Board of Governors of the Federal Reserve System

Audit of the Board's Information Security Program

Office of Inspector General

November 2010

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

OFFICE OF INSPECTOR GENERAL

November 15, 2010

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 March 2010 through October 2010, 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. In April 2010, OMB 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 OMB's revised requirements, our FISMA review included an analysis of the Board's information security-related processes in the following areas: certification and accreditation, continuous monitoring, plans of action and milestones (POA&Ms), account and identity management, remote access, security configuration management, security training, contractor oversight, contingency planning, and incident response and reporting. Appendix 1 contains our analysis of the Board's progress in implementing key FISMA requirements and discusses our recommendations 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, and is piloting a Board-wide information technology (IT) risk assessment framework to capture technology, operational, and strategic risks for IT resources. As NIST and OMB continue to develop new guidance and update existing standards and publications to transform the traditional Certification and Accreditation (C&A) process into a new Risk Management Framework, opportunities exist for the CIO to continue to mature the Board's information security processes through further assessment of risks and controls under an organization-wide risk management strategy, with a focus on more continuous monitoring and automated methods. Continuous monitoring of security controls is a cost-effective and important part of an organization-wide risk management strategy, which enables an agency to maintain an accurate understanding of its security risks by selecting subsets of security controls for monitoring on an ongoing basis.

The Board's C&A process meets the current standards as prescribed by NIST and OMB, but primarily relies on manual testing and evaluation of the information systems' security controls. During the past year, NIST and OMB have begun to issue updated guidance highlighting a new Risk Management Framework that focuses on agencies being able to continuously monitor security-related information across the agency in a manageable and actionable way. Continuous monitoring of security controls is required as part of the security authorization process to ensure controls remain effective over time (after the initial security authorization or reauthorization of an information system) in the face of changing threats, missions, operational environments, and technologies. As additional NIST and OMB guidance is issued and becomes effective, agencies will need to automate security-related activities, to the extent possible, and acquire tools that correlate and analyze security-related information. Our security control reviews show that the CIO continues to implement vulnerability scanning and network monitoring tools to expand the Board's capabilities to identify and defend against cyber attacks. The ISO is utilizing these tools and processes to meet NIST and OMB requirements for continuous monitoring. As additional NIST guidance is issued and becomes effective, a documented continuous monitoring strategy is needed to analyze how these automated processes, which are used in day-to-day operations, supplement the ISO's annual control testing. We believe an organization-wide risk management strategy, coupled with a continuous monitoring strategy, will provide a more meaningful and mature approach to FISMA compliance and will further strengthen the Board's information security posture.

Our report contains three recommendations. To transform the Board's C&A process into the NIST Risk Management Framework and implement new NIST requirements for assessing security controls, our report includes the following 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, Revision 3), 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, Revision 3, Security Assessment and Authorization family of controls.

Our report also includes 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 (GSS) or major application.

In addition, our report includes matters for management's consideration based on our analysis of the Board's security-related processes. Although not specifically required by NIST or OMB requirements, the following actions could help to strengthen the Board's information security posture: (1) under the Board's certification and accreditation program, provide system owners additional information on security assessments of the GSS components, include additional relevant information in system security plans, and implement risk-based sampling as part of the security control assessment testing; and (2) under the Board's configuration management program, separately accredit the externally facing components of the IT GSS and major applications, and clarify guidance to assist system owners in managing application level security settings. Appendix 1 contains our analysis of the Board's progress in implementing key FISMA requirements and discusses our recommendations and observations in more detail.

During this year's FISMA review, we also followed up on the status of corrective actions in response to five open recommendations from our prior FISMA reports and nine open recommendations from two security control reviews. As discussed in appendix 1, we determined that the Board's corrective actions are sufficient to close two of the four recommendations made in our 2009 FISMA report. The other two recommendations relate to improving the POA&M and information security training programs. While the ISO has made progress in these areas, corrective action is still underway. In addition, our 2008 FISMA report included a recommendation to ensure that risk assessments adequately identify, evaluate, and document the risks to an information system based on potential threats, vulnerabilities, and controls. As discussed earlier, the ISO continues to issue and update information security policies and guidelines, and is piloting a Board-wide IT risk assessment framework to capture technology, operational, and strategic risks for IT resources. We will keep this recommendation open as we continue to monitor the CIO's and the ISO's actions in overseeing the planned enhancements to the risk assessment process. In following up on the Board's actions in response to two of our prior security control reviews, we determined that sufficient actions have been taken to close all nine open recommendations. 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 security.

As stated previously, we also review security controls implemented for Board applications on an ongoing basis. During the past year, we reviewed security controls for two Board systems: (1) the Board's public web site system (PubWeb) and (2) the Visitor Registration System. We also reviewed the Federal Reserve System's National Remote Access Services, and we began a review of third-party applications operated by the Federal Reserve Bank of Richmond in support of the Board's Division of Banking Supervision and Regulation. Our reviews of these systems' information security controls identified areas where controls need to be strengthened but, given the sensitivity of the issues involved with these reviews, we will be providing the specific results to management in separate restricted reports that will be summarized on our publicly available website. We performed our application control testing based on selected controls identified in

NIST Special Publication 800-53, Revision 3. 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 provided a draft of our report to the Director 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 generally agreed with our three recommendations and stated that she intends to take immediate action to address each of the recommendations. This includes updating the Board's program documentation to more accurately reflect the risk management and continuous monitoring programs. In addition, she will be reviewing the system inventory with each division and office to validate that all contractor services are correctly reflected in the inventory. The director also plans to leverage the results from the continuous monitoring program to offset compliance testing requirements during 2011.

