

Board of Governors of the Federal Reserve System

**Audit of the Board's
Information Security Program**



Office of Inspector General

November 2011

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



OFFICE OF INSPECTOR GENERAL

November 14, 2011

Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Members of the Board:

The Office of Inspector General (OIG) is pleased to present its report on the *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 June 2011 through October 2011, and we reviewed security controls for Board applications 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 Office of Management and Budget (OMB) requests that both the Chief Information Officer (CIO) and the IG perform analysis of 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. 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 August 2011, DHS issued revised reporting requirements for IGs' analysis of their respective agency's information security management performance, in line with the requirements of FISMA. In accordance with DHS' revised requirements, our FISMA review included an analysis of the Board's information security-related processes in the following areas: risk management, continuous monitoring management, plans of action and milestones (POA&Ms), identity and access management, remote access management, security configuration management, security training, contractor oversight, contingency planning, incident response and

reporting, and security capital planning. Appendix 1 contains our analysis of the Board's progress in implementing key FISMA requirements and discusses our recommendation and observations in more detail. In addition to this report, we will provide our analysis to OMB under separate cover via automated submission. Our response will be submitted with the CIO's response to the OMB reporting requirements.

Overall, we found that the Board's CIO continues to maintain a FISMA-compliant approach to the Board's information security program that is generally consistent with requirements established by the National Institute of Standards and Technology (NIST) and OMB. The Information Security Officer (ISO) continues to issue and update information security policies and guidelines. During 2011, the ISO developed an enterprise information technology (IT) risk assessment framework initiative and a continuous monitoring strategy and began to implement a new automated workflow support tool that will provide an automated workflow method for documenting, reviewing, and approving the security posture of all Board information systems. In addition, the ISO took corrective actions in response to a number of open recommendations from our prior FISMA reports.

To transform the Board's Certification and Accreditation process into the NIST Risk Management Framework and implement new NIST requirements for assessing security controls, our 2010 FISMA report included two recommendations to the CIO: (1) continue to develop and implement a Board-wide IT risk management strategy as required by the NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (SP 800-53), Program Management family of controls; and (2) as additional NIST and OMB guidance is issued and becomes effective, develop a continuous monitoring strategy and implement a continuous monitoring program as required by SP 800-53, Security Assessment and Authorization family of controls. Because the ISO developed and began implementation of an enterprise IT risk assessment framework within the Division of IT, we are closing out the first recommendation. With the ISO issuing a continuous monitoring strategy and beginning the implementation of an expanded continuous monitoring program, we are also closing our second 2010 recommendation.

Although progress has been made by the ISO to address the new 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 report contains one recommendation that the CIO complete and fully implement the enterprise IT risk assessment framework Board-wide along with ensuring the automated workflow support tool is fully operational in order to comply with updated NIST guidance on the new Risk Management Framework. In addition, our report includes matters for management's consideration based on our analysis of the Board's contractor oversight and security capital planning programs. While not specifically required by NIST or OMB requirements, the following actions could help strengthen the Board's information security posture: (1) under the Board's Contractor Oversight program, ensure that the Board's new automated workflow tool for managing the security posture of all Board information systems incorporates appropriate security management information for third party systems operated by Federal Reserve Banks on behalf of the Board and (2) under the Board's Security Capital Planning and Investment Program, to ensure adequate

tracking of system security investments, enhance the Board's system development methodology by clarifying steps to account and budget for security over the system life cycle; and analyze how security capital planning information at the system and enterprise-level 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.

Given the new NIST guidance regarding risk management, that incorporates risk assessment, we are also closing a recommendation from our 2008 FISMA report that the CIO ensure 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. 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. Our 2010 FISMA report also included a third recommendation, for the CIO to identify all information technology services provided by organizations other than Board personnel, and determine if they need to be accredited as a third party contractor system or as part of an existing General Support System or major application. We believe the CIO has taken sufficient actions to close this recommendation.

As stated previously, we also review security controls implemented for Board applications on an ongoing basis. During the past year, we completed security control reviews for two Board systems: (1) the Board's public website system (PubWeb) and (2) the Visitor Registration System. We also completed a security control review of the Federal Reserve System's National Remote Access Services. Our reviews of these systems' information security controls have identified areas where controls need to be strengthened. Given the sensitivity of the issues involved with these reviews, the specific results are being provided to management in separate restricted reports that will be summarized on our publicly available website. During this year's FISMA review, we started audits of (1) the Board's contingency program, (2) third-party applications operated by the Federal Reserve Bank of Richmond in support of the Board's Division of Banking Supervision and Regulation, and (3) the Federal Reserve System's Office of Employee benefits and its third-party contractors.

