Board of Governors of the Federal Reserve System

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

OFFICE OF INSPECTOR GENERAL

September 2007

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

OFFICE OF INSPECTOR GENERAL

September 25, 2007

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 December 2006 through September 2007 in accordance with generally accepted government auditing standards.

To evaluate security controls and techniques, we reviewed controls over three Board applications and followed up on the open issues from our 2006 application control reviews. We also recently began a review of controls provided by the Federal Reserve Bank of Boston (FRB Boston) for applications the Reserve Bank maintains in support of the Board's supervision and regulation function. We performed our application control testing based on controls identified in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 1, *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, applications.

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." 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 2006 application control reviews allowed us to close several of the outstanding recommendations.

To evaluate the Board's compliance with FISMA and related policies and procedures, we followed up on open recommendations from prior information security audit reports issued pursuant to FISMA's requirements.[1] Because FISMA authorizes the IGs to base their annual evaluations 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; (2) our 2005 review of the Board's implementation of software security reviews; and (3) 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, controls over personally identifiable information (PII), and privacy impact assessment (PIA) processes.

Overall, we found that the Board's information security program continues to evolve and mature. The Board has made additional progress toward implementing a structured information security program as outlined by FISMA and has taken action to address open audit recommendations. Specifically, we found that the Board revised its information security program to incorporate guidance and standards recently issued by NIST. The Board also updated many of its information security policies and guidance, continued to certify and accredit information systems, and provided training to system owners and developers on their security-related responsibilities. Despite this progress, however, the Board still has work remaining to fully implement its information security program for all systems on the application inventory; consequently, three of our audit recommendations remain open or partially closed.

Based on our security-related fieldwork over the past year, we are not making any new recommendations in this report. In our opinion, the primary challenge going forward for the Board's Chief Information Officer (CIO) and Information Security Officer (ISO) is to ensure that all aspects of the revised information security program are 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 are implemented correctly, working as intended, and producing the desired results. We will continue to review the qualitative aspects of the program as part of future FISMA audits and evaluations.

---

[1] See the following OIG reports: *Audit of the Board's Information Security Program,* dated September 2004; *Audit of the Board's Information Security Program,* dated October 2005; and *Audit of the Board's Information Security Program,* dated September 2006.

[2] See the following OIG reports: *Audit of the Supervision and Regulation Function's Efforts to Implement Requirements of the Federal Information Security Management Act,* dated September 2005; *Review of the Board's Implementation of Software Security Reviews,* dated May 2005; and *Report on the Audit of the Board's Implementation of Electronic Authentication Requirements,* dated March 2006.

Appendix 1 contains our analysis of the Board's progress in implementing key FISMA requirements. Appendix 2 lists the ten prior OIG audit recommendations related to information security that were not fully closed as of the beginning of our 2007 information security audit and their status based on our current audit work. As discussed in appendix 1, we determined that the Board's actions over the past year were sufficient to close seven of these recommendations. In appendix 1, we also summarize the work that we believe remains for each FISMA requirement and the reasons why audit recommendations, or portions of recommendations, remain open.

We provided our draft report to the director of the Division of Information Technology (IT), in her capacity as CIO for FISMA, and discussed the report's content with her and the Board's ISO at our closing meeting. During the meeting, the director generally agreed with the report's contents. She and the ISO also discussed ongoing and planned activities to further enhance the Board's information security program. Because our report does not contain any new recommendations, we did not request separate written comments.

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. Roger Cole
Mr. Peter Purcell
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 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 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:

Our 2006 information security audit work found that the ISO had developed or revised guidance to help implement the Board's information security program and that the ISO had worked with Board staff in divisions and offices to implement the guidance for systems under their control. However, we also noted that key guidance was in draft and that additional training for information and information system owners would help to ensure the program's effective implementation. We recommended that the CIO enhance the security program by finalizing security-related policies and providing additional training focused on the information security program and associated Board policies and NIST guidance.

During the past year, the ISO has continued to enhance the Board's information security program. In March 2007, the ISO updated the overall information security program document. The ISO also updated guidance for categorizing information and systems, conducting risk assessments, and developing security plans. In addition, the ISO finalized guides for certifying and accrediting systems, training personnel with significant responsibilities for information security, and handling security incidents. The Board is also finalizing procedures for handling PII which will supplement the policies outlined in the Board's recently issued *Information Classification and Handling Guide*.

