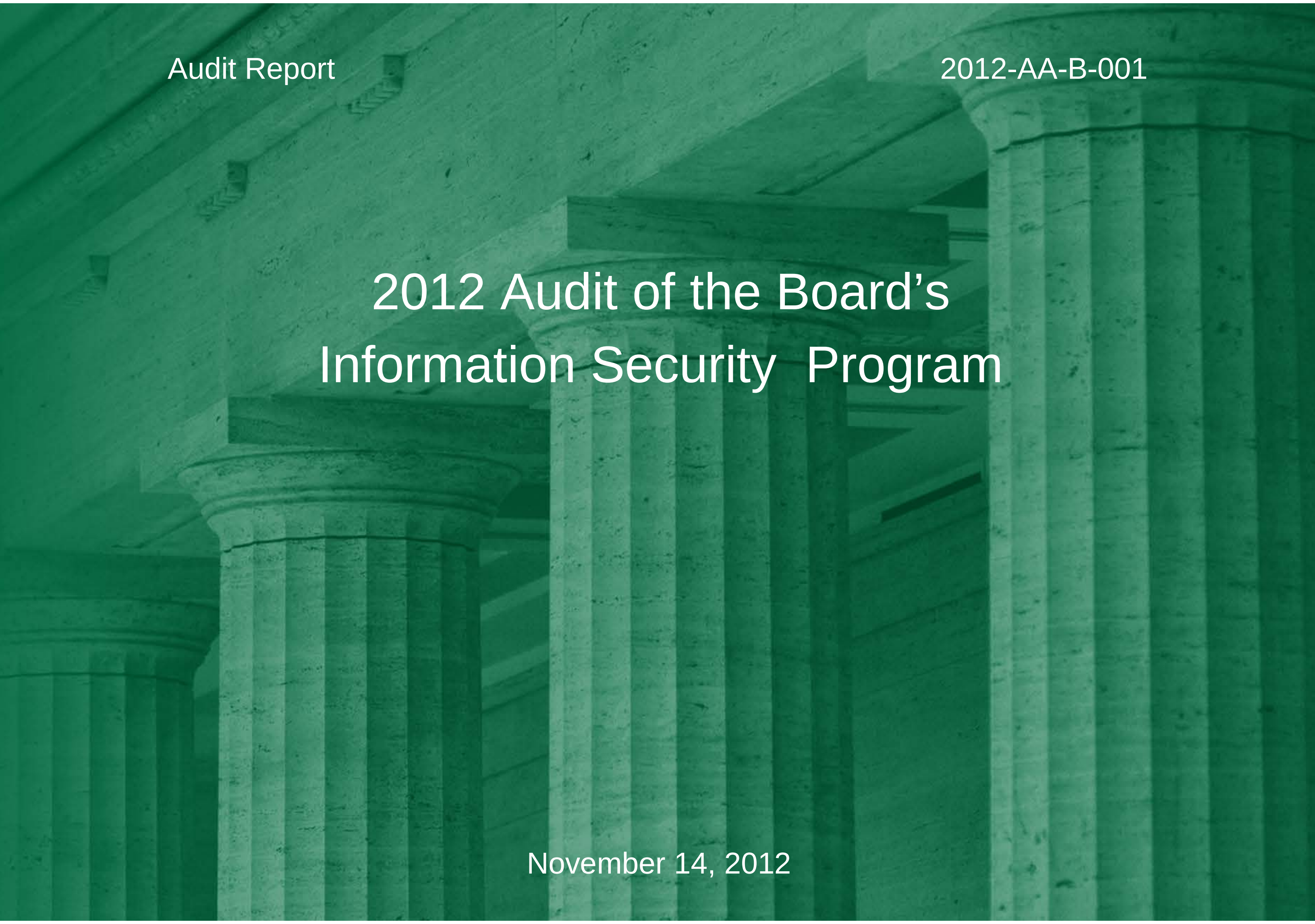
OFFICE OF INSPECTOR GENERAL



Audit Report

2012-AA-B-001

2012 Audit of the Board's Information Security Program

November 14, 2012

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

Report Contributors

Robert McMillon, OIG Manager
Satynarayana-Setty Sriram, Senior IT Auditor
Andrew Gibson, IT Auditor
Joshua Dieckert, IT Auditor
Adam Raley, IT Auditor
Peter Sheridan, Senior OIG Manager
Andrew Patchan Jr., Associate Inspector General for Audits and Attestations

Abbreviations

BISPMS	Board Information Security Program Management System
BS&R	Division of Banking Supervision and Regulation
DHS	Department of Homeland Security
GSS	General Support System
ISO	Information Security Office
NIRT	National Incident Response Team
NRAS	National Remote Access Services
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SP 800-39	Special Publication 800-39, Managing Information Security Risk
SP 800-65	Special Publication 800-65, Integrating IT Security into the Capital Planning and Investment Control Process
US-CERT	United States Computer Emergency Readiness Team

OFFICE OF INSPECTOR GENERAL

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

November 14, 2012

MEMORANDUM

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

FROM: Mark Bialek
Inspector General

Mark Bialek

SUBJECT: OIG Report: *2012 Audit of the Board's Information Security Program*

The Office of Inspector General (OIG) is pleased to present its report on the *2012 Audit of the Board's Information Security Program*. 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 (IG) to conduct an annual independent evaluation of the agency's information security program and practices. Our specific audit objectives, based on the legislation's requirements, were to evaluate the effectiveness of security controls and techniques for selected information systems and compliance by the Board of Governors of the Federal Reserve System (Board) with FISMA and related information security policies, procedures, standards, and guidelines. We also followed up on the status of the Board's corrective actions in response to open recommendations from our prior FISMA reports and security control reviews of specific systems.

