

Board of Governors of the Federal Reserve System

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



OFFICE OF INSPECTOR GENERAL

September 2006

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



OFFICE OF INSPECTOR GENERAL

September 27, 2006

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), 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 in accordance with generally accepted government auditing standards.

To evaluate security controls and techniques, we reviewed controls over two applications and followed up on the open issue from our 2005 application control review. We performed our application control testing based on controls identified in the National Institute of Standards and Technology (NIST) Special Publication 800-53, *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 (i.e., applicable across agency systems). As a result, although our focus was on evaluating specific applications, we also assessed many of the broader security controls that impact most, if not all, applications. One of the applications we reviewed is a supervision and regulation (S&R) system maintained at the Board. We also reviewed a system maintained by the Federal Reserve Bank of New York (FRB NY) in support of the Board's statistical reporting function.

Our control tests identified areas where controls need to be strengthened. Because some of the issues we identified are more significant—either alone or in combination with other weaknesses—we have classified several of our findings as "control deficiencies." As discussed more fully below, we also found that FRB NY had not yet implemented any of the processes associated with the Board's revised information security program for the application we reviewed; these processes are fundamental FISMA requirements. Given the sensitivity of the issues involved with these reviews, we will provide the specific results to management in separate restricted reports. Follow-up work on our 2005 application control review allowed us to close the outstanding recommendation.

To evaluate the Board's compliance with FISMA and related policies and procedures, we followed up on the open recommendations in our 2004 and 2005 information security audit reports issued pursuant to FISMA's requirements.¹ Because FISMA authorizes the IGs to base their annual evaluation in whole or in part on existing audits, evaluations, or reports relating to programs or practices of the agency, we also incorporated the results from, and actions taken on, (1) our 2005 audit of efforts by the Federal Reserve System (System) to implement FISMA's requirements for applications operated by the Reserve Banks in support of the Board's delegated S&R function and (2) our 2006 audit report related to electronic authentication (e-authentication).²

In addition, we compiled information on, and reviewed the Board's processes related to, areas for which the Office of Management and Budget (OMB) requested a specific response as part of the agency's annual FISMA reporting; our response will be provided to OMB by the Chairman under separate cover. Areas we reviewed include security awareness and training, certification and accreditation (C&A), remedial action monitoring, incident response, configuration management, and controls over personally identifiable information (PII). Our work on configuration management identified issues related to the Board's processes for establishing, implementing, and maintaining baseline configurations; we will share our specific testing results with management under separate restricted cover.

Overall, we found that the Board's information security program continues to evolve and mature. Our work showed that, over the past year, the Board has made considerable progress toward implementing a structured information security program as outlined by FISMA and has taken actions to address open audit recommendations. Specifically, we found that the Board has developed additional program guidance, revised its application inventory, begun C&A work, and incorporated the Reserve Bank S&R applications into the revised security program. However, the Board still has work remaining to fully implement recent NIST guidance, as well as all aspects of the Board's revised security program. Consequently, several of our audit recommendations remain open. As we reported in 2004 and 2005, the Board faces significant challenges in transitioning from its prior policies and procedures to the new NIST guidance. While we recognize the magnitude of the effort and the progress made, we once again note that complying with these new requirements is essential to maintaining compliance with the security legislation.

Appendix 1 contains our analysis of the Board's progress in implementing each of FISMA's primary requirements. We have identified areas where the Board's actions are sufficient to close a corresponding audit recommendation. We have also summarized the work we believe remains for each of the legislation's requirements and the reasons why audit

¹ See our *Report on the Audit of the Board's Information Security Program*, dated September 2004 and our *Report on the Audit of the Board's Information Security Program*, dated October 2005.

² See our *Report on the Audit of the Supervision and Regulation Function's Efforts to Implement Requirements of the Federal Information Security Management Act*, dated September 2005 and our *Report on the Audit of the Board's Implementation of Electronic Authentication Requirements*, dated March 2006.

recommendations, or portions of recommendations, remain open. Appendix 2 contains a high-level summary of our information security-related audit reports with outstanding recommendations and their current status (i.e., open or closed). Based on our audit fieldwork, we are also providing two additional recommendations related to training on the Board's new information security program and to training staff with significant security responsibilities.

