Board of Governors of the Federal Reserve System

REPORT ON THE AUDIT OF THE BOARD'S INFORMATION SECURITY PROGRAM

OFFICE OF INSPECTOR GENERAL

September 2008

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

OFFICE OF INSPECTOR GENERAL

September 30, 2008

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 to evaluate compliance by the Board of Governors of the Federal Reserve System (Board) with FISMA and related information security policies, procedures, standards, and guidelines. We conducted our audit from May through September 2008 in accordance with generally accepted government auditing standards.

To evaluate security controls and techniques, we review controls over Board applications on an ongoing basis. During the past year, we issued security control review reports for three of the Board's major applications: a bundle of subsystems referred to as the EGov Systems, the Federal Reserve Integrated Records Management Architecture (FIRMA), and the Currency Ordering System (COS). We also issued a report on the controls of two third-party applications operated by the Federal Reserve Bank of Boston in support of the Board's supervision and regulation function. Our control tests identified areas where controls need to be strengthened. Given the sensitivity of the issues involved with these reviews, we provided the specific results to management in separate restricted reports. We performed our application control testing based on selected controls identified in the 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 controls, risk assessment, and personnel security) and include controls that can be categorized as system-specific or common (that is, applicable across agency systems). Consequently, although our focus was on evaluating specific applications, we also assessed some of the broader security controls that affect most, if not all, of the applications.

In March 2008, we issued a restricted report on these common security controls that identified opportunities for the Board's Chief Information Officer (CIO) to enhance and enforce existing policies and procedures, and to provide additional guidance that would assist system owners in implementing security controls under the Board's security program. We also followed up on open recommendations from prior security control reviews.

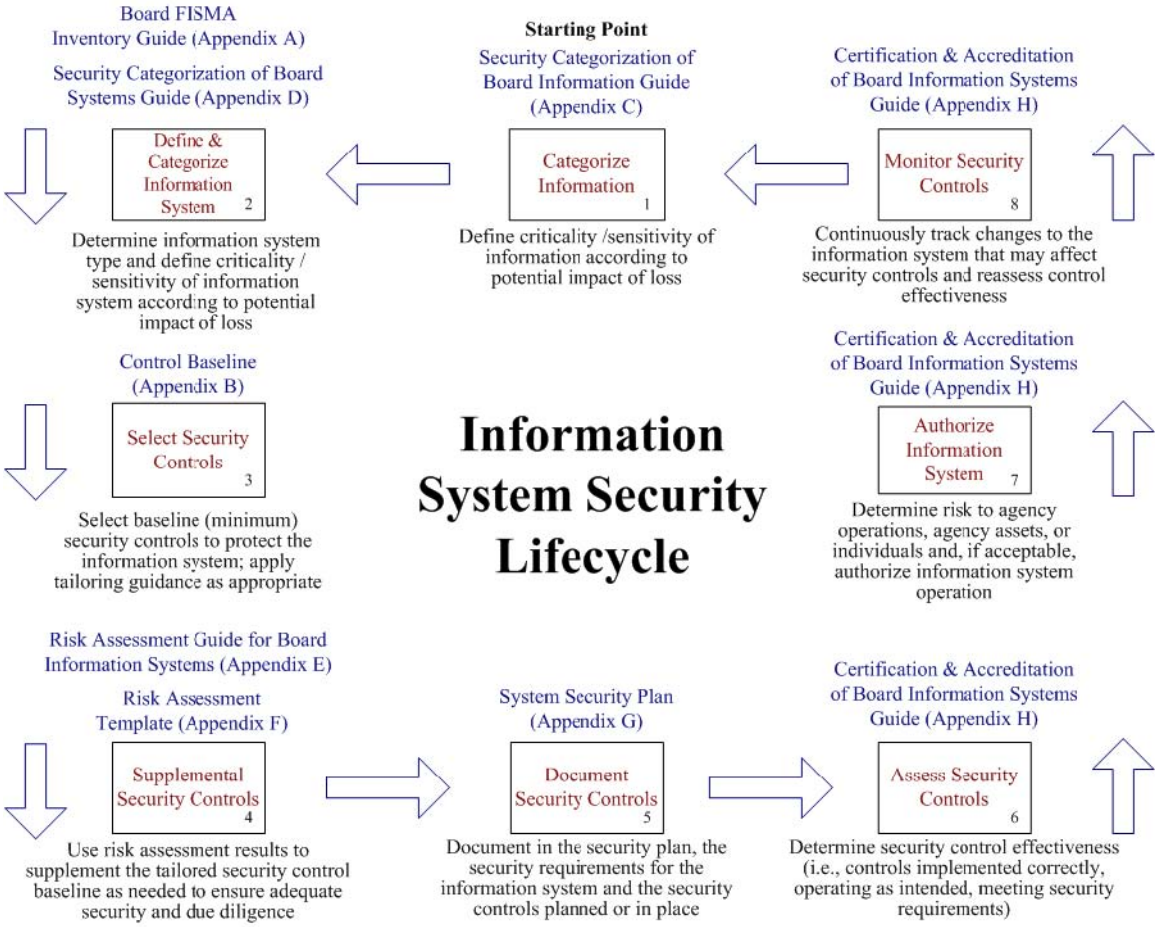
To evaluate the Board's compliance with FISMA and related policies and procedures, we reviewed components of the Board's certification and accreditation (C&A) process, including risk assessments, security plans, and security assessments. As part of the agency's annual FISMA reporting, the Office of Management and Budget (OMB) requests a specific response from both the agency and the OIG on certain security-related processes. Our work included analyzing the Board's security-related processes for security awareness and training, remedial action monitoring, incident response, configuration management, controls over personally identifiable information (PII), and privacy impact assessments (PIA). Our response will be provided to OMB by the Chairman under separate cover.