We conducted our audit of the Board's compliance with FISMA from May 2012 through October 2012, and we reviewed security controls for the Board's information systems throughout the year, 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.

As part of an agency's annual FISMA reporting, the Department of Homeland Security (DHS) requires that both the Chief Information Officer (CIO) and the IG perform an analysis of certain information security program components. 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),* DHS is exercising primary responsibility within the executive branch for the operational aspects of federal agency cybersecurity with respect to FISMA. OMB remains responsible for the submission of the annual FISMA report to Congress.

As stated in previous FISMA guidance, agencies are required to adhere to DHS direction to report data through CyberScope (an automated FISMA reporting tool). In February 2012, DHS issued reporting requirements for IGs' analysis of their respective agency's information security management performance in line with the requirements of FISMA.[1] In accordance with DHS's requirements, our FISMA review included an analysis of the Board's information security–related processes in the following areas: risk management, continuous monitoring management, plan of action and milestones (POA&Ms), identity and access management, remote access management, configuration management, security training, contractor systems, contingency planning, incident response and reporting, and security capital planning. Appendix 1 contains our analysis of the Board's progress in implementing key FISMA, OMB, and DHS requirements and discusses our observations and recommendations in more detail. In addition to this report, we will provide our analysis to DHS under separate cover through CyberScope, along with the CIO's response, pursuant to DHS's reporting requirements.

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. During the past year, the Information Security Officer (ISO) continued to issue and update information security policies and guidelines. In addition, progress has also been made to implement (1) an enterprise information technology (IT) risk assessment framework initiative and a continuous monitoring strategy as well as (2) a new automated workflow support tool to provide an automated method for documenting, reviewing, and approving the security posture of all Board information systems. These efforts were undertaken to transform the Board's Certification and Accreditation process into the NIST Risk Management Framework (RMF).

An additional part of the overall risk assessment framework requires the CIO to ensure that risk assessments are adequately identifying, evaluating, and documenting the level of risk to information systems based on potential threats, vulnerabilities, and currently implemented or planned controls to determine whether additional controls are needed. Although progress has been made by the ISO to address the NIST guidance regarding risk management, the enterprise IT risk assessment framework needs to be fully implemented Board-wide and the automated workflow support tool needs to be fully operational for the Board to meet the requirements of NIST's organization-wide risk management approach. Our 2011 report contained one recommendation: that the CIO complete and fully implement the enterprise IT risk assessment framework Board-wide and ensure that the automated workflow support tool is fully operational in order to comply with updated NIST guidance on the new RMF. This recommendation will remain open as work continues on various phases of the IT risk assessment framework initiative and continuous monitoring strategy. We will continue to monitor the ISO's actions in implementing the enterprise IT risk assessment framework Board-wide, which includes improving overall risk assessments.

This report contains two new recommendations related to the Board's contractor oversight program and incident response and reporting program. First, to ensure that all Board data meet the requirements of the Board's Information Security Program and NIST standards and controls, we recommend that the CIO develop and implement a security review process for third-party systems located outside the Federal Reserve System to ensure that systems employ information security controls sufficient to meet the requirements of the Board's information security program and NIST standards. Second, we recommend that the CIO document the roles and responsibilities of the Board and 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.

As stated previously, we also review security controls implemented for Board information systems on an ongoing basis. During the past year, we completed security control reviews for five Board systems: (1) the Board's third-party applications operated by the Federal Reserve Bank of Richmond in support of the Board's Division of Banking Supervision and Regulation (BS&R), (2) the Federal Reserve System's Office of Employee Benefits and its third-party contractors, (3) Contingency Planning Controls for the

[1] U.S. Department of Homeland Security, Federal Information Security Memorandum, FISM 12-02, February 15, 2012.

Division of IT General Support System (GSS), (4) National Remote Access Services (NRAS) System, and (5) the Board's Public Website. Our reviews of these systems' information security controls identified areas in which controls need to be strengthened. Given the sensitivity of the issues involved with these reviews, the specific results have been provided to management in separate restricted reports that will be summarized on our publicly available website. During this year's FISMA review, we also started security control reviews of the Board's National Examination Database system and the commercial data exchange service system.

We performed our security control review testing based on selected controls identified in NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (SP 800-53). The controls are divided into "families" (such as access, risk assessment, and personnel security) and include controls that can be categorized as system specific or common (applicable across agency systems). Consequently, although our focus was on evaluating specific applications, we also assessed some of the common security controls that affect most, if not all, of the applications. We will continue to follow up on actions taken regarding our FISMA and security control review report recommendations as part of future audit work related to information system security.

We provided a draft of our report to the Director of the Division of IT, in her capacity as the CIO for FISMA, for review and comment. Her response is included as appendix 2. In her response, the Director agreed with the two recommendations in our report and has initiated remediation efforts to address both issues.

We appreciate the cooperation that we received from the Board during our review. We are providing copies of this audit report to Board management officials. The report will be added to our publicly available website and will be summarized in our next semiannual report to Congress. Please contact Andrew Patchan Jr., Associate Inspector General for Audits and Attestations, at 202-973-5003 if you would like to discuss this audit report or any related issues.

cc: Sharon Mowry
Geary Cunningham
Raymond Romero
Charles Young
J. Anthony Ogden
Andrew Patchan Jr.

Appendix 1
OIG's Analysis of the Board's Progress in Implementing Key FISMA, OMB, and DHS Requirements

The following is our analysis of the Board's progress in implementing key FISMA, OMB, and DHS requirements, including progress to date and work to be done. Our analysis identifies two new recommendations (pages 16 and 18).