Earlier this year, the IT security staff provided training sessions on the updated information security program to system development staff and system owners. The sessions included a review of the Board's information security processes and discussed the security-related roles and responsibilities associated with each process. The ISO plans to offer additional training. As a result of the actions taken to update and finalize the security-related policies and to provide associated training, we are closing our 2006 audit recommendation.

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. We will continue to review the need for additional guidance as part of our ongoing work related to information security. Given the programmatic changes over the past year, the CIO and ISO will also need to remain vigilant in monitoring compliance with the program's requirements and in evaluating the requirement for refresher training.

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 all 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:

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 legislative requirements and related information security policy and guidance. Work completed as part of our 2006 information security audit closed the first part of this recommendation, since the CIO had issued an inventory guide to provide additional guidance for classifying systems, and the ISO had worked with divisions to implement the guidance. During the past year, the ISO updated the guide and issued additional procedures for determining system types, bundling applications where appropriate, and documenting security requirements. In our opinion, the guidance provides a systematic approach for identifying and classifying systems to ensure that all Board information assets are properly identified and achieve the appropriate level of security as established by the Board's information security program. The Board also continues to report progress in certifying and accrediting information systems on the inventory. During the past year, for example, the Board completed a certification of the IT general support system (GSS). As part of the certification, the IT security staff completed a baseline control matrix for each component of the GSS (such as Windows Active Directory, UNIX, and the mainframe).

Our 2006 information security audit report also noted that the Board's inventory guide contained guidance to help the System identify and organize information assets operated by Reserve Banks under delegated authority from the Board. During the past year, we reviewed the System's progress for identifying and grouping applications, and believe that sufficient work has been done to close the open inventory-related recommendation from our September 2005 report, *Audit of the Supervision and Regulation Function's Efforts to Implement Requirements of the Federal Information Security Management Act*.

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 the Board's security program's requirements for all systems on the inventory; therefore, we are leaving the second part of our 2005 recommendation open until this work is completed. 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 minor systems are bundled into a GSS or major application, the ISO will also need to ensure that controls are properly documented, implemented, and tested to provide the appropriate level of security.

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 developments from OMB. Until the work discussed above is completed, we will continue to hold this recommendation open and will reassess its status at that time.

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:

Our 2006 information security audit work found that the director of IT had issued a policy on risk assessments, including a standard template, to assist divisions and offices in performing the assessments. The risk assessment guide and template

were updated in 2007, and system owners must complete a risk assessment in preparing for a system C&A.

Our March 2006 *Report on the Audit of the Board's Implementation of Electronic Authentication Requirements* included a recommendation that the CIO: (1) finalize electronic authentication (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. Last year, we partially closed the recommendation because the ISO had included e-authentication guidance as part of the risk assessment guide. Since that time, we have reviewed e-authentication assessments completed as part of updated system risk assessments and believe that sufficient action has been taken to close the remaining portion of this recommendation.

During 2005, we conducted a review of the Board's implementation of software security reviews and recommended that the CIO develop guidance to ensure that single purpose software and other software products are evaluated as part of a GSS; as part of an application security review; or on an individual basis, as appropriate. Subsequently, the ISO developed a template for completing software security reviews for commercial off-the-shelf (COTS) products, and IT staff conducted several reviews during the year. In addition, as part of the Board's security-related training, the ISO developed a set of frequently asked questions, which includes questions and responses related to implementation of software security reviews for COTS products. We believe sufficient work has been completed to close this recommendation.

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 noted above, the ISO updated bundling guidance for determining system types and documenting security requirements. Systems bundled under a major application must be included in the risk assessment for the major application. For minor applications bundled under a GSS, the guidance requires that system owners complete a risk assessment and certify to the ISO that the controls have been successfully implemented (either by the GSS or by the application itself). If certain controls have not been satisfied, the owners must either accept the residual risk or describe the risk mitigation process. As system owners implement the bundling guidance, the ISO will need to ensure that all systems are appropriately assessed for risk and for the magnitude of 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 Board.

The first two security control reviews that we conducted this year identified areas where we believe the ISO needs to provide additional guidance for completing

risk assessments, and we are providing our recommendation to the ISO under separate restricted cover. We will continue to review implementation of the risk assessment process as part of our future application control reviews.

