

**Board of Governors of the Federal Reserve System**

**AUDIT OF THE BOARD'S  
INFORMATION SECURITY PROGRAM**



---

**OFFICE OF INSPECTOR GENERAL**

---

November 2009





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

OFFICE OF INSPECTOR GENERAL

November 17, 2009

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

Dear Members of the Board:

The Office of Inspector General 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 (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. As part of our review, 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 April 2009 through October 2009, and 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.

Overall, we found that the Board's Information Security Officer (ISO) continues to maintain a FISMA-compliant approach to the Board's information security program. The Board's inventory has remained stable from 2008. Based on our prior recommendations, the ISO has allocated additional resources to the Division of Information Technology's (IT's) Security Compliance unit and implemented an improved approach to security assessments that includes independent testing. In addition, the ISO continues to issue and update information security policies and guidelines, and has started to develop security metrics to measure security performance and compliance. The Board continues to emphasize information security awareness by offering additional automated presentations that highlight potential vulnerabilities, and posting awareness reminders throughout Board buildings.

During this year's FISMA review, we followed up on the status of corrective actions in response to open recommendations from our prior FISMA reports and security control reviews. As discussed in appendix 1, we determined that the Board's corrective actions are sufficient to close out two of three open recommendations from our prior FISMA reports. The third

recommendation was to ensure that risk assessments adequately identify, evaluate, and document the risks to an information system based on potential threats, vulnerabilities, and controls. The ISO has developed a Supplemental Controls Questionnaire to assist system owners in determining whether additional controls are needed. However, our detailed review of selected risk assessments showed that system owners can improve in identifying, evaluating, and documenting potential system vulnerabilities, the associated level of risk, and the need for additional controls to address these risks. The ISO has plans to further enhance the risk assessment process, and we will keep this recommendation open as we monitor the implementation of these enhancements. In following up on the Board's actions in response to our prior security control reviews, we determined that sufficient actions have been taken to close fifty-seven of sixty-one open recommendations. We will continue to monitor the Board's actions on the remaining open recommendations.

To further enhance the Board's information security program, this report includes the following four recommendations to the Chief Information Officer (CIO): (1) ensure all systems have updated security plans; (2) test select critical controls within the IT general support system (GSS) annually; (3) independently verify that appropriate corrective action has been implemented before items are removed from the Board's Plan of Action and Milestones (POA&M); and (4) provide mandatory FISMA training to selected staff with FISMA responsibilities. Appendix 1 contains our analysis of the Board's progress in implementing key FISMA requirements and discusses each of these recommendations in more detail.

As stated previously, we review security controls implemented for Board applications on an ongoing basis. During the past year, we reviewed security controls for three systems: (1) the Board's Electronic Security System; (2) the Board's Lotus Notes and Lotus Domino infrastructure, which is a component of the Board's GSS supported by IT; and (3) a third-party application operated by the Federal Reserve Bank of New York in support of the Board's Division of Monetary Affairs. We also conducted reviews of audit logging controls provided for a number of Board systems and by the IT GSS, and the Board's POA&M program and processes. We reviewed components of the Board's certification and accreditation (C&A) process, including risk assessments, security plans, and security assessments. Our reviews of Board applications' information security controls identified areas where controls need to be strengthened but, given the sensitivity of the issues involved with these reviews, we are providing the specific results to management in separate restricted reports. We performed our application control testing based on selected controls identified in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems* (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.

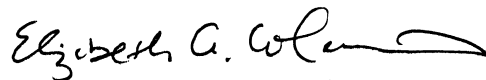
As part of agencies' annual FISMA reporting, the Office of Management and Budget (OMB) requested that both the CIO and the IG provide responses to certain security-related questions. To address OMB's security-related questions, our FISMA review included an analysis of the Board's security-related processes for security awareness and training, system

inventory, remedial action monitoring, incident reporting, configuration management, controls over personally identifiable information (PII), and privacy impact assessments (PIA).<sup>1</sup> In addition to this report, we will respond to OMB's questions under separate cover via automated submission (our response will be submitted with the CIO's response to the OMB questions).