We provided our draft report for review and comment to the director of the Division of Information Technology (IT), in her capacity as Chief Information Officer (CIO) for FISMA. Her response is included as appendix 3. In her response, the director agreed to implement our audit recommendations. The director also cited several efforts the Board has undertaken to protect its systems from malicious software, unauthorized use, and growing threats. 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 4. 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/

Barry R. Snyder
Inspector General

Attachments

cc: Mr. Stephen Malphrus
Ms. Marianne Emerson
Mr. Roger Cole
Mr. Peter Purcell
Mr. Raymond Romero

APPENDIXES

Appendix 1 – OIG Analysis of Board Progress in Implementing FISMA’s Primary 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 appropriate 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 effectively implement specific controls 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 Information Security Officer (ISO) has developed or revised guidance to help implement the Board’s information security program. The guidance includes policies on performing risk assessments, developing security plans, and tracking remedial actions. The ISO has worked with Board staff in divisions and offices to implement the guidance for systems under their control. The ISO has also worked with staff in the Division of Banking Supervision and Regulation (BS&R) to ensure that Reserve Banks are aware of, and implement, requirements of the Board’s information security program. The updated policy on risk assessments contains additional guidance for performing e-authentication assessments, and we are therefore closing the first part of the recommendation in our 2006 e-authentication report.

Work to Be Done:

The C&A policy remains in draft, although the Board has begun certifying and accrediting its information systems; the ISO should finalize and issue this policy to help divisions and offices meet the C&A requirements. The Board has also drafted a new policy on safeguarding PII. We reviewed the draft, and have identified several areas where we believe the policy can be enhanced. Specifically, we believe that the Board should ensure that the guidance addresses the protection needs associated with PII that is accessed remotely or is physically removed from Board-controlled areas. The final policy should also identify rules for determining whether physical removal, remote access, and downloading and remote storage are allowed. In addition, if these activities are allowed, the policy should clearly identify appropriate procedures for handling PII.

Given the volume of guidance issued over the past two years and the change that the guidance represents from the Board’s prior security program, we also believe that additional training for information and information system owners would help ensure the program’s effective implementation. Our discussions with

managers during the course of our control reviews showed that not all managers were aware of all aspects of the new program.

Recommendation:

We recommend that the Chief Information Officer (CIO) enhance the Board's security program by finalizing security-related policies and by providing additional training focused on the revised information security program and associated Board policies and NIST guidance.

Application Inventory

Requirement:

As part of the agency's security program, 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 FISMA's periodic testing requirement and should identify interfaces between each system and all other systems or networks. The inventory should also identify system criticality and risk levels. OMB expects agencies to have an inventory based on work completed in developing an enterprise architecture.

Progress to Date:

Our 2005 information security audit report contained a recommendation 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. During the past year, the Director of the Division of Information Technology (IT), who also serves as the Board's CIO for FISMA, issued an inventory guide which includes a decision tree to assist in determining whether a system is subject to the Board's information security program, and how the system should be classified on the inventory. The ISO also worked with all divisions and offices to clarify whether applications should be designated as major applications, general support systems, or sub-systems that are part of a major application or general support system. This work is responsive to the first part of our recommendation.

Our 2005 report on S&R's FISMA implementation efforts contained a similar recommendation for developing an inventory of S&R-related applications. The Board's inventory guide contains guidance to help Reserve Banks identify and organize information assets operated by Reserve Banks under delegated authority from the Board. Over the past year, BS&R staff worked with all of the Reserve Banks to review their application inventories, establish greater consistency across the System, and establish logical groupings of applications. Now that the S&R inventory is final, we will review the process followed for identifying and grouping applications; we anticipate closing the recommendation during the final quarter of the year.