Our prior annual FISMA audits of the Board's information security program contained recommendations focused on bringing the Board's program into compliance with FISMA and NIST requirements. In our 2007 *Report on the Audit of the Board's Information Security Program*, we noted the Board had made progress toward implementing a structured information security program as outlined by FISMA. At the time of our report in 2007, we concluded that the primary challenge going forward was for the Board's CIO and Information Security Officer (ISO) to ensure that all aspects of the revised information security program were fully and consistently implemented across the systems supporting divisions and offices—as well as for third-party applications supporting Board programs and operations—and that controls were implemented correctly, working as intended, and producing the desired results.

The Board continues to advance and improve its information security program. During 2008, the Board enhanced its annual security awareness training and its processes for tracking security-related issues and initiatives. It also certified and accredited minor applications and subsystems by bundling the systems under the security plans of (1) a GSS; (2) a major application that provides a significant portion of its security control requirements; or (3) other minor applications to form a single major application. We found that the Board's inventory has remained stable from 2007, and that the bundling of minor applications and subsystems is a reasonable approach to implement the Board's security program.

During 2008, the ISO continued to update the Board's security program and related guidance to maintain a FISMA-compliant approach to managing and evaluating each Board information system throughout its lifecycle. As shown in Figure 1, the Board has established processes throughout the system lifecycle to lead to the certification and accreditation (C&A) of the Board's major applications and General Support Systems (GSS).

Figure 1. Board's IT Security Framework for the Information System Security Lifecycle[1]



However, our review of the certification and accreditation of major applications and the GSS supported by the Division of Information Technology (IT GSS), the Board's central GSS, identified opportunities for the Board to improve its risk assessment process and security assessment testing. We found that the risk assessments can be improved to explicitly identify the residual risk remaining after implementing minimum baseline controls. We also found that the security assessments performed as part of the C&A process need to be strengthened to include necessary and sufficient independent testing to provide the system owners with assurance that information security controls for these systems are effectively implemented and functioning as intended. Our report contains two recommendations to the CIO designed to ensure that (1) risk assessments adequately identify, evaluate, and document the level of risk to an information system based on potential threats, vulnerabilities, and currently implemented or planned controls,