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 agreed with recommendations 2 and 3, and generally agreed with recommendations 1 and 4. The director stated that additional program enhancements are planned for the next two years that will address most of the key improvement opportunities highlighted in our report. We will follow up on actions taken regarding our recommendations as part of future audit and evaluation work related to information security.

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 the Congress. Please contact me if you would like to discuss the audit report or any related issues.

Sincerely,



Elizabeth A. Coleman  
Inspector General

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

---

<sup>1</sup> Our answers to the OMB questions regarding controls over PII and PIA are not included in this report, since they are not requirements of FISMA. However, PII and PIA are addressed in our response to OMB.



## **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 four recommendations, contained on pages 12, 14, 15, and 17.

### **Policies and Procedures**

#### **Requirement:**

Information security policy is an essential component of an information security program. An agency's information security policies should be based on a combination of relevant legislation, such as FISMA; applicable standards, such as NIST Federal Information Processing Standards and guidance; and internal agency requirements. Supporting guidance and procedures on how to implement specific controls effectively across the enterprise should be developed to augment an agency's security policy. To ensure that information security policies do not become obsolete, agencies should implement a review and revision process for their policies and procedures.

#### **Progress to Date:**

The ISO and his staff continue to issue new and updated information security guidance and procedures. During this past year, the ISO updated the Board's information classification and handling guide and issued policy on international travel with mobile devices and media disposal and sanitation. To assist system owners with their annual system reviews, the ISO developed FISMA process review checklists that identify the key courses of action necessary to complete the applicable review. Checklist selections are applied based on whether the system is major or minor; the system is a GSS subsystem; or a full C&A is to be performed for the system. Each checklist walks the system reviewer through the control baseline, system security plan, and risk assessment processes.

In addition, guidance to determine the minimum audit logging requirements for a Board system was issued in early 2009. The guidance contains attachments that address data access log requirements, infrastructure log review risk analysis, and application log review risk analysis. The ISO also updated the Board's access control and authentication standard to address revised password policy.

#### **Work To Be Done:**

Agencies have a continual need to update and refine their information security program and related policies and procedures as the program evolves and as NIST and OMB issue new guidance. In August 2009, NIST issued an updated version of SP 800-53, which contains new requirements to be implemented, and has issued a draft of SP 800-37, *Guide for Security Authorization of Federal*

*Information Systems: A Security Lifecycle Approach*, which, when issued, will also establish new requirements.

The ISO has responded appropriately in the past to OMB and NIST changes to FISMA requirements, as well as OIG audit analysis and findings, and has formed work groups that include officers and managers from IT who represent infrastructure and application development to assist with the review and revision of IT security policies to incorporate new guidance. We will continue to review the need for additional guidance as part of our ongoing work related to information security.

### **Application Inventory**

#### **Requirement:**

FISMA requires the head of each agency to develop and maintain an inventory of major information systems operated by or under the control of the agency. The inventory forms the basis for meeting the FISMA periodic testing requirement. The inventory should also identify system criticality and risk levels. OMB's annual FISMA reporting questions require agency IGs to determine if the inventory of major systems is materially correct; the IG agrees with the total number of reported systems, including those operated on behalf of the agency; and the inventory is updated annually.

#### **Progress to Date:**

The Board's FISMA inventory has remained stable over the past year. The ISO has reported that all major applications and GSSs have been certified and accredited, including those operated on behalf of the agency. The Board continues to refine how it accounts for the C&A of minor applications and subsystems. During the past year, the Board has continued to focus on refining the bundling of minor applications and subsystems into the security plans of a GSS, a major application that provides a significant portion of its security control requirements, or other minor applications to form a single major application. In addition, the ISO has continued to provide training to system owners who make the final determination of whether their minor application will be bundled or stand alone.