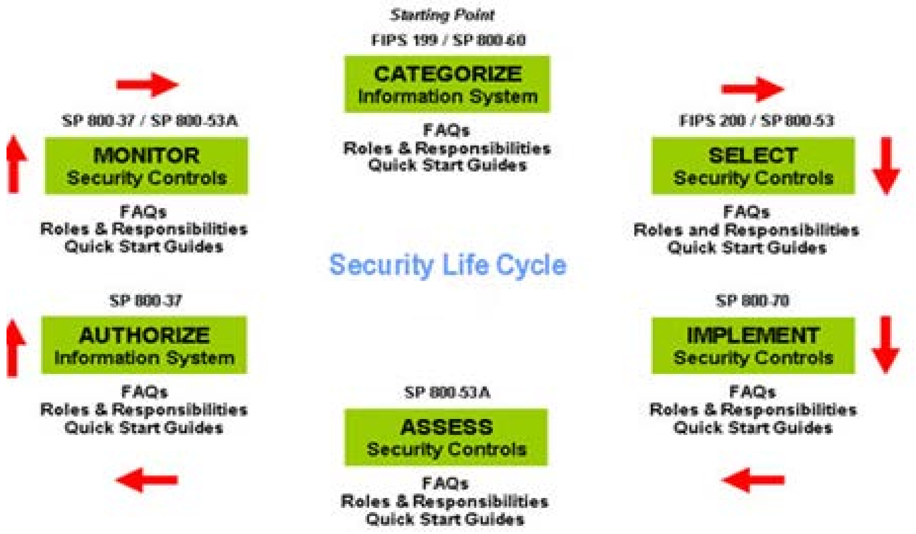
Risk Management Program

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, 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.

Figure 1 shows NIST's RMF and identifies NIST's related guidance.

Figure 1: NIST's Risk Management Framework



Source: NIST Computer Security Division, Computer Security Resource Center.

NIST SP 800-53 states that an organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time.

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.

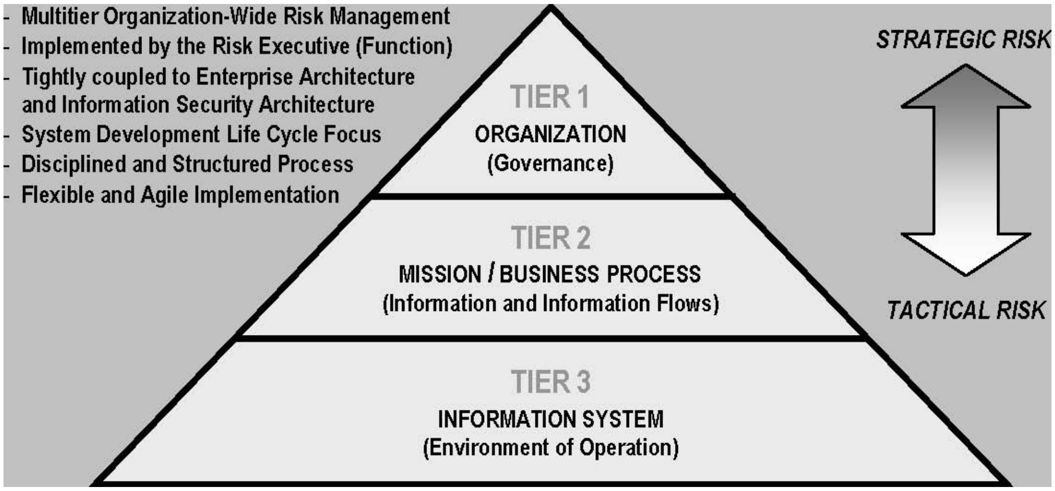
NIST Special Publication 800-39, *Managing Information Security Risk* (SP 800-39) states that it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk—that is, the risk associated with the operation and 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.

Progress to date:

The Board's risk management approach has traditionally focused on the information system level, which was based on NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*; the initial SP 800-37 (dated May 2004); SP 800-53; and other NIST publications. Revision 1 to SP 800-37 provides guidance for agencies to establish a risk management program that addresses risk from (1) an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy; (2) a mission and business process perspective, guided by the risk decisions at the organizational level; and (3) an information system perspective, guided by the risk decisions at the organizational level and the mission and business perspective.

Figure 2 shows the three-tiered approach introduced by SP 800-37, Revision 1, and expanded upon in SP 800-39, that revolves around the concept that 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 (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 2: NIST's Three-tiered Approach to Risk Management


- Multitier Organization-Wide Risk Management
- Implemented by the Risk Executive (Function)
- Tightly coupled to Enterprise Architecture and Information Security Architecture
- System Development Life Cycle Focus
- Disciplined and Structured Process
- Flexible and Agile Implementation
TIER 1
ORGANIZATION
(Governance)
TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)
TIER 3
INFORMATION SYSTEM
(Environment of Operation)
STRATEGIC RISK
TACTICAL RISK

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

To address risks at the organizational level and the mission/business level, the ISO developed an enterprise IT risk assessment framework initiative and began implementing it within the Division of IT. When fully implemented, the enterprise IT risk assessment framework is anticipated to identify those risks that most greatly inhibit the Board from achieving its strategic objectives. A key feature of the IT risk assessment framework is the development of a risk register. After the risk register is developed for the Division of IT, the ISO plans to roll out the risk register approach to the other Board divisions. As identified in the framework, the first milestone was to discuss the risk register with the division's Information Security Committee members first and then to receive input directly from the other Board divisions. During the past year, the ISO met with appropriate division officers to introduce the risk management program and the risk register and to discuss the risks that the Division of IT has identified. The next step will be to formalize the register so that each division can complete its own register.