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,

Elizabeth A. Coleman

Elizabeth A. Coleman
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 identified three recommendations (see pages 9, 16, and 24, respectively).

<u>Policies and Procedures</u>

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. For information systems under development or for legacy systems undergoing significant changes, agencies are expected to be in compliance with the NIST publications immediately upon deployment of each information system.

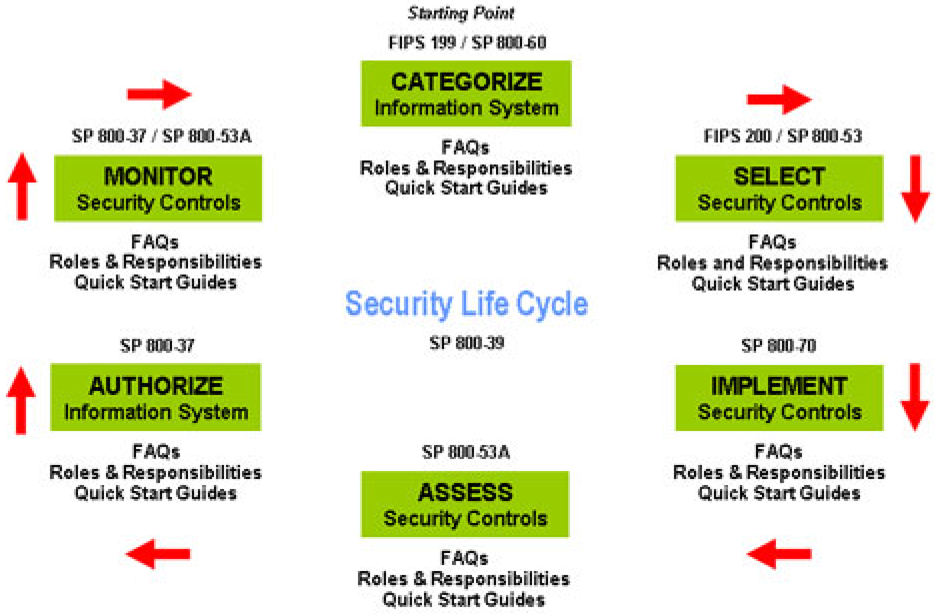
Although detailed guidance is still being developed, NIST has issued the following Special Publications (SP) that reference a new Risk Management Framework with a focus on continuous monitoring:

- In August 2009, NIST issued an updated version of SP 800-53, Revision 3; and in June 2010, issued SP 800-53A, Revision 1, *Guide for Assessing the Security Controls for Federal Information and Information Systems*; and
- In February 2010, NIST issued Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*.

In addition, within the next year, NIST is scheduled to release SP 800-30, Revision 1, *Guide to Conducting Risk Assessments*; and SP 800-137, *Guide for Continuous Monitoring of Information Systems and Organizations*.

In particular, NIST SP 800-37, Revision 1, updates an earlier guide for assessing security controls and transforms the traditional C&A process into a six-step Risk Management Framework. NIST's Risk Management Framework promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes; and provides emphasis on the selection, implementation, and assessment of security controls, information systems authorization, and security control monitoring. Figure 1 shows NIST's Risk Management Framework and identifies NIST's related guidance.

Figure 1. NIST's Risk Management Framework



According to NIST's development schedule for FISMA publications, Special Publication 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, is scheduled to be finalized in February 2011, and will provide guidelines for managing overall risk to organizational operations, organizational assets, individuals, and other organizations, resulting from the operation and use of information systems.

Progress to Date:

The ISO and his staff continue to issue new and updated information security guidance and procedures based on updated NIST guidance, and the ISO is piloting a Board-wide IT risk assessment framework to capture technology, operational, and strategic risks for IT resources. During this past year, the ISO updated the Board's information security program to reflect changes to individual security controls in NIST SP 800-53, Revision 3. SP 800-53, Revision 3, issued in August 2009, provides updated guidelines for selecting and specifying security controls for information systems to meet the requirements of Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*. To assist system owners with their annual system reviews, the ISO provided training to help system owners identify controls that were new for 2010, and developed FISMA process review checklists that identify the key courses of action necessary to complete the applicable review.

Work To Be Done:

NIST and OMB have identified requirements for organizational-wide risk management and continuous monitoring, and are finalizing additional detailed guidance. 2011 will be a transition year for the Board's information security policies and procedures as NIST and OMB issue and develop additional guidance and update existing standards and publications for agencies to implement the new Risk Management Framework. As the CIO starts planning to transition to the new framework, opportunities exist to continue to mature the Board's information security processes through further assessment of risks and controls under an organization-wide risk management strategy, and a focus on more continuous monitoring and automated methods. One of the changes in SP 800-53, Revision 3, is the addition of the information security Program Management (PM) family of controls. The PM controls focus on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. The Board's information security program already addresses many of the controls in the PM family, but prior to fully implementing the Risk Management Framework, the CIO will need to develop and formalize an organization-wide risk management strategy as required by SP 800-53, Revision 3.