[1] Each process in the lifecycle builds on the previous process, and any deficiency in one process will affect subsequent processes. For example, if the risk assessment does not adequately evaluate the level of residual risks remaining after the baseline controls are implemented, additional controls will not be identified as needed to lower the residual risk to an acceptable level, the security plan will not adequately describe how the risk is being addressed, and the security assessment will not provide the necessary assurances that the system is meeting its security requirements.

to determine if additional controls are needed; and (2) security assessments include necessary and sufficient independent testing to support the authorization for the system to operate, and provide the authorizing official and the Board assurances that information security controls for these systems are implemented correctly, working as intended, and producing the desired results. Appendix 1 contains our analysis of the Board's progress in implementing key FISMA requirements.

We provided our draft report for review and comment to the director of the Division of Information Technology (IT), in her capacity as the Chief Information Officer for FISMA. Her response is included as appendix 2. In her response, the director concurred with our recommendations. We will follow up on actions taken regarding our recommendations as part of future audit and evaluation work related to information security.

The principal contributors to this report are listed in appendix 3. We are providing copies of this audit report to Board management officials. In addition, the Chairman will provide the report to the director of OMB, as required by FISMA. 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,

/signed/

Elizabeth A. Coleman
Inspector General

Attachments

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

APPENDIXES

Appendix 1 – OIG Analysis of the Board's Progress in Implementing Key FISMA Requirements

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 (FIPS) 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 does not become obsolete, agencies should implement a review and revision process for its policies and procedures.

Progress to Date:

The ISO and his staff have completed a significant amount of work over the past few years to develop a security program that complies with NIST requirements. During the past year, the ISO has continued to enhance the security program to reflect changes in how the Board accounts for information assets, tracks the security compliance status of each system, and continues to develop policy and procedures for safeguarding personally identifiable information. To assist system owners in bundling minor applications and subsystems into the security plan of a major application or GSS that provides a significant portion of its security control requirements, the ISO developed an inventory guide that includes a decision tree for determining how the system should be included in the inventory. The ISO also updated the control baseline with instructions for subsystems, enhanced the risk assessment guide to reflect new system types, and developed a Bundled Subsystem Security Plan template.

In addition, the Board continues to develop policy and procedures for safeguarding PII. In the past year, the Board issued two new management policies that address privacy and information security issues. The "Policy for Handling Personally Identifiable Information" defines personally identifiable information and how to handle it at the Board; the updated "Data-Breach-Notification Policy and Plan" outlines the procedures that are to be followed if a loss of personally identifiable information occurs. The ISO has also issued a Mobile Code Policy, and a Media Disposal and Sanitation Policy that describe the process that the Board uses to sanitize and dispose of digital media that is not otherwise subject to particular restrictions. [2]

[2] Mobile Code, also known as Active Content, is defined as small pieces of software or program code that are automatically downloaded onto and executed on a user's PC, possibly without the explicit installation or execution by the recipient.

The IT security staff continues to conduct training for system owners and developers. The 2008 FISMA training consisted of sessions focused on the improvements and changes from last year's documents, addressing bundled subsystems. For those staff who were new to FISMA, an additional session was held to provide a step-by-step walk-through of how to complete FISMA documents for a sample system.

Work to Be Done:

An agency will always need to update and refine its information security program and the related policies and procedures as the program evolves and as NIST and OMB issue new guidance. To achieve this objective, agencies should implement a review and revision process for their policies and procedures to ensure that information security does not become obsolete and that the policies and procedures are working effectively to produce the desired results. While the Board does not have a formal review and revision process, we found that the Board has responded appropriately when OMB and NIST have issued changes to FISMA requirements. 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 and should identify interfaces between each system and other systems or networks. The inventory should also identify system criticality and risk levels. OMB expects agencies to have an inventory that is based on work completed in developing an enterprise architecture.