#### **Work To Be Done:**

The Board's third party applications are primarily located within the Federal Reserve Banks. Although the Federal Reserve System (System) maintains its own information security program, systems that process and store Board information are to be certified and accredited in accordance with the Board's information security program. Our security control reviews identified control weaknesses related to systems operating within infrastructures that were not certified and accredited in accordance with the Board's information security program. However, during the past year the Reserve Banks established plans to

implement an enterprise information security program based on the NIST framework. The Reserve Banks plan to transition over a four-year period and have started to train their staffs on the new NIST compliant security program. In addition, the ISO has coordinated through the Division of Banking Supervision and Regulation (BS&R) to ensure BS&R applications maintained within the Reserve Banks that process and store Board information complied with the Board's information security program. During the past year, the ISO and BS&R conducted a review of controls provided by the System's Groupware Leadership Center (GLC). The GLC is one of the Federal Reserve System's National Information Technology Operator competency centers responsible for the planning, implementation, and functional enhancement of the System's electronic mail and collaborative computing services.

Our 2005 FISMA audit report contained a recommendation that the Board establish full-time, independent CIO and ISO positions that have the authority to direct and enforce FISMA compliance for all information and information systems that support Board operations and assets, including those provided by the Reserve Banks and other third parties. Based on the Board's progress in designating the CIO and ISO positions for FISMA, and the CIO's and ISO's actions in ensuring FISMA compliance of systems throughout the Board and applicable Reserve Bank systems, we are closing this recommendation. 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.

### **Periodic Risk Assessments**

#### **Requirement:**

FISMA requires periodic assessments of the risk and 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. OMB's annual FISMA reporting questions take risk assessments into consideration as part of the overall qualitative assessment of the C&A process and direct agencies to follow applicable NIST guidance.

#### **Progress to Date:**

As part of the Board's information security program, the ISO has developed a Risk Assessment Template and a Risk Assessment Guide intended 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 of his/her systems, regardless of whether each is categorized as a GSS, a major application, a standalone minor application, or a subsystem to any of these

categories. During this past year, the ISO developed a Supplemental Controls Questionnaire to assist system owners in determining which NIST SP 800-53 controls that are listed as optional or intended for systems that are risk classified as high may be used to mitigate a unique system risk or satisfy a unique system requirement.

The Risk Assessment Guide assists an information system owner in determining what additional controls need to be implemented to decrease the information system's exposure to risk and in setting priorities for implementing the necessary additional new controls. The system owner documents the risk assessment that is performed using the Risk Assessment Template, which serves as a report of the results of the risk assessment for the information system. The template covers a number of areas, such as determining a security impact level, identifying the system technical components and users, listing known vulnerabilities, identifying controls that can minimize the vulnerabilities, and identifying any residual risk that is remaining after the controls are implemented. Finally, for risks that the system owner has decided to accept, the template is used to document the decision and its justification.

**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. While system owners were documenting that their systems met minimum controls, the security control baselines did not address what additional controls may be needed to protect against potential threats. As a result, the ISO agreed to work closely with system owners to ensure risk assessments effectively identify and more fully address additional risks.

Although the ISO developed a Supplemental Controls Questionnaire to assist system owners in determining whether additional controls are needed, we continue to find that system owners can improve their identification, evaluation, and documentation of the level of risk to information systems based on potential threats, vulnerabilities, and currently implemented or planned controls. Going forward, the ISO plans to utilize relevant NIST publications, such as SP 800-30, *Risk Management Guide for Information Technology Systems*, and SP 800-39, *Managing Risks from Information Systems: An Organizational Perspective*, once they are issued by NIST, to update the Board's risk assessment process. In addition, the ISO is reviewing automated tools to provide a structured approach and a more thorough risk assessment. We will keep the above mentioned recommendation open as we continue to monitor the CIO's and ISO's actions in overseeing the planned enhancements to the risk assessment process.

## **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. OMB's annual FISMA reporting questions include security plans as part of the overall qualitative assessment of the C&A process and direct agencies to follow applicable NIST guidance.

### **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 (i.e., 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.

We reviewed security plans as part of our three control reviews, and as part of our review of the Board's C&A process we reviewed security plans for two GSSs that had bundled subsystems and four major applications. We found each of the system owners of the major applications had developed security plans, and the subsystems that had been bundled into a GSS had a bundled subsystem security plan completed.

### **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. However, we found security plans that had not been updated and that referenced obsolete software versions and outdated security settings.