SP 800-37, Revision 1, states that an organization-wide risk management strategy should include: (i) the techniques and methodologies the organization plans to employ to assess information system related security risks and other types of risk of concern to the organization; (ii) the methods and procedures the organization plans to use to evaluate the significance of the risks identified during the risk assessment; (iii) the types and extent of risk mitigation measures the organization plans to employ to address identified risks; (iv) the level of risk the organization plans to accept (risk tolerance); (v) how the organization plans to monitor risk on an ongoing basis given the inevitable changes to an organization's information systems and their operational environments; and (vi) the degree and type of oversight the organization plans to use to ensure that the risk management strategy is being effectively carried out. In addition, the process should compile and track identified and residual risks noted from annual security assessments and certification testing. Continuous monitoring of security controls is a key component in the Risk Management Framework that would be implemented based on the organization-wide risk management strategy. SP 800-39, when finalized, will provide guidelines for managing overall risk to organizational operations, organizational assets, individuals, and other organizations, resulting from the use of information systems.

Recommendation 1: We recommend that the CIO continue to develop and implement a Board-wide IT risk management strategy as required by the NIST SP 800-53, Revision 3, Program Management family of controls.

Certification and Accreditation Program

Certification involves the evaluation of an information system's management, operational, and technical security controls. Accreditation involves a senior agency official's authorization of an information system to operate. OMB requires agencies to certify and accredit their information systems in accordance with federal security policies, standards, and guidelines. The Board's information security program requires that all information systems must be certified and accredited prior to being placed into production. Certified information systems must be re-accredited every three years or if a system undergoes a major modification. Identified weaknesses in information systems must be tracked in the respective division's POA&M.

Overall, the Board has established and is maintaining a C&A program that is generally consistent with NIST and OMB FISMA requirements. The Board's information security program currently documents policies and procedures describing the roles and responsibilities of participants in the C&A process; establishes accreditation boundaries; categorizes information systems; applies a minimum baseline of security controls; assesses risks; assesses the security controls; and provides the accreditation official with the security assessment, POA&M, and security plan. However, as the Board transitions to NIST's new Risk Management Framework, we believe that the Board can more fully utilize operational efficiencies through continuous monitoring that could be incorporated into the FISMA process. Going forward, the Board can improve and integrate both manual and automated monitoring processes into its continuous monitoring processes to mature existing information security processes. Through our security control reviews we have identified many monitoring components already in place, but the monitoring processes need to be incorporated into an organization-wide risk management strategy identified in Recommendation 1 of this report.

Periodic Risk Assessments

Requirement:

FISMA requires periodic assessments of the risk and the magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

Progress to Date:

The ISO is developing a risk assessment process that will fit into the new NIST Risk Management Framework. The NIST Risk Management Framework builds upon NIST guidance in SP 800-30, which requires system owners to select a minimum baseline of security controls and then conduct a risk assessment to supplement the security control baseline as needed to ensure adequate security. As part of the Board's information security program, the ISO has developed a Risk Assessment Template and a Risk Assessment Guide to provide a systematic approach that permits information system owners to determine the extent of potential threats and risks associated with their information systems. The information system owner must complete a risk assessment for each system, regardless of whether each is categorized as a GSS, a major application, a standalone minor application, or a subsystem to any of these categories. In 2009, the ISO developed a Supplemental Controls Questionnaire to assist system owners in determining which SP 800-53 controls that are listed as optional or intended for systems that are classified as high risk may be used to mitigate a unique system risk or satisfy a unique system requirement. This year we reviewed a sample of security plans, and we found that each of the system owners had documented a baseline of controls. Any non-compliance with the baseline controls was documented in a risk assessment template.

Work To Be Done:

Our 2008 FISMA audit report contained a recommendation that the CIO 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. The current process is focused on documenting risks associated with a system being in compliance with a baseline of controls. In response to our recommendation, the ISO continues to issue and update information security policies and guidelines, and is piloting a Board-wide IT risk assessment framework to capture technology, operational, and strategic risks for IT resources. This process is intended to ascertain what type and level of risks exist, how well the organization is managing these risks, and what residual risks remain.

In addition, our prior security control reviews identified that individual system risk assessments may not take into consideration the risks accepted by the CIO as the system owner of the infrastructure. To address this issue, the ISO has developed procedures to grant system owners access to IT GSS risk assessments and to (1) require a statement that they have reviewed the IT GSS risk assessment and (2) document any system-specific concerns related to IT GSS risks. The ISO can enhance risk assessments by providing system owners with additional information on risks accepted by the CIO, such as the results of security assessments of the IT GSS. These assessments identify the controls reviewed and tested, and include exposures, concerns, informational findings, and observations that may not be included in the individual system risk assessment. In addition, the assessment reports provide a status of previously identified vulnerabilities. These security control assessment reports could provide additional key information for system owners who rely on infrastructure controls. The ISO is continuing to implement an automated risk assessment tool to provide a structured approach that he believes will provide system owners additional information and will lead to a more thorough risk assessment. The tool is currently being piloted and, once implemented, will provide a structured approach to compliance testing, remediation tracking, and automatic notification.