We performed our application control testing based on selected controls identified in 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. In following up on open recommendations from prior security control reviews, we determined that sufficient corrective actions were taken to close 19 of 21 open recommendations from 3 security control reviews. We will continue to follow up on actions taken regarding our FISMA and security control review report recommendations as part of future audit and evaluation 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 recommendation that the CIO complete and fully implement the enterprise IT risk assessment framework Board-wide along with ensuring the

automated workflow support tool is fully operational for the Board to be compliant with updated NIST guidance on risk management.

We appreciate the cooperation that we received from the Board during our review. The principal contributors to this report are listed in appendix 3. We are providing copies of this audit report to Board management officials. The report will be added to our publicly-available web site and will be summarized in our next semiannual report to Congress. Please contact me if you would like to discuss the audit report or any related issues.

Sincerely,

A handwritten signature in cursive script, appearing to read "Mark Bialek".

Mark Bialek
Inspector General

cc: Ms. Maureen Hannan
Mr. Geary Cunningham
Mr. Raymond Romero

APPENDIXES

The Office of Inspector General's Analysis of the Board's Progress in Implementing Key FISMA and OMB Requirements

The following is our analysis of the Board's progress in implementing key FISMA requirements, including progress to date and work to be done. Our analysis identifies one new recommendation (see page 11).

Risk Management Program

Requirement:

FISMA requires organizations to develop and implement an organization-wide information security program for the information and information systems that support the operations and assets of the organization, including those provided or managed by another organization, contractor, or other source. For non-national security programs and information systems, agencies must follow NIST standards and guidelines. For legacy information systems, agencies are expected to be in compliance with NIST standards and guidelines within one year of the publication date unless otherwise directed by OMB. NIST has developed a Risk Management Framework and issued three special publications to 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.

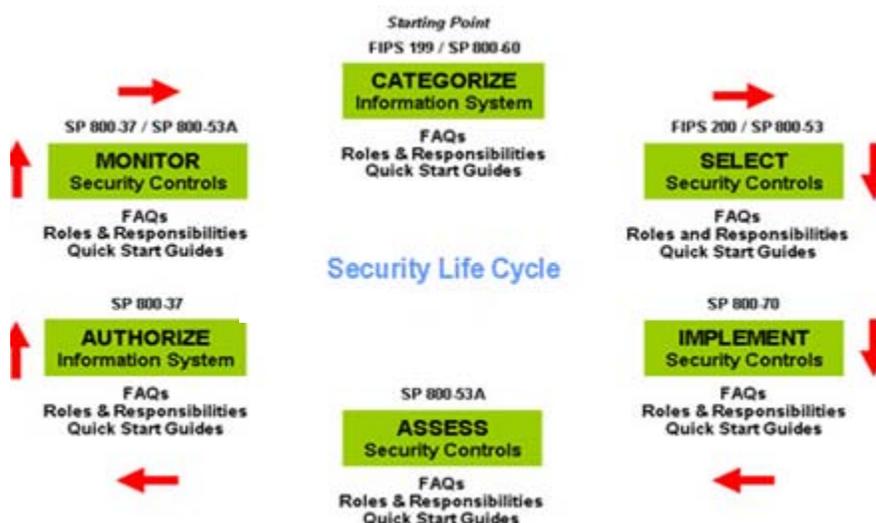
In August 2009, NIST issued SP 800-53 that contained a new information security Program Management (PM) family of controls. The PM controls focus on the organization-wide information security requirements and directed organizations to develop a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems and implement that strategy consistently across the organization. Additional information for this SP 800-53 control 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.

In February 2010, NIST issued Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (SP 800-37). 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 the NIST Risk Management Framework that we discuss in our prior year report 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.

In March 2011, NIST issued Special Publication 800-39, *Managing Information Security Risk* (SP 800-39). SP 800-39 states 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—providing both the necessary and sufficient risk response measures to adequately protect the missions and business functions of those organizations.

Figure 1 shows NIST’s Risk Management Framework and identifies NIST’s related guidance.