Progress to Date:

The Board's FISMA inventory has remained stable over the past year, but the Board continues to refine how it accounts for the certification and accreditation of minor applications and subsystems. During the past year, the Board has focused on bundling minor applications and subsystems into the security plans of either 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. According to the Board, bundling is a common practice and is encouraged to minimize the redundancy of security plan documentation. To bundle an application into a GSS under Board criteria, the application must have an impact rating of low or moderate, and the system owners must have reviewed the system-specific baseline of controls for the application and have documented in the risk assessment that the application relies only on the IT GSS for its non-system specific security controls (the system cannot rely on more than one GSS for its controls). We reviewed the rationale for bundling the minor applications into a

major application and determined that it was a reasonable approach to implement the Board's security program.

Our 2005 FISMA report recommended that the Board identify all information and information systems supporting its operations and assets, including those at Reserve Banks and other third parties, and ensure full and timely compliance with FISMA's legislative requirements and related information security policy and guidance. We did not close the recommendation in 2006 or 2007 because the Board still had work remaining to fully implement the Board's security program requirements for all systems on the inventory.[3] Subsequently, the Board has certified and accredited the IT GSS and major applications; in our opinion, this is sufficient action to close this recommendation. However, as discussed below, we believe that the Board can improve its risk assessment process and security assessment testing.

Work to Be Done:

Going forward, as new minor applications and subsystems are bundled into a GSS, the ISO will also need to ensure that controls are properly documented, implemented, and tested to provide the appropriate level of security. As the ISO continues to review the inventory and further implement the bundling guidance, we will evaluate the appropriateness of any revisions to the Board's application inventory.

As we reported last year, our 2005 information security audit report also 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. In responding to our recommendation, the Board's previous CIO for FISMA stated that the Board will continue to evaluate and make changes as appropriate to the organizational structure in light of the final inventory and any additional direction from OMB. Although the Board has finalized its inventory and has implemented components of its security program for systems maintained within the Board, our security control reviews have identified that the CIO and ISO need to ensure that system owners are clearly identifying system boundaries, and assessing the risk of relying on controls provided by entities that have not been certified or accredited in accordance with the Board's security program. We will continue to hold this recommendation open until the CIO has demonstrated the authority to fully implement the Board's security program for all information systems that support Board operations and assets, including those provided by the Reserve Banks and other third parties.

[3] See the following OIG reports: *Audit of the Board's Information Security Program*, dated October 2005; *Audit of the Board's Information Security Program*, dated September 2006; and *Audit of the Board's Information Security Program*, dated September 2007.

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.

Progress to Date:

The Board has developed a FISMA-compliant certification and accreditation process that requires system owners to determine the security categorization and impact rating of their system; apply minimum or a baseline set of NIST controls; perform a risk assessment to determine what residual risks remain after the baseline controls are implemented; and develop a security plan based on the complete set of controls needed.

To assist system owners, the ISO has issued guidance, including a standard template, and developed a set of minimum controls baseline that includes controls required by NIST Special Publication 800-53. The baseline identifies where the control is to be implemented (by the system or GSS), and the ISO provides information for the IT GSS controls and a template for use in documenting system specific controls. For major applications and stand-alone minor applications, the risk assessment consists of system owners documenting how the system specific controls are met and ensuring that the information on the IT GSS controls remains accurate, making revisions where necessary. For bundled subsystems, system owners are to review the information provided for the IT GSS and for any control that has not been documented, and provide the appropriate information or justification for the unique system controls in the bundled subsystem security plan. We judgmentally selected seven subsystems bundled into the IT GSS and verified that each had a risk assessment and a bundled subsystem security plan completed. The security plan included an assertion by the system owner that the security controls provided by the GSS had been reviewed.