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:

Last year, we noted that the ISO had developed new security plan templates for major applications, general support systems, and subsystems, and had required system owners to complete the appropriate template in preparation for certifying and accrediting their systems. During the past year, the ISO updated the security plan guidance and issued a revised control baseline template that includes all NIST SP 800-53 controls. The control baseline also includes suggested responses for each control in order to facilitate the system owner's completion of the baseline; however, every control must be reviewed to ensure that the suggested answers are correct, or are appropriately adjusted, and accurately describe how the control is implemented in the context of the specific system. As part of the IT GSS certification process, IT staff completed baselines for various components of the IT GSS which will provide a foundation for reliance by applications bundled under the general support system.

Work to Be Done:

Full implementation of the new security plan will not occur until all systems have been through a C&A. As minor systems are bundled into a GSS or major application, the ISO will need to ensure that security plans accurately describe the controls in place for all components within the GSS or major application, and that the certification provides the appropriate level of testing and verification to ensure that controls are in place and operating as intended. We will review completed security plans during future security control tests.

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 guaranteed 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, unless the system undergoes a significant change.

Progress to Date:

During the past year, the ISO finalized the Board's C&A guidelines. The guidance identifies roles and responsibilities for the C&A process, describes the required documentation, and discusses the various process phases. The guidance notes the importance of the post-accreditation phase, which includes configuration management and change control processes, continuous control monitoring (at both the information system and infrastructure levels), and annual security reviews. To help improve the Board's continuous monitoring processes, the ISO has documented the Board's vulnerability scanning environment (that is, the roles and responsibilities, and scanning tools currently used) and plans to further enhance scanning capabilities through automated tools. The ISO is also tracking the requirement for systems to undergo an annual security review in any year when the system is not subject to a C&A.

The table below shows the total number of Board general support systems, major applications, and third-party systems, and the number of systems that were certified and accredited as of September 20, 2007. The C&A process has been a high priority for the Board over the past year. As the table shows, the Board reports that most systems have completed C&As, and the ISO expects all but 6 systems to receive full authorizations to operate by the end of September. (The Board's inventory includes an additional 119 minor applications and subsystems; the inventory indicates that 62 of these additional systems have also completed the C&A process. Going forward, however, these systems will be included in the C&A for the GSS or major application under which they reside.)

			Accreditation Status		
Type of System	Total Number of Systems	Certification Completed	Full Authorizaon to Operate	Interim Authorization to Operate	No Accreditation Decision
Board General Support Systems	5	4	4	0	0
Board Major Applications	15	14	8	1	5
Third-Party Systems	43	42*	16	26	0

*The ISO has also performed a review of the Statement on Auditing Standards No. 70 report for the Federal Reserve System's outsourced contractor for retirement and benefit plan administration.

Work to Be Done:

During the past year, the OIG conducted an evaluation of the Board's C&A process and identified several areas of concern; we will provide our evaluation results to the CIO and ISO in a separate restricted report. In addition, as part of our security control review of a major application earlier this year, we reviewed the application's completed C&A package and identified weaknesses we believe should have been identified during the C&A process. Our ongoing security control review at FRB Boston will allow us to review the C&A work completed for third-party applications and evaluate the level of testing conducted as part of that process. As we complete other control reviews during the year, we will continue to compare our evaluation results with completed C&A packages, and we will provide the ISO with any additional recommendations for improving the Board's C&A process. We will also review implementation of the annual testing requirement for third-party systems (outside of the C&A process) so that we can close the remaining recommendation from our September 2005 report, *Audit of the Supervision and Regulation Function's Efforts to Implement Requirements of the Federal Information Security Management Act*.

Our security control review work to date has also identified concerns with the Board's configuration management process. We recognize, however, that the ISO is evaluating enhanced automation capabilities which we believe will improve this process. We will also monitor the Board's progress in enhancing configuration management processes as part of follow-up work on last year's control review reports.

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:

Our 2006 information security audit work found that the ISO had provided divisions and offices with additional guidance regarding the tracking and reporting of security-related issues, but that division-level reporting of performance metrics on outstanding issues was not always consistent from quarter-to-quarter. We noted that this issue could affect the roll-up of division-

level information to the overall Board POA&M which the CIO provides to OMB. During this past year, we found that divisions have more accurately tracked outstanding issues from one quarter to the next. Based on the guidance issued and the generally enhanced quality of the POA&Ms completed during the 2007 FISMA cycle, we are closing our recommendation.