Figure 1. NIST’s Risk Management Framework



Progress to Date:

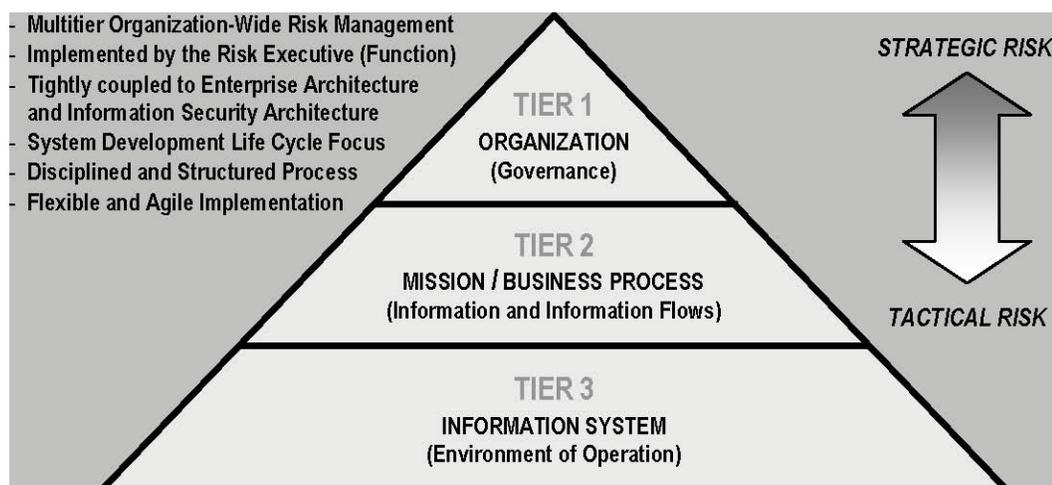
SP 800-37, which was required to be implemented by February 2011, incorporates the traditional processes the Board uses to authorize its information systems, but expands the risk management approach to address risk-related concerns at the organizational level, the mission and business level, and the information system level. SP 800-39, which is not required to be implemented until March 2012, provides detailed guidance for implementing the SP 800-37 requirement for an integrated, organization-wide program for managing information security risk.

In prior years, the Board’s information system risk management approach has been generally focused at the information system level, which was promulgated by 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. The SP 800-53 PM family of controls focuses on organization-wide information security controls that are independent of any particular information system. SP 800-37 integrates organization risks into the system authorization process that continues to include an overall analysis of individual system risk based on the control families contained in SP 800-53.

Figure 2 shows a three-tiered approach introduced by SP 800-37 and expanded upon in SP 800-39 that revolves around the concepts that managing information system-related security risks is a complex, multifaceted undertaking that requires the involvement of the entire organization—from senior leaders providing the strategic vision and top-level goals and objectives for the organization (Tier 1), to mid-level leaders planning and managing projects (Tier 2), to 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



Our 2010 Audit of the Board’s Information Security Program (2010 FISMA report) included a recommendation that the CIO continue to develop and implement a Board-wide IT risk management strategy to meet the requirement of SP 800-53. The Board’s information security program already addressed many of the controls in the PM family, but prior to fully implementing an organization-wide program for managing information security risk required by SP 800-37, the CIO needed to develop and formalize an organization-wide risk management strategy. During 2011, the ISO developed an enterprise IT risk assessment framework initiative and has begun implementation within the Division of IT. We believe this meets the intent of our recommendation, and we are closing our recommendation.

When fully implemented, the enterprise IT risk assessment framework will identify those risks that most greatly inhibit the Board from achieving its strategic objectives. In addition, the ISO has begun to implement a new automated workflow support tool that

will provide an automated workflow method for documenting, reviewing, and approving the security posture of all Board information systems. We will continue to monitor the ISO's actions as he implements the enterprise IT risk assessment framework Board-wide.

The 2010 Division of IT strategic planning initiatives included a section on enterprise risk management that states the purpose of this initiative 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. The 2010 and 2011 strategic planning initiatives also include the following:

- Developing an enterprise IT risk assessment;
- Piloting the enterprise risk management process with Board division(s);
- Preparing a common Enterprise Risk Management (ERM) framework for all divisions to use in identifying key operational and reputational residual risks;
- Developing an ongoing process for divisions to follow, assigning accountability through clearly defined roles and responsibilities, using a common risk language when evaluating the division's risks, and using a process to manage risks; and
- Creating an approach to further FISMA/ERM compliance for embedded IT.