The Board's information security program requires security plans to include system environment descriptions and diagrams of the system environment. However, our review of security plans found only limited descriptions and diagrams. In our 2008 FISMA audit report, we identified opportunities for the ISO to enhance security plans by including technical details for the servers that could affect a specific application. This enhancement would allow system owners to understand the risks and mitigating factors of certain design architectures and identify the software packages installed on the servers supporting their applications.

Full implementation of the security planning process will not occur until all plans provide an overview of the systems' specific security requirements and describe the controls in place or planned for meeting those requirements. The certification process includes having an independent certification agent review the security plan and test existing controls to ensure the controls provide the required level of security. If the control baseline and risk assessment are inadequate or outdated, the security plan will not fully describe the system's security environment or identify other needed controls. Controls missed in the baseline flow through the risk assessment and into the security plan.

**Recommendation 1:** We recommend that the CIO ensure all systems have updated security plans that include all requirements, as part of implementing the new risk assessment process.

### **Periodic Testing and Evaluation**

#### **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. 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. 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. OMB's annual FISMA reporting questions require the agency IG to provide a qualitative assessment of the agency's C&A process, including adherence to existing policy guidance and standards.

#### **Progress to Date:**

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.

Consistent with our 2008 FISMA audit, all Board systems and GSSs have undergone the Board's C&A process. The ISO continues to conduct security assessments on a three-year cycle, with all systems having annual testing.

In our 2008 FISMA audit report, we recommended that the CIO ensure that security assessments include necessary and sufficient independent testing to support the authorization to operate and provide the authorizing official and the Board assurance that information security controls for these systems are implemented correctly, working as intended, and producing the desired results. During the past year, the CIO allocated additional resources to increase staff in the IT Security Compliance unit that is responsible for independently conducting security assessments and developed a new testing approach for the 2009 review cycle. The security assessment test steps are based on the controls included in NIST SP 800-53, and each security control includes a corresponding testing approach from NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*. The ISO has also redesigned the certification assessment report to provide system owners more detailed information about the assessment process and control deficiencies.

As part of our review of the Board's C&A process, we reviewed the security assessments for two major applications that had all controls reviewed, one major application that had a subset of controls reviewed, two GSSs that each had a subset of controls reviewed, plus a component of the IT GSS that had all controls reviewed. Our review found that the ISO has made progress to ensure security assessments include independent testing. The security assessments we reviewed independently validated controls related to access control and configuration management to ensure the control has been implemented correctly, working as intended, and producing the desired results. As such, we believe sufficient corrective actions have been taken to close our 2008 recommendation.

**Work To Be Done:**

Under the Board's current approach, an assessment conducted for a C&A will include all controls being tested, and then a subset of controls will be tested during the intervening years. Testing plans have been tailored for GSSs, major applications, bundled systems, and non-bundled systems. The IT GSS is composed of eighteen components; each year one-third of the components will have all controls reviewed.

Assessments for major applications include reviewing system level management, operational, and technical controls as documented in the system security plans and control baselines. Evaluations of the common controls provided by the GSS on which the systems rely are conducted separately. This may lead to security gaps when a control is identified as missing or deficient during an assessment of the GSS but not communicated to the system owner who is relying on the control being provided by the GSS. In addition, upgrades to GSS components may affect

the security of the systems that rely on the GSS. These factors should be considered as the Board continues to implement its revised testing process.

In addition, the Board's process of testing one-third of the IT GSS components each year limits the controls tested each year. Although we understand the complexity of reviewing the IT GSS, some controls are so important to the Board's information security that they may need to be reviewed annually. NIST SP 800-53 recommends that those security controls that are volatile or critical to protecting the information system be assessed at least annually. When reviewing a subset of controls for a major application, Board officials stated that some vital controls will be tested annually. We believe the CIO should consider reviewing certain controls within the IT GSS annually. This would also eliminate any security gaps from reviewing controls over a three-year period.