At this time, we are keeping the 2008 recommendation open as we continue to monitor the CIO’s and ISO’s actions in overseeing the planned enhancements to the risk assessment process.

Matter for Management’s Consideration: Provide system owners additional information on security assessments of the GSS components to contribute to a more thorough risk assessment.

Security Plans

Requirement:

FISMA requires that agencies develop security plans for each system in their inventories. A system security plan should be based on the agency-wide plan, provide an overview of the system's specific security requirements, and describe the controls in place or planned for meeting those requirements. A system security plan should delineate the responsibilities, expected behavior, and training requirements for all individuals who access the system and describe appropriate controls for interconnection with other systems.

Progress to Date:

The Board's information security program requires the system owner to develop a security plan based on the complete set of controls required for the system (the baseline controls and any additional controls identified during the risk assessment process). To assist system owners, the ISO has developed security plan templates for major applications, general support systems, and standalone minor applications. An official System Security Plan Approval form is included in the security plan and, by signing it, the system owner is stating that the owner has reviewed the security plan and that the owner believes the security plan accurately and completely describes the security of the system. Approval of a security plan signifies approval of all documents referenced by the security plan and the baseline of security controls. A bundled subsystem security plan requires system owners to attest that all security controls provided by the baseline of controls have been reviewed to determine that the subsystem relies upon the provided GSS or major application security controls, and that the controls satisfy all subsystem control requirements with the exception of any other specific controls documented.

In our 2009 FISMA report, we found security plans that had not been updated and that referenced obsolete software versions and outdated security settings. As a result, we recommended that the CIO ensure all systems have updated security plans that include all requirements, as part of implementing the new risk assessment process. This past year the ISO implemented C&A planning checklists. The checklists outline the review process for system owners preparing for either a recertification or an annual assessment, and include a checklist for new major and minor applications, existing major and minor applications, and IT GSS subsystems. The checklists require the system owner to indicate that he/she has reviewed and updated the System Security Plan and submitted it to the certifying agent. Our control reviews this year did not identify obsolete software or outdated security settings. We also reviewed a sample of security plans and found each of the system owners had developed security plans, and the subsystems that had been bundled into a GSS had a bundled subsystem security plan completed. As a result, we are closing our recommendation.

Work To Be Done:

All Board information systems must be supported by a system security plan categorized as a major application, a minor application, or a general support system. The information system owner is responsible for the development and maintenance of a system security plan. Security plans must be reviewed annually. The Board's information security program requires that security plans include system environment descriptions and diagrams of the system environment. As the Board continues to mature its risk assessment processes, improvement opportunities exist to provide additional relevant details within the security plans, such as additional detailed information regarding system descriptions and diagrams, as well as technical details on servers that could affect a specific application. This enhancement would allow system owners to more fully understand the risks and mitigating factors, and assist in selecting a sample of controls for periodic testing and evaluation.

Matter for Management's Consideration: Include additional relevant details within system security plans, such as detailed information regarding system descriptions and diagrams, as well as technical details on servers that could affect a specific application.

<u>Periodic Testing and Evaluation</u>

Requirement:

FISMA requires periodic testing and evaluation of the effectiveness of an agency's information security policies, procedures, and practices. Testing of the management, operational, and technical controls for each system identified in the agency's inventory should be performed on a risk-based frequency, but not less than annually. As stated earlier, each system must also undergo a periodic C&A to ensure that security controls are commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information contained in the system. The Board's information security program requires the C&A of a system to include a security assessment. The security assessment is to be performed by an independent certification agent and provide assurance that controls are implemented correctly, working as intended, and producing the desired results. A C&A should be completed before a system is initially placed into operation and every three years thereafter or if the system undergoes a significant change.

Progress to Date:

The ISO continues to conduct security assessments on a three-year cycle, with all systems undergoing annual testing. Starting in 2009, testing has moved away from an every three-year C&A towards a more continuous monitoring approach. Each year, one-third of the total controls for major applications will be tested, although certain critical controls will still be tested every year. For the GSS, one-third of the individual components will be tested every year.

SP 800-53 recommends that those security controls that are volatile or critical to protecting the information system be assessed at least annually. In our 2009 FISMA report, we identified that the Board's process of testing one-third of the IT GSS components each year limits the controls tested each year, and some controls are so important to the Board's information security that they may need to be reviewed annually. We recommended that the CIO test select critical controls within the IT GSS annually. The ISO now includes a subset of controls related to access and identification, configuration management, and contingency for major IT GSS platforms on a quarterly basis. As a result, we are closing our 2009 recommendation on testing select critical controls of the IT GSS annually.