The 2011 strategic planning initiatives continued the focus on risks with the development of a Division of IT Risk Management Committee. This committee is to provide guidance and direction to the ISO and standing work groups tasked with addressing information security and risk management issues.

Work To Be Done:

The Division of IT has had components of the three-tiered risk management program in place in prior years with a system level focus based on the existing guidance at that time. Recent guidance has 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 General Support System. As previously discussed, the ISO has begun to implement a new automated workflow support tool that will provide an automated workflow method to filter down risks to individual information systems.

Although the Board has a process to document risks associated with an information system being in compliance with a baseline of controls, our 2008 FISMA report included a recommendation that the CIO ensure 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. Given the new NIST guidance regarding risk management that incorporates risk assessments, we are closing this recommendation. 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.

Although progress has been made by the ISO to address 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 needs to be fully operational for the Board to meet the requirements of NIST's organization-wide risk management approach.

Recommendation 1: We recommend that the CIO complete and fully implement the enterprise IT risk assessment framework across all divisions, along with ensuring the automated workflow support tool is fully operational, in order to comply with updated NIST guidance on the new Risk Management Framework.

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 Risk Management Framework with a target audience of individuals with implementation and operational responsibilities for mission/business processes, system development and integration, system and/or security management oversight, security control assessment and monitoring, and security.

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. Agencies are expected to be in compliance with NIST standards and guidelines within one year of the publication date unless otherwise directed by OMB.

SP 800-137 states 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 much 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; and
- Review and update the continuous monitoring strategy and program.

A robust continuous monitoring program 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.

Progress to Date:

Our 2010 FISMA report discussed the Board’s transition to the NIST Risk Management Framework and that the Board can improve and integrate both manual and automated monitoring processes into its continuous monitoring efforts to mature existing information security processes. This includes the annual testing of information system controls that the ISO has had in operation for many years as part of meeting FISMA requirements. Each year the ISO reviews one-third of the baseline controls for Board applications, with certain critical controls tested every year.

Our 2010 FISMA report included a recommendation that as additional NIST and OMB guidance is issued and becomes effective, the CIO develop a continuous monitoring strategy and implement a continuous monitoring program as required by NIST 800-53, Revision 3, Security Assessment and Authorization family of controls. During 2011, the ISO developed a continuous monitoring strategy based on a framework devised by DHS in concert with other agencies such as the Department of State. The ISO’s continuous monitoring strategy indicates that 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 CIO continues to implement vulnerability scanning and network monitoring tools, including intrusion detection and audit log consolidation processes to identify and defend against cyber attacks. 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 ISO is utilizing these tools and processes to meet NIST and OMB requirements for continuous monitoring. The ISO plans to implement this framework through September 2012.

With the ISO issuing a continuous monitoring strategy and beginning the implementation of an expanded continuous monitoring program, we are closing our 2010 recommendation. The ISO's continuous monitoring strategy incorporates 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 information technology operations. The strategy document reflects six automated data gathering mechanisms that are currently in use and additional mechanisms that are planned to be in place by July 2012. We will monitor the ISO's actions in implementing the continuous monitoring program.

Work To Be Done:

Since our 2010 FISMA report, the ISO has developed a continuous monitoring strategy and started the implementation of a new automated workflow support tool, and NIST has now issued SP 800-137 that provides more defined guidance on information system security continuous monitoring.

The ISO anticipates that the new automated workflow support tool will provide an efficient and automated workflow method for documenting, reviewing, and approving the security posture of all Board information systems. The ISO indicated that system categorization worksheets, system security plan information, supplemental control questionnaire items, and control baselines for all the major applications and IT General Support System components will be loaded into the automated tool by the end of 2011. Also, test results for major applications, as well as risk assessments and POA&M information, is planned for addition by the fourth quarter 2011. The ISO stated that General Support System subsystems and minor applications will be added in 2012. 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 where information technology 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:

Our 2009 FISMA report recommended that the CIO independently verify that appropriate corrective action has been implemented before items are removed from the Board's POA&M. Our security control reviews had identified instances where POA&M items that were designated as completed and removed from POA&Ms were only partially or not effectively remediated, which translates into extended security exposures for Board systems.