Work to Be Done:

As noted in several areas below (risk assessments, security plans, and certification and accreditation), the Board still has work remaining to fully implement FISMA's requirements for all systems on the inventory; we are therefore leaving our recommendation open until this work is completed. Although our audit work this year did not identify any additional applications that we believe should be added to the Board's inventory, we will continue to review the classification of systems as part of future audit work. In addition, other audits, inspections, and evaluations may identify additional applications that we believe meet FISMA's requirements for inclusion on the Board's inventory, and we will address with the ISO any concerns as they arise.

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 compliance with FISMA's requirements for all information and information systems that support Board operations and assets, including those provided by the Reserve Banks and other third parties. In her response to our recommendation, the Board's 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 developments from OMB. We will hold this recommendation open until the work discussed above is completed. At that time, if the Board has not yet implemented appropriate organizational changes, we will refer the recommendation to the Committee on Board Affairs for final resolution.

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:

Last year, divisions and offices identified and categorized Board information and the related information systems as outlined in NIST's Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199). The FIPS 199 assessment forms the basis of ensuring that information and information systems are provided the appropriate level of information security. The director of IT issued a policy on risk assessments, including a standard template to assist divisions and offices in performing the assessments. System owners are completing the revised risk assessment templates in preparation for each system's C&A. Reserve Bank systems supporting the S&R function are completing the revised template as well.

Work to Be Done:

Full implementation of the new risk assessment process will not occur until all systems have been through a C&A. As part of the new process, the ISO will also need to ensure that third-party systems not supporting the S&R function complete the risk assessment process. We found that the FRB NY staff supporting the application we reviewed had not yet completed the Board's risk assessment template, although another risk certification process had been completed as required by System guidance. We will review the completed assessments as part of future audit work on the Board's C&A process, as well as during future security control tests performed on selected systems.

Security Plans**Requirement:**

FISMA requires agencies to 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 ISO developed new security plan templates for major applications, general support systems, and subsystems. System owners are required to complete the appropriate template in preparation for certifying and accrediting their systems. In completing the templates, system owners must document how the SP 800-53 baseline controls have been implemented. The templates have also been applied to Reserve Bank systems in support of the S&R function, which allows us to close one of our recommendations from our 2005 report on S&R's FISMA implementation.

Work to Be Done:

Full implementation of the new security plan will not occur until all systems have been through a C&A. As part of the new security planning process, the ISO will also need to ensure that third-party systems not supporting the S&R function meet this requirement. We found that the FRB NY staff supporting the application we reviewed had not yet completed a system security plan. We will review completed security plans as part of future audit work on the Board's C&A process, as well as during future security control tests performed on selected systems.

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 every system identified in the agency's inventory and should be performed with a frequency depending on risk, 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 guaranteed that security controls are commensurate with the risk and magnitude of the harm resulting from the 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 then every three years thereafter, unless the system undergoes a significant change.

Progress to Date:

The ISO issued guidance for conducting security control reviews which includes specific testing requirements, and divisions followed the guidance for reviews conducted during 2005. Actions taken are sufficient to close the open recommendation from our 2004 information security audit report. The ISO has also drafted a new policy for C&A, and several Board systems have completed the C&A process.

Work to Be Done:

The table below shows the total number of Board and third-party systems and the number of systems that were certified and accredited—or certified, but not yet accredited—as of the end of our audit fieldwork on August 31, 2006. The table also reflects the number of additional systems that the ISO expects to complete the certification process by the end of September. The ISO stated that any systems not undergoing certification will have completed annual control reviews by September 30.

	Board Systems			Third Party Systems
	Major Applications	General Support Systems	General Support Subsystems	
Total number of systems	17	5	100	54
Systems with a completed C&A	1	0	3	0
Systems with a completed certification, but not yet accredited	1	0	7	0
Additional systems to be certified by September 30	6	3	72	41

We commend the Board for the C&A work accomplished. However, we believe the ISO has established an aggressive timetable to finish testing prior to the end of September. At the same time, we remain concerned that all systems have not completed the C&A process. Given the timing of the completed certification work, we have not yet reviewed the completed certification packages or the associated testing processes in depth. We plan to focus on this area in the latter part of the year.