**Recommendation 2:** We recommend that the CIO test select critical controls within the IT GSS annually.

### **Planning, Implementing, Evaluating, and Documenting Remedial Actions**

#### **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. OMB's annual FISMA reporting questions inquire whether an agencywide POA&M policy has been established; a POA&M process has been implemented and managed to incorporate all known IT security weaknesses; and once identified, the weaknesses are prioritized and tracked, effective remediation plans are established for correcting the weaknesses, estimated dates for remediation are reasonable, and system owners are reporting progress on weaknesses to the agency CIO at least quarterly. In addition, OMB questions ask if the CIO centrally tracks, maintains, and independently reviews and validates POA&M activities on at least a quarterly basis.

#### **Progress to Date:**

An agency-wide POA&M process has been established for many years at the Board to identify and address deficiencies in information security policies, procedures, and practices. The ISO developed this program based on OMB guidance issued as early as 2001. The ISO has developed POA&M reporting guidance for divisions and offices to comply with the OMB guidance. As indicated in our 2008 FISMA report, an IT automated issue tracking enhancement that complements the existing manual tracking of division POA&M items was implemented by the ISO. Our review of quarterly POA&Ms determined that the POA&Ms continue to identify the OIG security control review recommendations; IT security issues identified by other Board activities, such as the Board's annual



financial statement audits; as well as planned IT security enhancements for Board divisions and offices. The ISO compiles quarterly performance statistics and reviews the agency POA&M and the performance reports with the CIO.

**Work To Be Done:**

The ISO has adopted the POA&M reporting format provided by OMB, which tracks the weaknesses, point of contact, scheduled completion date, milestone or corrective action to be accomplished, status changes for the corrective action, and how the weakness was identified. Divisions and offices have followed this format for many years; however, our security control reviews and follow-up efforts on outstanding IT security recommendations continue to identify where POA&M items have been designated as completed and removed from the POA&M, but upon further audit analysis it was determined that such items were only partially or not effectively remediated. We also noted this concern in our 2008 FISMA audit report. These occurrences translate into weaknesses that can continue to exist for years or at a minimum until the next system review. Also, our 2009 analysis identified where a risk assessment performed for a bundled system listed IT weaknesses that should have been placed on the division POA&M, but were not addressed and, accordingly, continue to represent some level of exposure.

Additionally, in our opinion, in many instances weaknesses that should have a quicker remediation timeframe or higher prioritization (notwithstanding resource limitations) remain on POA&Ms for an extended period, which translates into extended exposure for Board systems. The ISO maintains a repository for POA&Ms and reviews issues quarterly with the CIO. However, the primary responsibility for POA&M monitoring is placed with the division Information Security Representatives, and there is no formal coordinated effort for the division representatives to meet with the ISO to discuss their outstanding POA&M items and remediation plans and timeframes.

The POA&M process is one of the key, necessary tools to accomplishing the FISMA and OMB objective of improved security. Substantial time, effort, and resources are expended to perform reviews of agency systems at many levels and by various groups to identify needed improvements. The ISO has recently issued POA&M guidance that, once implemented, requires the ISO to test closed issues to certify they have been properly addressed. The ISO testing can be accomplished by either direct validation with the divisions and offices, or by working with the division representatives who are responsible for addressing the weaknesses.

**Recommendation 3:** We recommend that the CIO independently verify that appropriate corrective action has been implemented before items are removed from the Board's POA&M.

## **Security Awareness Training and Training Personnel with Significant Security Responsibilities**

### **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. OMB's annual FISMA reporting questions inquire whether (1) agencies have developed a process for identifying all general users, contractors, and system owners/employees who have log-in privileges and (2) IT awareness training has been provided to all such users with log-in privileges. In addition, agency employees with significant security responsibilities are to receive specialized training.

### **Progress to Date:**

The Board continues to provide security awareness training through an interactive computer-based system. All Board employees, contractors, and interns are required to complete the training. In addition to the standard mandatory security awareness training, the ISO provides additional awareness training modules and quizzes. Also, IT established a security awareness intranet page that contains complementary security awareness information, such as security articles issued throughout the year, password tips, prohibited system usage information, document information classifications, and other important security awareness material.