The Division of IT has established a Risk Management Committee (RMC). A key priority for the RMC is to create an approach to further FISMA and Enterprise Risk Management compliance throughout the Board. Under the direction of the RMC, the Division of IT has begun a risk assessment of all areas of the division. The process used for this review will serve as a model for all Board divisions to follow when conducting their own business risk reviews going forward.

In addition, the Division of IT strategic planning initiatives continue to include milestones and priorities that focus on risk management. The purpose of these initiatives is to identify, evaluate, and manage risks that could impede the successful achievement of the Board's mission and objectives. Through this process, Board divisions are expected to identify the residual risks that cannot be mitigated to their satisfaction and that, if realized, would be impediments to achieving their objectives.

Work to be done:

The Division of IT has had components of the three-tiered risk management program shown in figure 2 in place in prior years with a system-level focus based on the existing guidance at that time. NIST SP 800-37 and SP 800-39 have placed further emphasis on overall organizational risk management at the Tier 1 and 2 levels. The additional risks that are considered at the organizational level will ultimately need to be filtered down to the individual information systems and IT GSS. The ISO has begun implementing the risk assessment framework initiative within the Division of IT, as well as portions of the continuous monitoring strategy that include a new automated workflow support tool; however, additional actions need to be finalized before the risk program is fully in place and operable.

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 to comply with updated NIST guidance on the new RMF. Although the ISO has made progress in addressing the new NIST guidance regarding risk management, an enterprise IT risk assessment framework needs to be fully implemented Board-wide and the automated workflow support tool fully operational for the Board to meet the requirements of NIST's organization-wide risk management approach. Accordingly, our 2011 FISMA recommendation will remain open. We will continue to monitor the ISO's actions in implementing the enterprise IT risk assessment framework Board-wide.

Continuous Monitoring Program

Requirement:

In September 2011, NIST issued Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (SP 800-137). SP 800-137 ties continuous monitoring into the NIST RMF. Although NIST and OMB have placed a focus on continuous monitoring, FISMA has always required that an agency's information security program include an entity-wide continuous monitoring program to assess the security state of information systems in accordance with NIST and OMB FISMA-related requirements. SP 800-137 provides new perspectives for manual and automated continuous monitoring and details the major phases of establishing, implementing, and maintaining an agency information security continuous monitoring program.

SP 800-137 states that organization-wide monitoring cannot be efficiently achieved through either manual processes or automated processes alone. Where manual processes are used, the processes are repeatable and verifiable to enable consistent implementation. Automated processes, including the use of automated support tools (such as vulnerability scanning tools and network scanning devices) can make the process of continuous monitoring more cost effective, consistent, and efficient. Many of the technical security controls defined in SP 800-53 are good candidates for monitoring using automated tools and techniques. Real-time monitoring of implemented technical controls using automated tools can provide an organization with a more dynamic view of the effectiveness of those controls and the security posture of the organization.

Organizations take the following steps to establish, implement, and maintain a continuous monitoring program:

- Define a continuous monitoring strategy.
- Establish a continuous monitoring program.
- Implement a continuous monitoring program.
- Analyze data and report findings.
- Respond to findings.
- Review and update the continuous monitoring strategy and program.

Progress to date:

The Board's continuous monitoring program has traditionally included ongoing assessments of security controls. The ISO continues to conduct security assessments on a three-year cycle, with all systems undergoing annual testing. For major applications, one-third of the total controls will be tested every year, although certain critical controls will still be tested every year. For general support systems, one-third of the individual components will be tested every year. SP 800-137 requires agencies to move toward a continuous monitoring program that enables organizations to move from compliance-driven risk management to data-driven risk management that provides organizations with information necessary to support risk-response decisions, security status information, and ongoing insight into security control effectiveness.

The ISO has developed a continuous monitoring strategy based on a framework devised by DHS in concert with other agencies, such as the Department of State. DHS has developed the framework as a maturity model that will help agencies determine next steps in developing a continuous monitoring program. The framework consists of four subsystems:

- Sensor Subsystem
- Database/Repository Subsystem
- Analysis/Risk Scoring Subsystem
- Presentation and Reporting Subsystem

The ISO's continuous monitoring strategy lists tools (such as various software scanning and logging tools) that are currently in use or planned for use at the Board. The continuous monitoring strategy entails leveraging these tools and processes already in place to evolve the program into an automated and integrated continuous monitoring program. Additional software has been acquired for expanded vulnerability scanning and configuration-setting monitoring, as well as software for enhanced logging capabilities. The ISO is also incorporating the use of the automated workflow support tool that will make use of many of the security monitoring mechanisms already in place for the Board's IT infrastructure and embedded division IT operations. The tool will provide an automated workflow method for documenting, reviewing, and approving the security posture of all Board information systems.

Work to be done:

At the time of our previous audit in 2011, the ISO's continuous monitoring strategy reflected implementation of this framework through September 2012. September 2012 coincides with the one-year time frame for agencies to be in compliance with SP 800-137 standards and guidelines. The ISO has recently upgraded the continuous monitoring strategy and is currently adding additional Board information system security data into the automated workflow support tool. These actions will result in an automated workflow method for documenting, reviewing, and approving the security posture of all Board information systems. The ISO has indicated that all information system security plans and risk assessments are currently being loaded into the automated tool. The ISO anticipates that all the tools slated for the overall continuous monitoring strategy will be in place no later than 2013. We will continue to monitor the overall development of the new continuous monitoring initiatives.