Work to be done:

As part of our review of the Board's C&A process, we reviewed a sample of ten major applications that had been certified and accredited to operate between June 2007 and March 2008. We found that each application applied the minimum or baseline set of NIST controls and had completed a risk assessment template. However, we found no documentation or evidence that system owners are fully complying with the Board's risk assessment process and identifying the residual risk that remains after implementing the minimum set of controls defined in the Board's security control baseline. System owners are documenting that their system is meeting the minimum controls, but the security control baselines are not designed to protect against all threats. A comprehensive risk assessment should explicitly address the system owner's analysis of potential system vulnerabilities and demonstrate a thorough understanding of any associated risk. We believe that

the CIO needs to ensure that risk assessments are adequately identifying, evaluating, and documenting the level of risk to an information system based on potential threats, vulnerabilities and currently implemented or planned controls, to determine whether additional controls are needed.

Based on recommendations from our security control reviews, the ISO agreed to update the Risk Assessment Guide for Board Information Systems with additional guidance to ensure that system owners more effectively identify system boundaries and more fully address additional risks that may result when interconnections to other systems are established. The ISO will also perform a common risk assessment addressing Reserve Bank direct access to Board Systems. We will continue to review implementation of the risk assessment process as part of our future application security control reviews.

Recommendation 1: We recommend that the CIO ensure that risk assessments are adequately identifying, evaluating, and documenting the level of risk to an information system based on potential threats, vulnerabilities and currently implemented or planned controls, to determine whether additional controls are needed.

Security Plans

Requirement:

FISMA requires that agencies develop security plans for each system in the inventory. The system security plans should be based on the agencywide plan, provide an overview of the system's specific security requirements, and describe the controls in place or planned for meeting those requirements. System security plans 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 Security Program requires the system owner to develop a security plan based on the complete set of controls required for the system (that is, 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 bundled subsystems. In addition, the ISO has updated the security plan template to document whether the system contains PII.

As previously described in the Periodic Risk Assessment section, system owners are required to analyze the template information to ensure that controls are sufficient for their systems. The baseline becomes part of the security plan. Approval of a security plan signifies approval of all documents referenced by the security plan and baseline. The bundled subsystem security plan requires system

owners to assert that all security controls provided by the control baseline have been reviewed to determine that the subsystem relies upon the provided GSS security controls, and that the controls satisfy all subsystem control requirements with the exception of any other specific controls documented.

As part of our review of the Board's C&A process we judgmentally selected a sample of twenty-six subsystems and minor applications that have been bundled into nine major applications, and found each of the system owners of the major applications had developed security plans that include the subsystems. We also selected a sample of seven subsystems that had been bundled into the IT GSS and verified that each had a risk assessment and a bundled subsystem security plan completed.

Work to be done:

Full implementation of the security planning process will not occur until all plans provide an overview of the system's specific security requirements, and describe the controls in place or planned for meeting those requirements. As discussed under the risk assessment section, if the control baseline and risk assessment is inadequate or contains errors, the security plans will not fully describe the system's security environment or identify other needed controls.

In addition, our security control reviews 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. We will review completed security plans during future security control reviews.

Periodic Testing and Evaluation

Requirement:

FISMA requires periodic testing and evaluation of the effectiveness of an agency's information security policies, procedures, and practices. The evaluation includes testing of the management, operational, and technical controls for each system identified in the agency's inventory and should be performed on a risk-based frequency, but not less than annually. Each system must also undergo a periodic certification and accreditation to ensure that the individual responsible for the system has performed activities needed 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, of if the system undergoes a significant change.

Progress to Date:

The Board's security program requires the certification and accreditation of a system based on a system security plan, security assessment report, and plan of actions and milestones (POA&M). The security assessments are to be performed by an independent certification agent and directly support the security accreditation by providing authorizing officials with the information necessary to make credible, risk-based decisions on whether to place an information system into operation or to permit an existing system to continue its current operation.

The ISO has issued security certification review reports for the IT GSS and major applications on the Board's inventory. Minor applications and subsystems bundled into the security plans of a major application or GSS are certified with the major application or GSS, and will be tested as part of that major application or GSS.