Work To Be Done:

NIST and OMB have placed a focus on agencies developing abilities to continuously monitor security controls. However, continuous monitoring does not replace security certifications, and not all controls are well suited to continuous monitoring or automation, so other testing methods are required. OMB states that agencies should develop an enterprise-wide strategy for selecting subsets of their security controls to be monitored on an ongoing basis to ensure all controls are assessed during the three-year authorization cycle. The ISO process for assessments for major applications currently includes annually reviewing one-third of the system level management, operational, and technical controls as documented in the system security plans and control baselines, although certain critical controls will still be tested every year. Evaluations of the common controls provided by the GSS on which the systems rely are conducted separately.

As previously stated, NIST has recently revised its guidance to support organizations in assessing the effectiveness of the security controls that are implemented in federal information systems. The selection and assessment of appropriate security controls are important steps in the comprehensive process of managing risks and maintaining effective security of those information systems. SP 800-53, Revision 3, identifies related security controls across families, and the ISO has tried to assure concurrent testing for those related controls that are synergistically related in their operation. Concurrent testing of related controls, in addition to the testing schema of testing one-third of the controls each year, can work to close any gaps in assessing risk between related controls. A risk-based approach to testing IT GSS components would enhance control testing of the IT GSS components. Currently the ISO tests a random sample of components, but we found during one of our security control reviews that the IT GSS components supporting a critical application were not selected through the random sampling approach.

The ISO has stated that in 2011, security assessments will be moving to more control-focused testing where they will focus on testing controls across all platforms on a frequency that will vary based on control nature and importance. For instance, some controls may be looked at monthly, some quarterly, some yearly, some every 3 years, etc. How the ISO plans to evaluate the effectiveness of the controls and select the subsets of security controls to be continuously monitored should be part of (1) the Board-wide IT risk management strategy identified in Recommendation 1 of this report and (2) a continuous monitoring strategy.

Matter for Management's Consideration: Implement risk-based sampling as part of the security control assessment testing.

Continuous Monitoring Program

Requirement:

One of the recent changes in SP 800-53, Revision 3, requires agencies to establish a continuous monitoring strategy and implement a continuous monitoring program. 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 consistent with NIST and OMB FISMA related requirements. Organizations are required to develop a continuous monitoring program for their information systems and environments in which those systems operate. Continuous monitoring of security controls is required as part of the security authorization process to ensure controls remain effective over time (after the initial security authorization or reauthorization of an information system) in the face of changing threats, missions, environments of operation, and technologies.

Progress to Date:

OMB states that agencies need to be able to continuously monitor security-related information from across the enterprise in a manageable and actionable way. CIOs, ISOs, and other agency managers all need to have different levels of this information presented to them in ways that enable timely decision-making. To do this, agencies need to automate security-related activities, to the extent possible, and acquire tools that correlate and analyze security-related information. Agencies need to develop automated risk models and apply them to the vulnerabilities and threats identified by security management tools. Previously, the Board's ISO has tested a subset of controls through annual security reviews primarily using manual techniques, and has expanded this approach through having one-third of the total controls of major applications tested each year. In addition, the ISO has started to develop quarterly information security metrics for senior management. The metrics track both (1) security related metrics, such as incidents reported, and (2) compliance metrics, such as security assessments completed and POA&M statistics.

In addition, 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 is utilizing these tools and processes to meet NIST and OMB requirements for continuous monitoring.

Work To Be Done:

OMB guidance places a focus on continuous monitoring, and as stated above, SP 800-53, Revision 3, requires agencies to establish a continuous monitoring strategy and implement a continuous monitoring program, in the Security Assessment and Authorization (CA) family of controls. Although continuous monitoring of controls has always been required, NIST continues to develop guidance for continuous monitoring. For example, SP 800-137, which will provide a guide for agencies to develop a continuous monitoring program is scheduled to be issued in 2011.

Continuous monitoring of security controls using automated tools facilitates near real-time risk management. Our security control reviews have identified that the CIO continues to acquire tools that correlate and analyze security-related information. We will continue to review the Board's capabilities as part of our ongoing FISMA-related audits. As additional NIST guidance is issued and becomes effective, a documented continuous monitoring strategy is needed to analyze how the ISO's automated monitoring tools and processes, which are used in day-to-day operations, supplement the ISO's annual control testing. Documenting how the ISO plans to monitor risk through these tools on an ongoing basis should be part of the continuous monitoring strategy and complement the Board-wide IT risk management strategy identified in Recommendation 1 of this report.

Continuous monitoring, in and of itself, does not replace security control assessments. A robust and effective continuous monitoring program will ensure important procedures included in an agency's security authorization package (as described in system security plans, security assessment reports, and POA&Ms) are updated as appropriate and contain the necessary information for authorizing officials to make credible risk-based decisions regarding the security state of the information system on an ongoing basis.

Recommendation 2: We recommend 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.