Plan of Action & Milestones Program

Requirement:

FISMA requires agencies to establish a process for addressing any deficiencies in information security policies, procedures, and practices. OMB guidance requires agencies to prepare and submit POA&Ms for all program reviews and evaluations in which IT security weaknesses are identified. OMB guidance further states that an agency's POA&M program should track and monitor known information security weaknesses, include documented policies and procedures, and establish and adhere to reasonable remediation dates. The guidance also calls for the CIO to centrally track and independently review and validate the POA&M activities at least quarterly.

Progress to date:

The Board has established internal processes to govern its practices around POA&Ms. These processes include a quarterly submission by the Board divisions tracking POA&M progress, as well as a quarterly independent review and validation by the Information Security Compliance group of the Division of IT to verify the progress of the open POA&Ms. There are several repositories used to track the ongoing progress of POA&Ms within the Board. The ISO has begun to transition POA&M information into the Board's automated workflow tool with the intent to centrally monitor POA&Ms. However, all POA&M information has not yet been migrated to the automated workflow tool.

Work to be done:

We verified that the Information Security Compliance group is continuing the ongoing POA&M verification process during the overall development of the new continuous monitoring initiatives. We will continue to monitor the ISO's progress in implementing the automated workflow tool and integrating POA&M data.

Identity and Access Management Program

Requirement:

The Board is required to establish an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The Board's information security program requires controls to be incorporated for all information systems that ensure that each user, or process acting on behalf of a user, is uniquely identified and authenticated. The Board's information security program requires that only authorized users have access to information systems and that access be based on business requirements.

Further, security officials are required to implement account management processes for establishing, activating, modifying, disabling, and removing system accounts.

Progress to date:

Identification and authentication includes security controls designed to verify the identity of individual users, processes, or devices as a prerequisite to allowing access to information systems and data. Identification and authentication can be accomplished using various means, such as passwords, card tokens, biometrics, or some combination thereof. We found that the ISO has established and is maintaining an identity and access management program that is generally consistent with NIST and OMB FISMA requirements.

The Division of IT's GSS provides identification and authentication services that Board systems rely on. The Board has developed a central process for issuing and managing network user identification. As part of this process, the Board's human resources system generates a unique network ID prior to an employee's start date. This information is communicated to the IT security unit, which adds the user to the Board's network and other systems as needed.

Work to be done:

As part of the Board's physical security program, Personal Identity Verification (PIV) cards are used for physical access control to its buildings, but are not used to provide access to information systems. Multifactor authentication at the Board is implemented with use of a token that is separate from the PIV card that all employees have and use for access to Board buildings. As reported in our 2011 FISMA report, the ISO had scheduled a pilot program to test the use of PIV cards for access to the Board's network. Due to technical difficulties and higher-priority projects, the formal pilot has been delayed. However, the Board has made progress in analyzing the use of PIV cards for Windows authentication, Windows administration authentication, hard-disk encryption, and remote access.

Our 2010 FISMA report noted that the Board had not implemented a solution to identify or authenticate devices attached to the network. We did note that compensating controls were in place and that a pilot program was scheduled for 2012 to test a solution to identify devices attached to the Board's network. During our 2012 FISMA review, we found that the scheduled pilot program for authenticating devices was delayed due to budget and resource constraints. Board officials notified us that the pilot program is planned for later this year. As part of our ongoing work related to information security, we will continue to monitor the ISO's efforts to strengthen the Board's identity and access management program.

Remote Access Program

Requirement:

NIST requires that agencies document allowed methods of remote access, establish usage restrictions, monitor for unauthorized access, authorize access, and enforce security requirements for all users of the organization's systems.

Progress to date:

The Federal Reserve System continues to have an established remote access program, NRAS, which is managed by the Federal Reserve Bank of New York and services both the Board and the Reserve Banks. In 2012, we completed a security control review of the NRAS system. Our objectives were to evaluate the effectiveness of selected security controls and techniques to ensure that the Board maintains a remote access program that is generally compliant with FISMA requirements. Our review was divided into two separate phases: the first phase primarily addressed technical and operational control areas, and the second phase addressed procedures. Overall, our review found that the Federal Reserve's remote access system is technically and operationally sound and that the Board has developed an adequate process to administer the token keys for Board personnel.

Work to be done:

During the most recent audit, NRAS was noted as being operationally sound; however, we identified opportunities to strengthen information security controls to be in compliance with federal regulations. The Federal Reserve Bank of New York continues to implement an information security program that is based on standards and policies developed by NIST. The program provides management direction and requirements for the support of information security and is approved, published, and communicated, as appropriate, throughout the Federal Reserve System. During 2012, the NRAS system was assessed and received an authorization to operate.

Although NRAS has received an authorization to operate, the Federal Reserve Bank of New York continues to implement information security enhancements to meet the intent of our audit recommendations. During the upcoming year, we will follow up on our open recommendations and continue to monitor the Reserve Bank's progress with its security program to bring the NRAS system into full compliance with FISMA.

Security Configuration Management

Requirement:

The Board is required to establish and maintain a security configuration management program that is generally consistent with NIST and OMB FISMA requirements. SP 800-53 established configuration management controls that cover operational aspects such as policy, baseline configuration, configuration change control, security impact analysis, access restrictions for changes, configuration settings, least functionality, information system component inventory, and configuration management plan.

NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems,* states that security-focused configuration management of information systems involves a set of activities that can be organized into four major phases—Planning, Identifying and Implementing Configurations, Controlling Configuration Changes, and Monitoring. These different phases address the key aspects of maintaining a desired security posture in the Board's environment.