To provide consistency and document the security review, the ISO has developed C&A testing steps for the certification agent to follow and document their work. We compared the certification test steps to the Board's baseline and found that the test steps incorporated the baseline controls implemented by the GSS and the system. The test steps included controls for applications at all impact levels (low, moderate, high).

Work to be done:

As part of our review of the Board's C&A process, we reviewed both the security assessments for a sample of ten major applications that had been certified and accredited to operate between June 2007 and March 2008, as well as components of the 2007 security assessment of the IT GSS. We found a lack of necessary and sufficient independent testing conducted by the certification agent that is supposed to provide the system owners assurance that information security controls for these systems are effectively implemented and functioning as intended. The certification testing focused on validating that the system owner provided correct information for controls in the baseline and that the control exists, not whether the control is operating effectively. We also found that the C&A test step documentation was not centrally maintained or always retained. We believe that the CIO needs to ensure that security assessments include necessary and sufficient independent testing to support the authorization to operate, and to provide the authorizing official and the Board assurances that information security controls for these systems are effectively implemented and functioning as intended.

The IT GSS has been separated into nineteen components and the ISO has developed individual security control baselines for each component. The ISO plans to conduct reviews over the next three years on the various components and subsystems. To ensure that all systems are appropriately tested, the ISO will need to document a three-year review schedule for the nineteen components and

ensure that each of the bundled minor applications and subsystems will be tested within the components.

In addition, the IT GSS and Management GSS security plans encompass: common controls provided by the CIO and ISO offices for all Board information systems; infrastructure component specific controls; and common controls provided by infrastructure components to Board information systems. Since all systems at the Board rely on these common controls, the ISO will need to coordinate the results of the security testing with system owners.

Recommendation 2: We recommend 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 assurances that information security controls for these systems are implemented correctly, working as intended, and producing the desired results.

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. The POA&Ms should include all security weaknesses found during any review done by, for, or on behalf of the agency, including Government Accountability Office audits, financial statement audits, and critical infrastructure vulnerability assessments. In addition, program officials should regularly update the CIO on their progress in implementing corrective actions to better enable the CIO to monitor agencywide remediation efforts and provide the agency's quarterly POA&M update to OMB.

Progress to Date:

The ISO continues to ensure that divisions accurately update their division-level information and has developed a centralized web interface to manage POA&M items. We believe that this is a significant improvement that will assist the ISO in tracking security-related issues and addressing deficiencies. Our review of the quarterly POA&Ms identified that the OIG's security control review recommendations have been placed on appropriate division POA&Ms, and the IT Division's POA&M has been expanded to track all security related initiatives in addition to security weaknesses. The ISO has stated that he regularly updates the CIO on the division's progress in implementing corrective actions.

Work to be done:

Our security control reviews identified two POA&M items that had been removed from the POA&M without corrective actions being documented and validated; a recommendation was addressed to the system owner. As part of future security assessments, we believe that the certification testing needs to ensure that previously identified vulnerabilities that have been removed from the POA&M have had necessary and sufficient action taken to resolve the vulnerabilities. We will continue to review the Board's tracking and resolution of POA&M items as part of our ongoing FISMA related audit work.

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 in complying with agency policies and procedures. FISMA also requires that the CIO train and oversee personnel with significant responsibilities for information security.

Progress to Date:

The Board requires all employees and contractors to take an annual security awareness training and quiz. The quiz reinforces security articles posted throughout the year on the Board's internal website. During the past year, the ISO upgraded the training and quiz to an interactive, computer based system that requires the user to be connected to the Board's network to participate. Upon completion of the security awareness quiz, employees are required to acknowledge that they will abide by all Board policies and rules that apply to the Board's IT resources.

Work to be done:

In our 2007 FISMA report, we found that the ISO had developed guidance regarding the identification of personnel with significant responsibilities for information security, and had outlined a minimum set of training that staff should receive based on their role. The ISO is currently conducting a survey of training taken by individuals with significant security responsibilities. We will review the Board's progress in identifying and providing training to individuals with significant security responsibilities as part of our future security control reviews.