In response to our recommendation, the ISO established POA&M procedures for the ISO's Information Security Compliance staff to validate the remediation of action items during a system control review or otherwise request documentation to determine if corrective action has been sufficiently completed. Items with insufficient evidence or those that have been delayed will be evaluated as to why the actions have not been completed and revised accordingly with an updated completion date.

We have reviewed supporting documentation that substantiates the implementation of the ISO's independent verification of POA&M action items. Based on this verification program we are closing our 2009 recommendation.

Work To Be Done:

Now that the independent verification program has been implemented, the ISO plans for this to be an ongoing process and part of the continuous monitoring program. Verification of supporting documentation will be part of the remediation of completed actions. We will monitor the ongoing verification process as part of the overall development of the new continuous monitoring initiatives.

Identity and Access Management Program**Requirement:**

The Board is required to establish and maintain an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Such a program should include:

- Documented policies and procedures for account and identity management,
- Identification of all users that access agency systems,
- Integration between the Agency's Personal Identity Verification (PIV) program, which includes the use of a PIV smartcard for access to facilities and information systems, and its use of multi-factor authentication¹, and
- Identification of devices that are attached to the agency's network.

¹ Multi-factor authentication refers to using two or more factors to achieve authentication. These factors can include (1) passwords, (2) electronic tokens, and/or (3) biometrics. In the context of an agency's PIV program, multi-factor authentication can refer to granting access to an information system based on a PIV card and a password.

The Board's information security program requires controls to be incorporated for all information systems that ensure 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 General Support System provides identification and authentication services that Board systems rely on. This includes Active Directory network level authentication, Lotus Notes user identification and passwords, and remote access using multifactor authentication. The Board has also 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 Active Directory and other systems as needed.

Active Directory provides a way to manage elements of a network, including desktops, servers, groups, users, domains, security policies, and user-defined and computer-defined objects. Our 2010 FISMA report noted that local change-control processes and procedures utilized for Active Directory updates were not documented in the Division of IT's policies and procedures. In 2011, the ISO updated procedures for the Board's Active Directory operating environment. These procedures cover configuration management and change control, account management, and audit and accountability. The ISO has also implemented automated tools to ensure consistent configuration of active directory settings Board-wide.

Work To Be Done:

As part of the Board's physical security program, PIV cards are used for physical access control to its buildings, but are not used to provide access to information systems. Multi-factor 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. The ISO has a pilot program underway to test the use of PIV cards for access to the Board's network. This pilot program is currently limited to specific Board staff.

Our 2010 FISMA report noted that the Board does not identify or authenticate devices that are attached to the network or have the capability to distinguish these devices from users. Our review also noted that compensating controls were in place and that several initiatives were underway to identify devices. During our 2011 FISMA review, we found that the ISO has not implemented a solution to identify or authenticate devices attached to the Board's network. The ISO plans to pilot such a solution in 2012. 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 agencies to establish and maintain a remote access program that (1) includes documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access; (2) protects against unauthorized connections or subversion of authorized connections; and (3) uniquely identifies and authenticates users for all access.

Progress to Date:

As part of our 2011 FISMA work in analyzing the Board's remote access program, we completed an audit of the Federal Reserve System's National Remote Access Services (NRAS) infrastructure. The Board and the 12 Federal Reserve Banks use NRAS for remotely accessing Board and Federal Reserve Bank information systems. Our objectives were to evaluate the effectiveness of selected security controls and techniques to ensure the Board maintains a remote access program that is generally compliant with FISMA requirements.

Our review was divided into two separate phases, with the first phase primarily addressing technical and operational control areas, and the second phase addressing procedures. Overall, our review found that the Federal Reserve's remote access system is technically and operationally sound, and the Board has developed an adequate process to administer the token keys for Board personnel.

Work To Be Done:

Although our review found that the Federal Reserve's remote access system is technically and operationally sound, we identified opportunities to strengthen information security controls to help ensure the Federal Reserve's remote access system meets FISMA's requirements. While we did not identify any significant improvement opportunities, we did note that NRAS is not fully in compliance with FISMA and the Board's information security program. NRAS is considered a contracted service—it is not an application that stores or processes Board data, and it is not listed on the Board's FISMA inventory.

The Reserve Banks have established plans to implement an enterprise information security program based on the NIST framework. The Reserve Banks plan to transition over multiple years. As the Reserve Banks implement a FISMA compliant program, NRAS will be brought into compliance. We will continue to monitor the CIO's and ISO's actions in overseeing the Reserve Banks' compliance with FISMA as they transition to an information security program based on the NIST framework.