Plan of Action & Milestones Program

Requirement:

FISMA requires agencies to establish a process for addressing any deficiencies in information security policies, procedures, and practices. To implement this requirement, OMB has issued guidance requiring agencies to prepare and submit POA&Ms for all programs and systems where an information technology security weakness has been found. The guidance 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 POA&M is a tool to communicate to management the proposed and actual implementation of risk management plans. As reported in our 2009 FISMA report, an agency-wide POA&M process has been in place for many years at the Board. The ISO continues to collect POA&Ms on a quarterly basis from Board divisions and offices that reflect identified information technology security weaknesses or exposures. Also, as outlined in our 2009 FISMA report, the ISO issued POA&M guidance for the Board which states, "The Board ISO reviews the Division POA&M for completeness and to determine if any issues identified at the Division level warrant escalation to the agency level POA&M. In addition, the ISO tests closed issues to certify they have been properly mitigated."

Work To Be Done:

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. Even though Board divisions and offices have been reporting information technology security weaknesses, we included a recommendation for improvement actions in our 2009 FISMA report because our security control reviews continue to identify instances where POA&M items that were designated as completed and removed from POA&Ms were only partially or not effectively remediated. This translates into extended security exposures for Board systems.

In response to our recommendation, the ISO has established new POA&M procedures. A member of the ISO's staff validates the remediation of action items during a system controls review or otherwise requests documentation to determine if the control related to the POA&M corrective action has been sufficiently completed. Items with insufficient evidence or those that have been delayed will be evaluated as to why the action(s) have not been completed and revised accordingly with an updated completion date. However, at the time of our review, the new process had been implemented for only one division (this division has the largest number of POA&M items). The ISO plans to implement the independent verification of completed POA&M items for all Board divisions during the 2011 program year. We will keep our recommendation open and continue to monitor the ISO's corrective actions on POA&Ms.

Account and Identity Management Program

Requirement:

FISMA requires that the agency has established and is maintaining an account and identity management program that is generally consistent with NIST and OMB FISMA requirements. 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.

Progress to Date:

We found that the ISO has established and is maintaining an account and identity management program that is generally consistent with NIST's and OMB's FISMA requirements. The Board's information security program includes documented policies and procedures to ensure that the users are granted access based on needs and separation of duties principles. Procedures also ensure accounts are properly issued to new users and are properly terminated when users no longer require access. The Board's account and identity management program, which is linked to the Board's personnel system, ensures that accounts are terminated or deactivated once access is no longer required.

We also found that administrator privileges were appropriately limited. Privileges granted do not result in the capability to perform conflicting functions. The Board utilizes dual accounts for administrators and does not allow shared administrator accounts to ensure the proper tracking of administrator actions.

Work To Be Done:

The ISO has established documented policies and procedures for account and identity management; however, we noted that localized change-control processes rely primarily on IT Division-wide policies and procedures which do not accurately reflect the tasks performed at the local level. Local change-control processes and procedures utilized for Active Directory updates were not documented in the IT Division's policies and procedures, and documentation of the local procedures do not reflect the actual work processes. The ISO should consider clarifying the existing account management procedures to accurately reflect all processes currently implemented.

OMB reporting requirements also inquire whether agencies can identify network devices, and utilize multi-factor authentication. We found that the Board utilizes multi-factor authentication for remote access devices and identification of remote users. However, the Board does not currently identify or authenticate devices that are attached to the network or have the capability to distinguish these devices from users. Devices that join the network cannot currently be identified or authenticated, although users' access is controlled. We determined that compensating controls are in place, and several initiatives are currently underway, at the local and the Federal Reserve System (System) level, to identify devices.

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 2010 FISMA work in analyzing the Board's remote access program, we reviewed the System's National Remote Access Services (NRAS) infrastructure. NRAS delivers enterprise-level mobile and remote-access services to the Board and Reserve Banks. Our review found that while NRAS is not covered under the Board's information security program, there are documented policies and procedures for authorizing, monitoring, and controlling methods of remote access. NRAS protects against unauthorized connections, encrypts files on transmission, and uniquely identifies users.

Work To Be Done:

Our review of the security controls for NRAS identified various improvement opportunities that we will report under a separate, restricted report to the Board's CIO. 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. As described in our 2009 FISMA report, 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 Program

Requirement:

FISMA requires that the agency has established and is maintaining a security configuration management program that is generally consistent with NIST and OMB FISMA requirements. Configuration management comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.

A key to ensuring the confidentiality, integrity, and availability of any information system is implementing structured processes for managing the inevitable changes that will occur during the system's life cycle. Such processes, collectively referred to as configuration management, include evaluating, authorizing, testing, tracking, reporting, and verifying both hardware and software changes. Inadequate configuration management controls increase the risk that unauthorized programs or untested changes could inadvertently or deliberately be implemented and negatively affect system performance or security.

Progress to Date:

The Board has established and is maintaining a security configuration management program that is generally consistent with NIST and OMB FISMA requirements. The ISO has documented policies and procedures, and standard baseline configurations for IT GSS components that have been developed and continue to be updated in operating environment documents. The operating environment documents provide details on various monitoring tools the ISO has implemented to monitor and deploy changes to configurations, including Federal Desktop Core Configuration settings. The ISO employs automated tools to apply patches and security related updates to desktop workstations, and a change control system to document changes to configuration settings. Many of these tools are used by IT support staff in their day-to-day operations. These tools could be further utilized to reduce the reliance on the current manual testing of controls, under the continuous monitoring strategy discussed in Recommendation 2 of this report.