Progress to date:

The Board's security configuration management program is generally consistent with NIST and OMB FISMA requirements. The ISO has established operating environment documents and procedures for its infrastructure services. This configuration management process is an ongoing operational support function and covers baseline security controls and corresponding configuration settings of infrastructure components. The authorized changes to configurations are documented in the Division of IT's change control system. The patches and upgrades that are essential for hardware, operating systems, and software are applied during a scheduled maintenance window as required under the Board's information security program. The changes to configurations require approval from system owners and require necessary testing and analysis.

Work to be done:

As part of the Board's continuous monitoring program, the CIO continues to implement network monitoring tools, including audit log consolidation processes, to monitor configuration settings. During 2012, the OIG has started scanning the Board's configuration baselines using automated scanning tools. As part of our ongoing work related to information security, we will continue to monitor the ISO's efforts to strengthen the Board's configuration management program

Security Training Program

Requirement:

FISMA requires that an agency's information security program include 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 (a) security awareness training for the entire staff, (b) training content based on the organization and roles, and (c) tracking of employees with significant information security responsibilities that require specialized training.

Progress to date:

The Information Security Compliance group continues to provide ongoing security awareness through its website, communications, and various training based on organizational policy requirements. The Division of IT's security awareness webpage is host to items such as policies, security articles, and training materials. The webpage offers security articles that cover a broad range of security topics.

The Board's security training includes basic annual security awareness training, information security awareness training for technical and system administration staff, and management security awareness training for authorizing officials and system owners.

The Board requires and tracks annual security awareness training of all employees, contractors, and interns with access to the Board network. Also, the Division of IT monitors the training received by individuals with significant security responsibilities by surveying the IT leadership of the various divisions.

Work to be done:

The ISO has developed an online training module for individuals with significant security responsibilities to be combined with existing security awareness training already implemented. The ISO plans to have the training module completed by the end of November 2012. Further, the ISO continues to offer training to system owners regarding their FISMA responsibilities and will also cover the topic of a risk register. We will continue to monitor the Division of IT's ongoing efforts to provide security training.

Contractor Oversight Program

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, contractor, or other source. The Board's 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:

The ISO has developed a security policy that applies to all third parties that collect or maintain Board information or that operate or use information systems on behalf of the Board. The ISO has also published an inventory guide that outlines how the Board accounts for all information assets and tracks the security compliance of all systems, including systems used or operated by third parties on behalf of the Board. In addition, the ISO has developed an inventory of systems that identifies third-party systems and their risk rating, authorization status, and interconnections based on Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems.*

The Board's third-party systems are primarily located within the Federal Reserve Banks; however, third-party systems located outside of the Federal Reserve System also exist. The ISO and BS&R perform onsite security reviews of Federal Reserve Bank systems that store or process Board data to ensure that the systems are meeting the Board's information security program requirements. In addition, BS&R has developed and implemented the Board Information Security Program Management System (BISPMS), an automated tool to facilitate standardization and consistency in implementation of the requirements of the Board's Information Security Program for Federal Reserve Bank systems that store or process Board data. The BISPMS is used by BS&R to conduct security control assessments, store system security documentation, and report on compliance activities.

The Board has developed a process for performing security reviews of third-party systems managed by Federal Reserve Banks that store or process Board data to ensure that the systems are meeting the Board's information security requirements. In 2012, we completed a security control review that included several third-party Lotus Notes–based systems located at the

Federal Reserve Bank of Richmond that support BS&R. Overall, our review found that controls for these systems were adequately designed and implemented to meet Board and NIST requirements. However, we identified several opportunities to strengthen the security controls around these systems, and we communicated our recommendations to BS&R as well as to other relevant parties under separate cover.

Work to be done:

The Federal Reserve Banks are not required to follow NIST and OMB guidance but are transitioning to an information security program that is based on standards and policies developed by NIST. The planned benefits include clarifying information security risks from an enterprise perspective and providing better support for Board customers who are already utilizing NIST standards and guidance. The transition includes IT infrastructure that Federal Reserve Banks rely on for such functions as Internet access, search functionality, remote access, and electronic mail. The Federal Reserve Banks plan to transition their respective systems to the new program by 2013.

As previously discussed, the Board has developed a process for performing security reviews of third-party systems managed by Federal Reserve Banks; however, the Board 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's information system program and NIST standards and controls.

As part of our ongoing work related to information security, we continue to monitor the ISO's oversight of third parties' compliance with FISMA and the requirements of the Board's information security program through the security control reviews completed for third-party applications located outside of the Federal Reserve System. Our security control reviews identified several control deficiencies that will be communicated to Board management in separate reports:

- During 2012, we performed a security control review of the Aon Hewitt Employee Benefits System, a third-party application under the Management Division. Our review noted that total reliance had been placed on third-party internal control reviews to gain assurance that Board and NIST requirements were being met. The third-party internal control reviews did not directly map to and assess compliance with NIST controls and standards.

- We also performed a security control review of a third-party application utilized for external data collaboration and managed by BS&R at the Federal Reserve Bank of Philadelphia. Our review noted that the ISO had not completed a detailed onsite security review of the application prior to placing the application into production. Instead, we noted that BS&R had placed heavy reliance on internal control reviews completed by a third-party public accounting firm to gain assurance that effective controls were implemented. Further, we noted the review did not directly map to and assess compliance with NIST standards and controls.

Based on our findings during these contractor information security control reviews, we concluded that the Board had not obtained sufficient assurance that security controls had been effectively implemented to comply with federal and Board guidelines and that the Board's review processes for third-party applications located outside the Federal Reserve System need to be enhanced and strengthened.

Recommendation 1:

We recommend that the CIO develop and implement a security review process for third-party systems located outside of the Federal Reserve System to ensure that systems employ information security controls sufficient to meet the requirements of the Board's information security program and NIST standards.