As previously discussed in the Policies and Procedures section, the Board continues to develop policy and procedures for safeguarding PII, and during the past year issued two new management policies that address privacy and information security issues. The Board plans to develop an education/training

program to assist in implementing the policies and procedures. We will review the education/training program as part of future FISMA related audits.

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 OIGs. US-CERT has also established requirements for incident reporting, which include priority levels for categories of incidents and the timeframes for reporting each priority level.

Progress to Date:

The ISO continues to issue 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 and issued a standard template form to document a suspected or confirmed theft or loss of any computers, mobile devices, data storage devices or media, and restricted documents.

To reinforce employees' responsibilities, the ISO continues to post articles on this topic on the Board's website as part of security awareness training. The most recent Security Awareness Quiz included a review of the Permissible-Use and Privacy Policy, Information Classification & Handling Guide, and Security Incident Handling Guide.

Work to be done:

The Board's security program requires system owners either to complete a Privacy Impact Assessment (PIA) as part of the planning process or to obtain a determination from the Board's Legal Division that a PIA is not required. To assist system owners, the Legal Division has developed draft guidance that outlines the PIA requirements for those systems with PII. The guidance consists of two parts: a Frequently Asked Questions section and a Privacy Impact Assessment Questionnaire (PIAQ) that staff responsible for the system will fill out for those systems that require a PIA or are subject to the requirements of the Privacy Act. The information provided in the response to the PIAQ is used to prepare the PIA. We will continue to review the Board's actions to complete and implement the guidance as part of future security control reviews.

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 FISMA reporting guidance also indicates that contingency planning is a requirement for certification and accreditation, with annual contingency plan testing required thereafter.

Progress to Date:

The Board continues to conduct semiannual contingency testing. Divisions participate in the semiannual contingency tests and the ISO uses the Board's application inventory to track the systems that have been tested. During the past year, the Board continued to update equipment at its contingency site, and mitigate the risks that were observed during recent national disasters.

Work to be done:

The Board conducted a contingency test in September 2008. However, the prior scheduled contingency test was cancelled due to the exigencies of the economic situation at the time. The CIO based her decision on the circumstances that the Board may have needed, at any time, all resources that could be available. If the semiannual contingency testing becomes burdensome, the Board may want to consider smaller, more focused contingency tests.

To help ensure that the contingency tests continue to provide value to the Board, the CIO and ISO (in conjunction with Board staff responsible for contingency planning) will need to ensure that the tests continue to be rigorous, that participants are challenged by the exercises, and that the participants do not become complacent. In addition, although not a requirement of SP 800-53 for moderate rated systems, the Board may wish to consider capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations. We will continue to monitor the contingency tests as part of our ongoing FISMA work.

APPENDIX 2

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

DATE: September 19, 2008

TO: Ms. Elizabeth A. Coleman

FROM: Maureen Hannan ***/signed/***

SUBJECT: Comments on the Office of Inspector General's 2008 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 of the program continues to recognize that our information security policies and processes are FISMA-compliant and that we continue to enhance the program. As noted in your report, we continue to improve and enhance our security policies and procedures, tracking of remediation action, and security awareness training. We maintain an accurate inventory of all systems and have performed certification and accreditation reviews for each system. We continue to strengthen configuration management processes and maintain an effective layered security model as demonstrated by our most recent independent verification and validation exercise.

We concur with the recommendations to improve the risk assessment and control testing processes. These recommendations are consistent with our own self-assessment of the information security program and our plans to improve the program. We plan to work closely with system owners over the next year to ensure risk assessments are comprehensive and we are evaluating tools that may be employed to assist system owners perform and maintain risk assessments. We have also expanded our information security compliance unit and will be enhancing our control testing processes.

Appendix 3 – Principal Contributors to the Report

Peter Sheridan, Audit Manager

Richard Allen, IT Auditor

Robert Delgesso, IT Auditor

Satynarayana-Setty Sriram, IT Auditor

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