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 Plans of Action and Milestones (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:

Earlier this year, the ISO provided divisions with additional guidance regarding the tracking and reporting of security-related issues. We reviewed the Board's POA&M process as part of our current audit and found that the level of detail included by some of the divisions on their POA&Ms has improved during the year. Specifically, the information identifying weaknesses and enhancements was clearer and better documented in the appropriate sections of the reports we reviewed.

Work to Be Done:

Our review of POA&Ms completed since September 2005 found that division-level reporting of performance metrics on outstanding issues is not always consistent from quarter to quarter; this could affect the roll-up of division-level information to the overall Board POA&M which is reported to OMB. These inconsistencies were one reason for not closing our 2004 audit recommendation related to POA&Ms. Our review also found that weaknesses were removed from division POA&Ms although it was unclear that sufficient actions had been taken to close the item. We will continue to review quarterly submissions by the divisions to the ISO as well as the ISO's submission to OMB, and we will close the recommendation once the ISO's guidance has been fully implemented. Given the continuing issues we identified regarding the performance metrics, the ISO may want to incorporate this area into the additional training discussed in our recommendation regarding training on the Board's security program.

Security Awareness Training/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 continues to post security awareness articles on the Board's internal website. During the past year, these articles have covered topics such as information handling specifications, password requirements, and PII. In addition, the Board administers an online security awareness quiz covering security articles posted during the year.

Work to Be Done:

As noted above, we believe that the new guidance related to the Board's revised security program provides an opportunity for additional training focused on the revised program and the corresponding Board policies and NIST guidance. We also believe that opportunities exist to enhance the Board's process for designating and training staff with significant security responsibilities. Identifying employees with significant security responsibilities and establishing their training requirements remain the responsibilities of the individual divisions and offices, although the ISO annually requests this information as part of his reporting responsibilities. Our control review of one Board system found that individuals who were application system security administrators had not been designated as having significant security responsibilities and, in our opinion, had not received the proper level of training. Our work at one Reserve Bank also found that none of the system security administrators involved with the application had been so designated, and thus had received limited training. We note that a web-based training program for which the Board had previously contracted was poorly utilized, and the Board discontinued the contract; no additional specific training-related guidance has been provided.

Recommendation:

We recommend that the CIO provide additional guidance for designating individuals with significant security responsibilities and identify specific training requirements.

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 Federal Computer Incident Response Center (FedCIRC)/United States Computer Emergency Readiness Team (US-CERT), appropriate law enforcement agencies, and relevant OIGs. FedCIRC/US-CERT has also established requirements for incident reporting, which include five priority levels for categories of incidents and the timeframes for reporting each priority level.³

Progress to Date:

Consistent with our 2004 information security audit report recommendation, the ISO expanded the types of information being reported to FedCIRC/US-CERT to include reporting of level 5 incidents. The ISO continues to interact with System staff responsible for security incidents and receives daily reports of potential incidents from across the System.

Work to Be Done:

The ISO does not yet report level 4 incidents, although he stated that he would report incidents that, in his opinion, raise security concerns. The ISO was also in the process of revising the Board's incident response procedures, to include additional guidance for third parties. We will review the guidance when issued and determine whether the ISO's actions are sufficient to close our open recommendation. Our security control review of a Board application also identified opportunities to enhance incident reporting by third parties and we are providing a recommendation to management as part of our control review report.

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.

³ FedCIRC/US-CERT established the incident categories and reporting timeframes to enable improved communications between and among agencies. The categories range from category 1 (unauthorized access) which should be reported within one hour of discovery or detection, to category 5 (scans, probes, and attempted access) which should be reported on a monthly basis.

Progress to Date:

The Board conducts semiannual contingency testing. All divisions participate in the semiannual contingency test and report to the ISO which of their systems were tested.

Work to Be Done:

We shared our observations of the past two contingency tests with IT management and offered suggestions for enhancing the testing. Our suggestions included reviewing required recovery timeframes, coordinating backup tape delivery, and developing after-action reports. We believe the latter suggestion could be particularly useful in assisting the ISO with identifying items that divisions and offices should include on their POA&Ms.