Management's Response

The Director of the Division of IT, in her capacity as the CIO for FISMA, stated that she agreed with the recommendation and has initiated remediation efforts to address the issue.

OIG Comment

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

Contingency Planning

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. NIST 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:

The Board has established and is maintaining a contingency program for the IT GSS 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. We recently completed an audit of the contingency planning for the IT GSS and, although we did not identify any significant discrepancies, we found opportunities to strengthen the IT GSS contingency planning by updating documentation and assessing capacity and capabilities.

Responsibility for the Board's contingency-related operations is split among various divisions. The Management Division is responsible for the logistics and facilities of the contingency site. The Division of IT is responsible for ensuring operational readiness of IT infrastructure services. System owners determine the resources and testing for each of the Board's systems and applications.

The alternate processing site used by the Board in contingency situations is a shared facility and is considered an extension of the Board's primary data center for IT infrastructure operational purposes. Access to the Board's contingency site is restricted to authorized Board staff only. In addition to Board identification badges issued to employees, a separate identification badge is necessary to access the contingency site. The issues identified during the contingency tests are recorded in the help desk system, and appropriate IT staff is assigned to these issues for resolution. The semiannual tests include testing and availability of infrastructure services that are essential for mission-critical applications.

Work to be done:

Because the responsibility for the Board's contingency-related operations is split among various divisions, there is no coordinated analysis of contingency capabilities across Board divisions. Without a coordinated analysis of the semiannual tests and after-action reports, the Board lacks assurance that there are adequate capabilities to perform Board operations in the event of a contingency situation, as required by NIST and other federal regulations. We reported last year that (1) a central point of contact for Board-wide coordination, validation, reporting, and verification of mission-critical applications would improve efficiency and (2) a Board-wide process of monitoring and analysis of test results should be established.

We continue to believe that monitoring and oversight of contingency-related operations across divisions will improve the efficiency and effectiveness of the Board's preparedness for a contingency situation. We plan to conduct additional audit work in the area of continuity of operations and contingency planning across divisions.

Incident Response & Reporting

Requirement:

The Board is required to create and operate a formal incident response capability. Federal law requires federal agencies to report incidents to the United States Computer Emergency Readiness Team (US-CERT) office within DHS.

FISMA requires agencies to develop procedures for detecting, reporting, and responding to security incidents. 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 1, *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 based on the incident response policy; (3) setting guidelines for communicating with outside parties regarding incidents; (4) selecting a team structure and staffing model; (5) establishing relationships between the incident response team and other groups, both internal (such as the legal department) and external (such as 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 an *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. The Board has also issued a Device and Document Loss Notification Report, which is a form that should be used to report lost or stolen Board devices such as mobile phones, storage media, and laptops.

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, 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 IT 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 several incident response–related services to the Board and Federal Reserve Banks, including incident detection, response, and analysis; however, the ISO has not documented the specific responsibilities of Board staff in the event of an incident and the specific services for which the Board relies upon NIRT staff in supporting Board incidents.

The Board does not have a direct agreement for services with NIRT. The Board has a service level agreement with Federal Reserve Information Technology that offers operational agreements for IT services offered, such as NIRT incident response services. The operation agreement for NIRT incident response services specifies services offered, including identification of appropriate technical responses, managing communications with management and technical staffs, and tracking incident impacts, but it is not specific to the Board. As the ISO documents Board and NIRT staffs' roles and responsibilities the CIO will need to analyze how these agreements provide the Board the 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 staffs is established, and (4) other expected services/outcomes are covered.

Recommendation 2:

We recommend that the CIO document the roles and responsibilities of the Board and 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.

Management's Response

The Director of the Division of IT, in her capacity as the CIO for FISMA, stated that she agreed with the recommendation and has initiated remediation efforts to address the issue.

OIG Comment

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

Security Capital Planning and Investment Program

Requirement:

FISMA requires agencies to ensure that information security management processes are integrated with strategic and operational planning processes. Capital planning and investment control refers to a decision making process for ensuring that IT investments integrate strategic planning, budgeting, and IT management considerations. NIST Special Publication 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process* (SP 800-65), issued January 2005, notes that while security and capital planning have traditionally been thought of as separate activities, FISMA charges agencies with integrating the two.

SP 800-65 distinguishes between enterprise-level and system-level security investments. Enterprise-level security investments are ubiquitous across the agency and are designed to improve the agency's overall security posture. Examples include an enterprise-wide firewall or intrusion detection system. System-level investments are designed to strengthen a discrete system's security environment, such as strengthening password controls or testing a contingency plan. SP 800-65 further states that at the system level, managers should account and budget for IT security over the system investment life cycle. This information will flow to the enterprise level to support IT compliance and integration activities.

The DHS FISMA reporting metrics direct IGs to determine whether their agency has established and maintains a security capital planning and investment program. DHS outlines specific attributes that should be included in such a program, including employment of Exhibit 53, *Agency IT Investment Portfolio,* and Exhibit 300, *Capital Asset Plan and Business Case Summary,* to record required information security resources. Federal agencies that receive appropriated funding are required to submit these exhibits to OMB annually to request and justify their planned budget for IT and information security. The Board does not receive appropriated funds from Congress. As such, several of the security capital planning and investment program attributes DHS has asked the IGs to evaluate, including use of Exhibit 53s and Exhibit 300s, are not directly applicable to the Board.