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. The Board's information security program requires that the changes to configuration settings of infrastructure services require approvals, testing, and documentation and need to be performed within the scheduled maintenance window.

The configuration of an information system and its components has a direct impact on the security posture of the system. A baseline configuration is a set of specifications for a system, that has been formally reviewed and agreed upon at a given point in time and that can be changed only through change control procedures. This baseline configuration is used as a basis for future builds, releases, and/or changes. Changes to the configuration are often needed to stay up-to-date with changing business functions and services and information security needs.

In August 2011, NIST issued Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems* (SP 800-128). SP 800-128 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 application configurations require approval from system owners and require necessary testing and analysis.

Work to be done:

In our review of the Board's contingency plan for infrastructure services, we noted that there is not separate and detailed documentation of security configuration settings for infrastructure services at the contingency site. Once we complete our review we will report our results under separate cover.

In our 2010 FISMA report, we identified as a matter for management's consideration that the CIO should evaluate separately accrediting the Board's infrastructure services supporting external facing systems and clarify guidance to assist system owners in managing application level security settings. The ISO continues to make progress in this area. The Information Security Unit is continuously monitoring the external facing systems for threats and vulnerabilities. We will continue to monitor the ISO's actions in implementing security configuration management.

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 includes (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 Board continues to require all Board employees, contractors, and interns to complete an annual security awareness quiz that includes topics such as security incidents, safety precautions for international travel, handling personally identifiable information, and phishing-fraudulent e-mails. The ISO also publishes periodic articles discussing various computer security topics, such as tips on how to become a highly secure computer user, as well as conducts annual training on the Board's information security program, updates, and changes. Board divisions also continue to report to the ISO on the status of specialized training for personnel with significant information system security responsibilities.

The Board's security awareness training program is geared towards creating awareness of FISMA requirements and the Board Information Security Program for various end users,

including system owners, developers, managers, quality assurance analysts, and authorizing officials who are responsible for making decisions regarding information systems. Our 2009 FISMA report contained a recommendation that the CIO provide mandatory specific FISMA training for selected staff with FISMA responsibilities. Our 2010 FISMA analysis of security training continued to identify key individuals responsible for various aspects of ensuring the security of Board systems who had not attended any session of the FISMA training provided by the CIO.

During 2011, the ISO established a process that entailed the ISO and the Manager for the Information Security Compliance group providing a Board Information Security Program training update to each of the Board divisions' key end users, such as system owners, authorizing officials, and system managers, some of whom did not attend the annual information security program training that is provided by the ISO. As a result of the performance of this information security program update, we are closing our recommendation that specific FISMA training be provided for selected staff with FISMA responsibilities.

Work To Be Done:

The ISO has performed a Board information system security program training activity that helps fill a training gap for a number of the key end users for Board systems. Some key end users may miss the opportunity to attend the annual Board information security program overview, updates, and changes training sessions that are generally conducted by the ISO in the first quarter of each year. The ISO should consider how the recently completed division-by-division update can be integrated into the overall Board information systems security training program to better ensure full Board coverage. We will continue to monitor the ISO's annual FISMA training efforts.

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 information and services provided. 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 Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, risk rating, authorization status, and interconnections.

The Board's third party systems are primarily located within the Federal Reserve Banks. The ISO and the Board's Division of Banking Supervision and Regulation (BS&R) perform on-site 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. Further, 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.

Our 2010 FISMA report identified a contractor service that, while being essential to the Board's recruitment process, was not included in the Board's FISMA inventory. We recommended that the CIO identify all information technology services provided by organizations other than Board personnel and determine if they need to be accredited as a third party contractor system or as part of an existing General Support System or major application. In response to our recommendation, the ISO updated the Board's FISMA inventory to include the contractor service we identified. Further, the ISO undertook a broader effort to identify other third party systems and services across the Board that are not on the FISMA inventory and their associated security requirements. As such, we are closing our 2010 recommendation.

Work To Be Done:

The Federal Reserve Banks are not required to follow NIST and OMB guidance but have decided to transition 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 migration to this new information security program has begun for Federal Reserve Bank national IT infrastructures. This 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 stated earlier, BS&R is utilizing BISPMS for Federal Reserve Bank systems that store or process Board information. As previously discussed in the Risk Management Program section of this report, the ISO is in the process of transitioning Board divisions to an automated workflow support tool that provides an automated workflow for documenting, reviewing, and approving the security posture of all Board information systems, as required by FISMA.