Appendix 2 – Status of Audit Recommendations Related to Information Security

2004 Report on the Audit of the Board’s Information Security Program

Original Recommendation	Status
We recommend that the CIO enhance the process for prioritizing, tracking, and managing security performance gaps by (1) providing additional guidance on the level of detail that should be reported on Plans of Action and Milestones (POA&Ms) and (2) ensuring that all security related tasks are monitored through the Board’s POA&M process.	Partially Closed
We recommend that the CIO provide guidance for conducting information security reviews that (1) includes specific requirements for control testing and (2) establishes greater consistency across all reviews.	Closed
We recommend that the CIO expand the Board’s reporting of security incidents to include all five incident priority levels, as well as incidents that occur at the Reserve Banks and other third-party contractors. ⁴	Open

2005 Report on the Audit of the Board’s Information Security Program

Original Recommendation	Status
We recommend 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.	Partially Closed
We recommend that the Board establish full-time, independent Chief Information Officer (CIO) and Information Security Officer (ISO) positions that have the authority to direct and enforce compliance with FISMA’s requirements for all information and information systems that support Board operations and assets, including those provided by the Reserve Banks and other third parties.	Open

⁴ At the time of our audit recommendation in 2004, FedCIRC/US-CERT had only established four priority levels. During 2005, FedCIRC/US-CERT revised their reporting guidelines to be consistent with NIST and established five reportable categories. We have updated our recommendation wording to reflect this change.

2005 Report on the Audit of the Supervision and Regulation Function's Implementation of FISMA

Original Recommendation	Status
We recommend that the CIO provide guidance for developing an inventory of S&R-related applications and ensure that the guidance is implemented consistently across the System.	Partially Closed
We recommend that the CIO issue guidance to clearly define the requirements for a system security plan.	Closed
We recommend that the CIO issue guidance for conducting information security reviews that includes specific requirements for control testing.	Open
We recommend that the CIO issue guidance that clearly defines the roles and responsibilities for implementing corrective actions.	Closed

2005 Report on the Audit of the Board's Implementation of Electronic Authentication Requirements

Original Recommendation	Status
We recommend that the CIO: (1) finalize e-authentication guidance, to include providing additional guidance regarding assurance levels; (2) ensure that all applications meeting e-authentication requirements are identified and properly assessed; and (3) ensure that procedures are in place to include the validation and periodic reassessment of assurance levels as part of the Board's revised information security program.	Partially Closed

Appendix 3 – Division Director’s Comments

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

MEMO

DATE: September 25, 2006
TO: Mr. Barry R. Snyder
FROM: Marianne M. Emerson */signed/*
SUBJECT: Comments on the Office of the Inspector General’s 2006 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 glad that you recognize that our information security program continues to mature from a Federal Information Management Security Act (FISMA) perspective. At the same time, we have a strong program without any intrusions. We continue to strengthen our automated log monitoring, configuration and patch management processes, to protect our systems from malicious software and unauthorized use. We continue to add new security safeguards to protect our systems from growing threats. Also, as you noted, we continue to strengthen our security awareness program, helping to ensure that all Board employees and contractors know what to do to protect our information. I will see that we will provide additional training to business owners and software developers on the revised program, associated Board policies and National Institute of Standards and Technology (NIST) guidance, as you recommend. I will also provide additional guidance on designating individuals with significant security responsibilities and their training requirements, again as you recommend.

c: S. Malphrus
S. Alvarez
P. Purcell
W. Mitchell
A. Foster

Appendix 4 – Principal Contributors to this Report

Robert McMillon, Senior IT Auditor and Auditor-in-Charge

Richard Allen, IT Auditor

Gerald Edwards, Auditor

Peter Sheridan, Senior IT Auditor

Satynarayana-Setty Sriram, IT Auditor

Keisha Turner, Auditor

Silvia Vizcarra, Auditor

William Mitchell, Assistant Inspector General for Audits and Attestations