Work To Be Done:

The management of security configurations of infrastructure components is challenging in terms of both complexity and frequency. The continual changes to security settings are essential based on changing security threats and vulnerability. The Board's infrastructure includes internal servers and applications that also face externally outside (the internet) the Board's firewall. These components require specific configuration settings based on external threats and potential vulnerabilities. For some systems that contained both internally and externally facing components, we found the Board utilizes one set of baseline of controls, operating environment documents, and procedures for day-to-day operations of the servers and applications. However, having the same documentation may not be sufficient to distinguish between the internally and externally facing environments, and more comprehensive documentation may be necessary for externally facing servers and applications. The CIO may want to consider separately accrediting the externally facing components of the IT GSS and major applications.

In addition, the Board's information security program includes a configuration management policy that requires configuration baselines to be developed for and applied to each type of infrastructure component. However, our security control review found that the information security program does not provide detailed procedures for establishing and managing application security settings. Although the ISO requires a software security review for all commercial off-the-shelf products, we found a software component for a major application that requires configuration settings, but which was not documented as part of the major application's security plan. Clarifying guidance would further assist system owners in managing application level security settings across Board applications. We will report on this specific issue in our security control review report.

Matters for Management's Consideration: Separately accredit the externally facing components of the IT GSS and major applications, and clarify guidance to assist system owners in managing application level security settings.

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 improve upon its interactive computer-based security awareness training that complies with NIST and OMB FISMA requirements. All Board employees, contractors, and interns are required to complete an annual security awareness quiz that includes topics such as incident handling, data breach notification, information classification and handling, permissible use and privacy policy, handling personally identifiable information, and phishing-fraudulent e-mails. The ISO also continues to provide additional computer-based training modules on topics such as mobile storage devices and international travel, and the Board's overall information security program. The ISO has also provided a module for new Board employees.

Board divisions report training for personnel with significant information system security responsibilities to the ISO. In addition, the Information Security Compliance unit continues to offer several versions of in-house FISMA training to Board personnel. The training modules cover both FISMA compliance requirements and Board-specific requirements for system documentation, procedures, and implementation of security controls. The ISO also plans on meeting with individual system owners to discuss their FISMA responsibilities.

Work To Be Done:

The Board continues to make improvements in the quality, tracking, and monitoring of its security awareness training program. The 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. As stated above, the Information Security Compliance unit offers several versions of in-house training to Board personnel; however, this FISMA training continues to be optional and not mandatory for personnel with significant information system security responsibilities. In performing our 2010 FISMA fieldwork and our analysis of FISMA training, we 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. As stated in our 2009 FISMA report, our security control reviews continue to identify deficiencies that we feel may have been avoided if FISMA training on NIST standards and guidelines and Board security policies, procedures, and practices was mandatory.

Our 2010 security control reviews continue to indicate that FISMA training for Board information system personnel could be beneficial in securing the Board's information systems by instructing information system personnel on how to implement controls and meet NIST requirements. Going forward, as the ISO transitions to more continuous monitoring of controls, training will be necessary to ensure that personnel responsible for day-to-day operations are fully aware of their FISMA responsibilities. We believe that the training should have a focus on areas of non-compliance or technical deficiencies that have been identified not only by the OIG control reviews, but also by the ISO's staff who perform control reviews of the Board's information systems. We will continue to keep this recommendation open as we monitor the ISO's actions to improve staff's knowledge of and training in FISMA.

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. OMB requires that the agency develop policies and maintain a program to oversee systems operated on its behalf by contractors or other entities.

Progress to Date:

The Board's third party applications are primarily located within the Federal Reserve Banks. Although the System maintains its own information security program, systems that process and store Board information are required to be certified and accredited in accordance with the Board's information security program. The ISO has established and maintains a program to obtain assurance that security controls of selected systems operated by Federal Reserve Banks are effectively implemented and comply with the Board's information security program. The program, which is updated annually, includes policies and procedures and an inventory of systems that identifies interfaces.

The ISO coordinates with the Board's Division of Banking Supervision and Regulation's Information Security and Continuity Management Section (ISCM), which serves as the focal point for FISMA compliance of the Reserve Banks' FISMA assets. The ISCM provides annual training on the Board's information security program to Reserve Bank staff with FISMA- related responsibilities.

The ISO has overall responsibility to ensure contractor systems comply with the Board's information security program and conducts security assessments of systems within the Reserve Banks that store or process Board data. In addition, the ISCM conducts their own review of the Reserve Banks, in addition to the certification assessments conducted by the ISO. The reviews focus on continuous monitoring activities and a review of security controls from the security baselines, as well as common controls, such as personnel security, which are outside of the system baseline but require verification to ensure these common controls are supported by other organizations at a Reserve Bank or other support organizations within the Federal Reserve System.

Work To Be Done:

As discussed earlier, the System has established plans to implement an enterprise information security program based on the NIST framework. The Reserve Banks plan to transition through a multi-year approach and have started to train their staffs on the new NIST compliant security program. As part of our ongoing work related to information security, 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.