Both tools are used to support FISMA compliance activities for Board systems and they serve similar purposes. The ISO's tool currently does not include in its automated workflow support tool information on BS&R's FISMA continuous monitoring activities for Federal Reserve Bank systems that store or process Board information. For example, the BISPMS contains information on security control assessments and POA&Ms for Federal Reserve Bank systems that store or process Board information. Security control assessments and POA&Ms provide important information on security weaknesses and related mitigation plans. Including this information within the Board's automated workflow support tool could assist the ISO in implementing the Board's risk management and continuous monitoring strategies mentioned earlier in our report. As part of our ongoing work related to information security, we will continue to monitor the ISO's actions in overseeing third parties' compliance with FISMA and the requirements of the Board's information security program.

Matters for Management's Consideration: Ensure that the Board's automated workflow support tool for managing the security posture of all Board information systems incorporates appropriate security management information for third party systems operated by Federal Reserve Banks on behalf of the Board.

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. In May 2010, NIST issued Special Publication 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems* (SP 800-34). SP 800-34 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.

Contingency planning considerations and strategies address the impact to Board operations and functions based on availability security objectives of mission critical applications. SP 800-34 defines a seven-step contingency planning process. These seven progressive steps are designed to be integrated into each stage of the system development life cycle: (1) develop the contingency planning policy statement; (2) conduct the business impact analysis; (3) identify preventive controls; (4) create contingency strategies; (5) develop an information system contingency plan; (6) ensure plan testing, training, and exercises; and (7) ensure plan maintenance. In addition, the NIST guidance requires that agencies' continuity of operations must be sustained 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 that include policy, planning,

training, testing, alternate storage site, alternate processing site, telecommunication services, backup, recovery, and reconstitution.

Progress to date:

The Board is maintaining an agency-wide business continuity plan that is consistent with NIST and OMB requirements. The Board continues to conduct semi-annual contingency tests of its mission critical applications. The Board divisions are participating in these tests to verify that their applications are working as designed in a contingency situation. The ISO has issued a Business Impact Analysis template as guidance to determine individual applications' continuity of operations requirements. The semi-annual tests include testing and availability of infrastructure services that are essential for mission critical applications. 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.

Work to be done:

We are currently reviewing security controls of the Board's contingency program, which we will report under separate cover. The Board's contingency planning, logistics, implementation, and testing of operations are handled by different divisions. The Board's continuity of operations document identifies the key personnel and their corresponding technical teams and reporting hierarchy that are responsible for different areas of infrastructure services. However, a central point of contact for Board-wide coordination, validation, reporting, and verification of the mission critical applications would improve efficiency. In addition, a Board-wide process of reconciliation and monitoring of what applications were tested and reporting of the test results should be established. The IT infrastructure resources and the capacity at the contingency site also need to be analyzed to ensure consistency with the Board's primary data center capabilities.

Incident Response & Reporting

Requirement:

The Board is required to create, provision, 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.

An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Performing incident response effectively is a complex undertaking, and establishing a successful incident response capability requires substantial planning and resources. Continually monitoring threats through intrusion detection and prevention

systems and other mechanisms is essential. The typical types of incidents include denial of service, malicious code, unauthorized access, inappropriate usage, and lost or stolen devices/storage media, including laptops. The incident response team is required to offer services such as advisory distribution, vulnerability assessment, intrusion detection, education and awareness, and patch management.

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:

The Board has issued the *Information Security Incident Handling Guide* as an appendix to the Board's information security program. This guidance helps users to appropriately handle security incidents and identifies the roles and responsibilities of the incident response team. In addition, the Board has issued *Device and Document Loss Notification Report*, a form that should be used to report lost/stolen Board devices such as mobile phones, storage media, and laptops. The ISO produces quarterly performance reports on security incidents, security patches, virus protection, POA&M's, and penetration test findings. The ISO continues to send monthly security log information to US-CERT and reports security incidents within established timeframes. In addition, the ISO has implemented automated tools for detecting intrusions, centralized log file analysis, and network analyzers for prevention of denial of service attacks.

Work to be done:

The ISO continues to post security related articles, security incidents, and advisories on the Board's internal website. We will continue to monitor incident reporting and handling at the Board as part of our ongoing FISMA related audit work.