The ISO continues to track divisional security training information for Board personnel with significant information system security responsibilities. In addition, IT security staff offers special training to system owners, developers, managers and other senior officials responsible for making decisions regarding information systems. This special training covers FISMA compliance requirements and Board-specific requirements for system documentation, procedures, and implementation of security controls.

### **Work To Be Done:**

The Board has made significant improvements in the quality, tracking, and monitoring of its security awareness training program. The training program is geared towards helping the end users who are faced with security vulnerability scenarios in day-to-day use of the Board's IT resources. We recognize the Board's additional FISMA compliance training offered to staff and managers responsible for system-related decisions; however, this training is optional. We consider this special FISMA compliance training important to strengthen and address FISMA-related issues and potential changes in the Board's Information Security Program. Further, our security control reviews continue to identify

deficiencies. We believe that the CIO should consider making appropriate portions of the FISMA training program mandatory. Making such training mandatory can assist in increasing awareness and reinforce overall responsibilities for system security.

**Recommendation 4:** We recommend that the CIO provide mandatory specific FISMA training for selected staff with FISMA responsibilities.

### **Detecting, Reporting, and Responding to Security Incidents**

#### **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 also established requirements for incident reporting, which include establishing priority levels for categories of incidents and timeframes for reporting each priority level. OMB's annual FISMA reporting questions require the agency to report how often the agency complies with documented policies and procedures for identifying and reporting incidents internally; for timely reporting of incidents to US CERT; and for reporting to law enforcement agencies.

#### **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. During the past year, the ISO updated the Information Security Incident Handling Guide to include a Device and Document Loss Notification Report and developed a Media Sanitization and Disposal Policy and an International Travel Policy for Mobile Devices.

#### **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 review 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.

## **Continuity of Operations Plans and Procedures**

### **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. OMB's annual FISMA reporting questions require agencies to identify what systems in their inventories have contingency plan testing.

### **Progress to Date:**

During the past year, the Board conducted semiannual contingency tests. Divisions participate in tests, and the ISO uses the Board's application inventory to track the systems that have been tested. During this FISMA reporting period, the Board continued to update equipment for its contingency site.

In addition, IT reported it successfully tested the Board's new backup mainframe and disk replication services with the recently expanded bandwidth to the contingency facility. With the new technology in place, IT was able to restore mainframe services within one hour and provide "up-to-the-minute" data from the replicated disk services.

### **Work To Be Done:**

As stated in our 2008 FISMA audit report, although not a requirement of SP 800-53 for moderate rated systems, adequate capacity is necessary for information processing, telecommunications, and environmental support during crisis situations. The upgrade in the amount of bandwidth mentioned above should be beneficial with regard to capacity planning. We will continue to monitor the Board's contingency processes and procedures as part of our ongoing FISMA work.



BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM  
DIVISION OF INFORMATION TECHNOLOGY

DATE: November 12, 2009  
TO: Ms. Elizabeth A. Coleman  
FROM: Ms. Maureen Hannan */signed/*  
SUBJECT: Comments on the Office of Inspector General's 2009 Review of the Board's Information Security Program

Thank you for the opportunity to comment on the Office of the Inspector General's (OIG's) 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. We generally agree with the recommendations contained in this year's report and concur that the recommendations are primarily focused on enhancement opportunities. As part of our continual improvement efforts, we already have plans for additional program enhancements over the next two years that address most of the key improvement opportunities highlighted by your report. Provided below is a more detailed response to each of the recommendations contained in your report.

## **2008 Recommendation**

- 1. The OIG's 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. This recommendation is not being closed pending additional corrective action.**

The CIO generally agrees with this recommendation. In response to the 2008 recommendation and feedback from the OIG staff, a supplemental process was instituted to ensure that system owners perform a comprehensive risk assessment. This effort focused on ensuring that assessments take into consideration whether additional controls are required beyond the mandatory controls prescribed in the minimum control baseline. All Major Applications, stand alone Minor Applications or General Support System (GSS) subsystems which fall under the Board Information Security Program with a Moderate or High rating were required to complete this supplemental risk assessment process. The CIO reviewed the supplemental risk assessment process with office and division directors. Information Security Committee members were actively involved in the development of the supplemental

risk assessment process and the new process was highlighted during the annual FISMA training. All system owners completed the supplemental process and results were validated during this year's FISMA testing performed by the ISO.

