Federal Reserve System. The Board has developed a high-level concept of how the security reviews will be performed; however, additional work is needed to fully develop and implement this process. Without a process in place for these reviews, the Board cannot be assured that third-party systems located outside the Federal Reserve System employ security controls that meet the requirements of the *Board Information Security Program* and NIST standards. We plan to continue to follow up on the division's actions to ensure that our recommendation from 2012 is fully addressed.

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 Audit of the Board's Information Security Program*, 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. The CIO stated that she agreed with the recommendation. 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.

Work to Be Done

The Board has developed a process for performing security reviews of third-party systems managed by Federal Reserve Banks; however, the Board still does not have adequate processes in place to ensure that third-party systems located outside the Federal Reserve System meet the requirements of the *Board Information Security Program* and NIST standards and controls. During our ongoing security control review of the Board's travel system, we found that a process for third-party system reviews was not in place to ensure adequate security controls before authorizing the system to operate. Further, we performed a security control review earlier this year of a third-party application utilized for external data services and managed by the Division of Banking Supervision and Regulation at the Federal Reserve Bank of Philadelphia. In this review, we identified several control deficiencies that we communicated to Board management.

The Board 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 able to better ensure that all third-party systems employ information security controls that meet the requirements of the *Board Information Security Program* and NIST standards. We plan to continue to follow up on the division's actions to ensure that our 2012 recommendation is fully addressed.

Appendix A
Scope and Methodology

To accomplish our audit objectives, we reviewed the effectiveness of the Board's information security program across eleven areas outlined in DHS's 2013 FISMA reporting guidance for IGs. These areas include 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, contractor systems, and security capital planning. 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.

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

We conducted our fieldwork from April 2013 to September 2013. 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 7, 2013

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 "2013 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 two recommendations offered in your report. We intend to take immediate action to address each of these recommendations. This includes continuing to implement and mature the Board's Continuous Monitoring Program. In addition, we will be reviewing the Board's security training program for individuals with significant security responsibilities to ensure it adequately addresses the Board's information security training requirements. 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. Geary Cunningham
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