Progress to date:

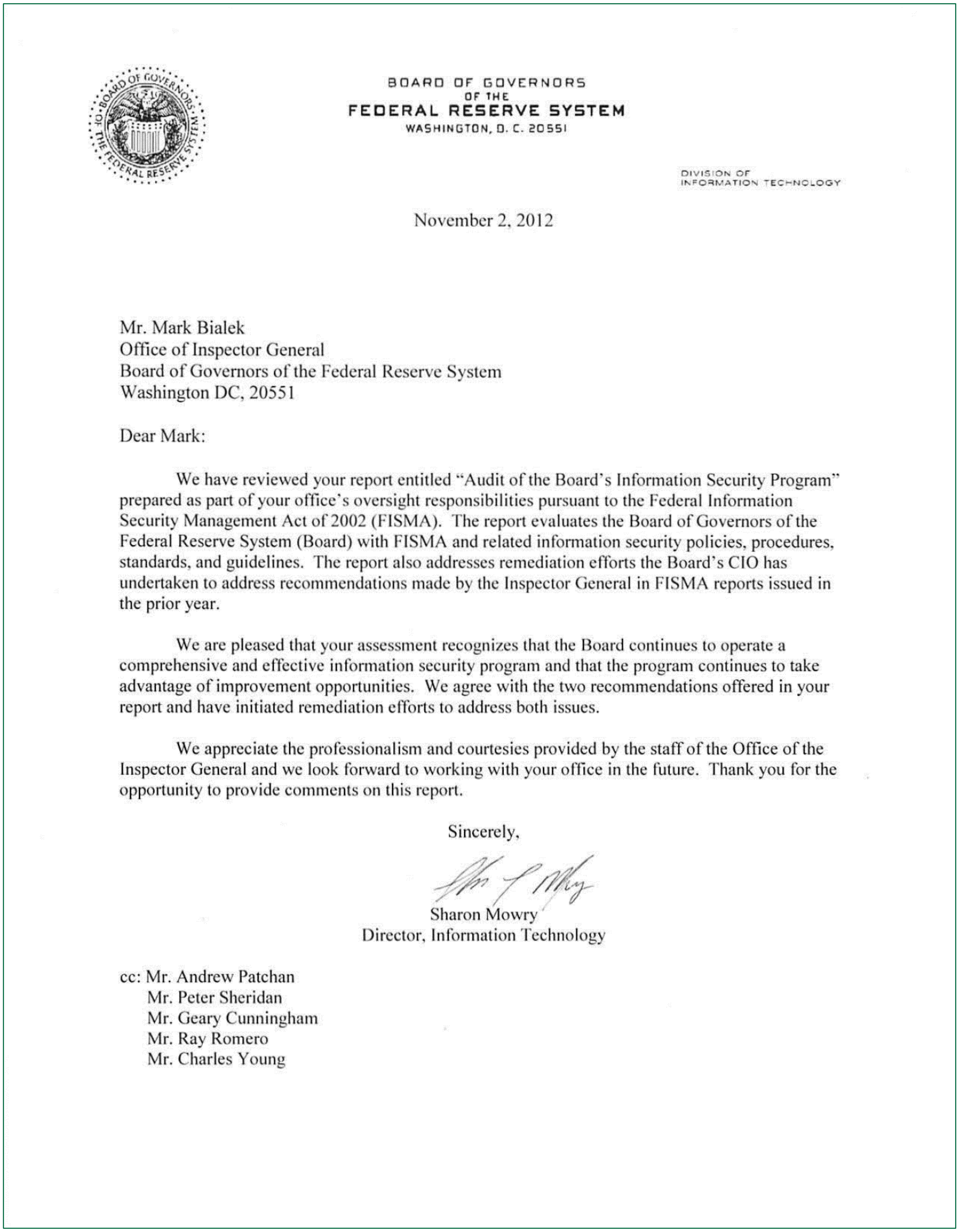
The Board has an overall governance approach for capital planning and budgeting that covers investments in information security. The Division of IT is responsible for financing the security of general support systems such as e-mail as well as other elements of the technical infrastructure. The Committee on Board Affairs in turn is responsible for approving the Board's overall budget. NIST SP 800-53 states that organizations may designate and empower an investment review board (or similar group) to manage and provide oversight for the information security–related aspects of the capital planning and investment control process.

Work to be done:

The Division of IT has implemented an IT performance reporting dashboard that is designed to capture the business value and performance of the Board's information systems. Currently, the dashboard is focused on providing an overview of performance, such as security patching, virus detection, and POA&M reporting. For POA&M reporting, the dashboard provides quantitative information on the status of remediation efforts. The dashboard can also be considered for use by Division of IT management in identifying or tracking the information security investment for remediation efforts.

Our 2011 FISMA report included as a matter for management's consideration that, to ensure adequate tracking of system security investments, the CIO should (1) enhance the Board's system development methodology by clarifying steps to account and budget for security over the system life cycle and (2) analyze how security capital planning information at the system and enterprise levels can be integrated into the IT performance dashboard to provide a more comprehensive understanding of the business value and performance of the Board's information systems. We continue to believe that the CIO should consider enhancing the Division of IT's system development methodology to account for information security expenditures and integrating security capital planning information into the IT performance dashboard.

Appendix 2
Management's Comments



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

DIVISION OF
INFORMATION TECHNOLOGY

November 2, 2012

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 "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 Board's CIO has undertaken to address recommendations made by the Inspector General in FISMA reports issued in the prior year.

We are pleased that your assessment recognizes that the Board continues to operate a comprehensive and effective information security program and that the program continues to take advantage of improvement opportunities. We agree with the two recommendations offered in your report and have initiated remediation efforts to address both issues.

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. Peter Sheridan
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

www.federal reserve.gov/oig
www.consumerfinance.gov/oig
11/12