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 IT investments integrate strategic planning, budgeting, and IT management considerations. NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, 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 overall agency's 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 investment life cycle. This information will flow to the enterprise level to support IT compliance and integration activities.

The 2011 DHS FISMA reporting questions direct IGs to determine if 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 53's and Exhibit 300's, are not directly applicable to the Board.

Progress to Date:

The Board has developed an overall governance approach for capital planning and budgeting that covers investments in information security. Board divisions are required to prepare and submit budget and planning requests for information security investments to the Strategic Planning Group (SPG). The SPG reviews the requests and makes recommendations to the Committee on Board Affairs (CBA). The CBA in turn is responsible for approving the Board's overall budget.

The Division of IT has established a system development methodology (SDM) that provides a framework for managing project life cycles. The SDM includes seven phases that are designed to ensure that systems meet business requirements, use appropriate technology, and meet quality standards. The phases include project initiation, planning, requirements specification, design and development, testing, implementation, and maintenance. The SDM requires that the estimated budget and resources required to complete a project be stipulated and updated as the project progresses. In addition, as part of its POA&M program, the ISO requires Board divisions to provide a high-level

estimate of the man hours and/or funds required to address the identified weaknesses or enhancements.

The Division of IT has also implemented an initial version of 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 Board plans to evolve the dashboard to provide a comprehensive picture of IT performance.

Work To Be Done:

As stated earlier, the Board's SDM requires that resources and budget estimates be documented and updated throughout a project's lifecycle. However, the SDM does not specifically require managers to account and budget for security over the system life cycle. For example, as part of the maintenance phase of the SDM, security configuration, change management, and continuous monitoring activities would be performed for a system. This would include monitoring security controls through vulnerability scans and penetration testing. While the SDM requires managers to ensure that resources are available to support maintenance activities, it does not specifically require managers to account and budget for these activities.

Budget information related to system security activities could serve as an input to the IT performance reporting dashboard to provide a more comprehensive view of the business value and performance of Board information systems. For instance, expenditures for continuous monitoring activities could be used in conjunction with information on system vulnerabilities and patching to determine the impact of resources spent.

As noted in the section of our report on the Board's risk management program, the ISO is in the process of implementing an automated workflow support tool to provide a workflow method for documenting, reviewing, and approving the security posture of all Board information systems. Information on security weaknesses for all Board systems is to be included in this tool. When fully implemented for all Board divisions, this tool could help the ISO in identifying system-level and enterprise-level security investments that could increase the overall security posture of the Board and mitigate risks.

Matters for Management's Consideration: To ensure adequate tracking of system security investments, the CIO should enhance the Board's system development methodology by clarifying steps to account and budget for security over the system life cycle and analyze how security capital planning information at the system and enterprise-level 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.



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

DIVISION OF
INFORMATION TECHNOLOGY

November 9, 2011

Mr. Mark Bialek
Office of the Inspector General
Board of Governors of the Federal Reserve System
Washington, D.C. 20551

Dear Mark:

We have received and 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 CIO has undertaken to address recommendations made by the Inspector General FISMA reports issued in prior years.

We appreciate the report's findings that the Board's CIO continues to maintain a FISMA-compliant approach to the Board's information security program that is generally consistent with requirements established by the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB). The report also recognizes that adequate corrective action has been taken to close open recommendations from prior FISMA reviews.

The report recognizes that the Board has initiated an enterprise IT risk assessment framework and a continuous monitoring strategy that are consistent with new NIST guidance on risk management. We agree with the recommendation that the CIO complete and fully implement the enterprise IT risk assessment framework Board-wide along with ensuring the automated workflow support tool be fully operational for the Board to be compliant with updated NIST guidance on risk management.

We appreciate the professionalism and courtesies provided by the staff of the Office of 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,

A handwritten signature in cursive script that reads "Maureen Hannan".

Maureen Hannan
Director, Information Technology

cc: Mr. Geary Cunningham
Mr. Andrew Patchan
Mr. Ray Romero

Principal Contributors to the Report

Robert McMillon, Auditor-in-Charge

Khalid Hasan, Senior IT Auditor

Satynarayana-Setty Sriram, IT Auditor

Robert Delgesso, IT Auditor

Peter Sheridan, OIG Manager

Andrew Patchan, Jr., Associate Inspector General for Audits and Attestations