In addition to the supplemental guidance, the Information Security unit continues to evaluate new guidance from the National Institute of Standards and Technology (i.e. Special Publication 800-53 Revision 3, Special Publication 800-37, Special Publication 800-39, and Special Publication 800-30) and has formulated initial plans to enhance existing risk assessment processes. The most recent draft of 800-37: *Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach*, was issued in April 2008 and introduced the concept of a Risk Executive Function and need to aggregate system risk assessments into a functional level assessment. The final version of 800-37 is scheduled for release in December 2009. Agencies are given one year to comply with the new guidance once it is finalized. Moreover, NIST Special Publication 800-39: *Managing Risk from Information Systems: An Organizational Perspective*, which provides guidance for building an organization wide risk management framework, is currently in draft and is scheduled to be finalized in December 2009. Additionally, Special Publication 800-30: *Risk Management Guide for Information Technology Systems*, which addresses performing risk assessments at the information system level, is currently being rewritten and the first public draft is scheduled to be released in December 2009. Special Publication 800-30 will likely not be finalized until December 2010.

The Information Security Officer is currently working with the Information Steering Committee to determine how best to address new requirements introduced by NIST in late 2009 and will work with the system owners to enhance the risk assessment process to better define business risks. The ISO also intends to implement a Risk and Compliance software package which is being considered as a standard by Reserve Banks. This initiative will help staff more effectively develop and maintain security plans, track FISMA and SOX testing results, and automate POA&M processes. This automated solution will also help system owners monitor the state of their systems and can simplify the risk assessment process. The conversion to the new Risk and Compliance system will take place in phases and will focus on GSS elements during 2010 and applications security plans in late 2010 and into the first half of 2011.

## **2009 Recommendations**

- 1. We recommend that the CIO ensure all systems have updated security plans that include all requirements, as part of implementing the new risk assessment process.**

The CIO generally agrees with this recommendation. GSS and system security plans are typically well maintained, but can become dated when GSS subsystems are updated due to a new software release or a configuration change. Such changes, however, do not typically have a material impact on the actual security posture of an application. Security plans are updated at least annually or any time that a major change takes place. The new Risk and Compliance system permits inheritance of controls between systems which is expected to reduce the duplicative impact of changes. Plans for implementing the new Risk and Compliance software are underway as previously described. The ISO will work closely with system owners to ensure that they update the technical details in their plans as they convert to the new Risk and Compliance system.

**2. We recommend that the CIO test select critical controls within the IT GSS annually.**

The CIO agrees with this recommendation. Presently, several GSS subsystems are tested quarterly as part of the SOX compliance program. In addition to testing one-third of the GSS subsystems annually, any subsystem that undergoes a significant change is re-tested. The ISO will also coordinate with the GSS system owners to identify key controls for GSS subsystems and will institute testing procedures to ensure that these key controls are tested at least annually.

**3. We recommend that the CIO independently verify that appropriate corrective action has been implemented before items are removed from the Board's POA&M.**

The CIO agrees with this recommendation. The ISO already implemented a quarterly testing process at the start of the fourth quarter to validate items removed from the POA&M during the previous quarter.

**4. We recommend that the CIO provide mandatory specific FISMA training for selected staff with FISMA responsibilities.**

The CIO generally agrees with this recommendation. The ISO has implemented new employee orientation training, annual employee awareness training, ad hoc focused training to address specific security issues or new policies, and annual FISMA training. The ISO also works closely with the ISC members to ensure that system owners receive annual training regarding the Board's security program and their specific roles and responsibilities. The ISO will reassess the current training process for system owners and will either continue to work with the ISC to ensure that all system owners receive the required training or will create a new training module to supplement the current system owner training.

## **Principal Contributors to the Report**

Robert McMillon, Auditor-in-Charge

Richard Allen, Senior IT Auditor

Satynarayana-Setty Sriram, IT Auditor

Peter Sheridan, Project Manager

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