As previously stated, NRAS was identified as a contracted service that is essential to the Board's operations, but it is not listed on the Board's FISMA inventory. As part of our security control review of the Board's PubWeb application, we identified another contractor service that, although essential to the Board's recruitment process, was not included on the Board's FISMA inventory. Since this system stores Board data, the ISO should determine that security controls are in place. The ISO has stated the application will be added to the Board's FISMA inventory, and that he is working with the division to determine the appropriate security requirements. We believe that the CIO needs to identify all information technology services provided by entities other than Board personnel, and determine whether each needs to be accredited as a third party contractor system or as part of any existing GSS or major application.

Recommendation 3: We recommend 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 GSS or major application.

Contingency Planning Program

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. Our analysis of the Board's information security program included reviewing how the Board has established and is maintaining an entity-wide business continuity/disaster recovery program that is consistent with NIST's and OMB's FISMA requirements.

Progress to Date:

The Board has established and is maintaining an agency-wide business continuity/disaster recovery program that is consistent with NIST and OMB requirements. During the past year, the Board continued to conduct semiannual contingency tests. Divisions participate in the tests, and the ISO uses the Board's FISMA inventory to track the systems participating in the testing. The IT Division's Strategic Plan for 2007-2010 outlined a number of contingency objectives, one of which was bringing mainframe backup capabilities in-house, which was accomplished. Also the Board continued to update operations and preparations to address various aspects of contingency/continuity. This includes enhancing tracking of any issues identified during the contingency exercises, providing videoconferencing capabilities, and updates to contingency logistical guidance in terms of contingency teams and accommodations.

Work To Be Done:

During the Board's semiannual contingency tests, the IT division provides the infrastructure services for system owners to test applications for their availability. As the ISO develops a Board-wide IT risk management strategy identified in Recommendation 1 of this report, the ISO will need to consider the continuity and disaster recovery of critical systems to ensure the strategy is both broad-based and comprehensive.

We indicated in our 2009 FISMA Report that we will continue to monitor the Board's contingency processes and procedures as part of our ongoing FISMA work. We participated in the March 2010 contingency test as observers and noted high level strategic as well as technical/operational matters that require further detailed analysis to address potential gaps that could hamper a smooth and efficient recovery of operations in the event of a contingency. During our 2011 FISMA cycle, we are planning to perform an audit of the overall Board contingency framework in order to provide input for improvements or enhancements to the Board's preparedness for contingency/continuity.

Incident Response & Reporting Program

Requirement:

FISMA requires agencies to develop procedures for detecting, reporting, and responding to security incidents. The procedures should include steps to mitigate risks from security incidents before substantial damage is done and to notify and consult with the United States Computer Emergency Readiness Team (US-CERT), appropriate law enforcement agencies, and relevant IGs. US-CERT has established requirements for incident reporting, which include establishing priority levels for categories of incidents and timeframes for reporting each priority level.

Progress to Date:

To assist Board staff in understanding their responsibilities related to security incidents, the ISO has developed policy and procedures to inform employees of their responsibilities for reporting incidents. When applicable, the CIO reports to the US-CERT and law enforcement within established timeframes. In the past, the ISO has responded to and resolved incidents in a timely manner to minimize further damage.

The ISO has started to develop quarterly information on security incidents for senior management. The quarterly reports also included detail on incidents from across the Reserve Banks for any BS&R delegated functions.

Work To Be Done:

To reinforce employees' responsibilities, the ISO continues to post articles on this topic on the Board's website as part of security awareness training. We will continue, as part of our ongoing FISMA-related audit work, to monitor how the Board handles information security incidents to ensure that incidents at the Board and the Reserve Banks continue to be reported to US-CERT pursuant to the relevant requirements.

APPENDIX 2

Division Director's Comments

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

November 15, 2010

Ms. Elizabeth A Coleman, Inspector General
Office of the Inspector General
Board of Governors of the Federal Reserve System
Washington, D.C. 20551

Dear Ms. Coleman:

Thank you for the opportunity to comment on the Office of Inspector General's 2010 review of the Board's information security program. We are pleased that your assessment continues to recognize that the Board operates a comprehensive and effective information security program and recognizes the progress we continue to make to enhance the program.

We generally agree with the three recommendations offered in your report. We intend to take immediate action to address each of these recommendations. This includes updating our program documentation to more accurately reflect the risk management and continuous monitoring programs. In addition, we will be reviewing the system inventory with each division and office to validate that all contractor services are correctly reflected in the inventory. We also plan to leverage the results from continuous monitoring program to offset compliance testing requirements during 2011.

The Information Technology Division's Plan of Actions and Milestones will be updated to reflect this corrective action. We look forward to continuing to work with your office.

Sincerely,

/signed/

Maureen Hannan
Director, Division of Information Technology

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

Principal Contributors to the Report

Robert McMillon, Auditor-in-Charge

Richard Allen, Senior IT Auditor

Satynarayana-Setty Sriram, IT Auditor

Robert Delgesso, IT Auditor

Peter Sheridan, OIG Manager

Andrew Patchan, Jr., Associate Inspector General for Audits