Work to Be Done:

The ISO should continue to ensure that divisions accurately update their division-level information so that the POA&M functions effectively as an agencywide vehicle for tracking security-related issues and monitoring agencywide remediation efforts. We will continue to review quarterly submissions by the divisions to the ISO, as well as the ISO's submission to OMB.

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:

As part of security awareness and training, the Board continues to post security-related articles on its internal website. During the past year, these articles have covered password requirements and encrypting data on USB drives. IT's intranet website related to information security also includes links to security awareness articles from the past ten years. In addition, the Board administers an online security awareness quiz covering security articles posted during the year; the quiz also provides a mechanism for staff to provide feedback to the ISO. As noted earlier, the IT security staff conducted training sessions on the Board's information security program for development staff and system owners.

Our 2006 information security audit work identified individuals who we believed should have been designated as having significant security responsibilities and who, in our opinion, had not received the proper level of training. We recommended that the CIO provide additional guidance for designating individuals with significant security responsibilities and identify specific training requirements. During the past year, the ISO issued guidance for designating individuals with significant security responsibilities. The guidance, which is an appendix to the Board's information security program document, includes categories of individuals that meet the definition of having significant security responsibilities and identifies the levels of knowledge appropriate for each category. This action is sufficient to close the recommendation.

Work to Be Done:

Given the volume of updated guidance issued over the past year, the ISO should evaluate the need for additional training over the coming year. As NIST and OMB issue new guidance, and the Board incorporates this guidance into its information security program, the ISO will need to consider refresher training on a regular basis. In addition, the ISO will also need to monitor actions taken in response to the recent guidance for designating individuals with significant security responsibilities to ensure that the guidance is implemented consistently for Board staff, and that Reserve Bank staff responsible for systems supporting delegated functions meet comparable requirements. As with other areas contained in the FISMA legislation, 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.

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.[3]

Progress to Date:

Our 2004 information security audit work found that the ISO was not reporting all levels of incidents that are required to be reported to the US-CERT; our audit report included a recommendation 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. Earlier this year, the ISO issued a new *Information Security Incident Handling Policy* that includes requirements to report all levels of incidents. Over the past year, we have reviewed incidents reported by the ISO to US-CERT and found that the reports include incidents at the Board and the Reserve Banks. To inform employees of their responsibilities, the ISO has also posted articles on this topic on the Board's website as part of security awareness training. We believe sufficient action has been taken to close the recommendation.

[3] 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.

To comply with new OMB privacy-related requirements, the Board's Legal Division (Legal) has drafted a data breach notification policy and is finalizing PII procedures. The ISO has also identified applications on the Board's inventory that contain PII and sensitive data. To supplement the Board's policy, the Division of Banking Supervision and Regulation (BS&R) and the Division of Consumer and Community Affairs issued additional guidance for safeguarding and reporting a loss of confidential information that includes PII. Earlier this year, we began an inspection with the objective of evaluating policies, procedures, practices, and controls to safeguard PII that is collected during examinations conducted by Federal Reserve Banks under the Board's delegated authority. We will provide the results of our inspection to Board management once our fieldwork is completed.

Work to Be Done:

This year's OMB reporting requirements ask the IGs to evaluate their agency's processes related to PIAs. Our initial work in this area found that the Board has completed four assessments and posted the documents to its public web page. The security control baseline issued earlier this year contains a requirement for system owners to either complete a PIA as part of the planning process or obtain a determination from Board Legal that a PIA is not required. However, guidance for completing the assessment is still in draft. Legal staff also informed us that BS&R is performing a Systemwide review of systems supporting the supervision and regulation function to identify additional systems that may require an assessment (although BS&R is determining whether similar systems may be combined under one umbrella assessment). In addition, our control review of one major application found that a PIA had not been completed, although the system owners are presently working with Legal to comply with the assessment requirement. As we complete the fieldwork necessary to respond to OMB's reporting requirement, we will report any additional areas of concern to appropriate officials.

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 which systems have been tested. The Board recently expanded the contingency testing to include a separate, full-day senior management exercise at the Board's contingency site. In addition, divisions were

requested to supplement their contingency planning documents to address the avian flu threat. As part of that update process, the Staff Director for Management requested that divisions review and confirm critical business functions and evaluate technical requirements, such as remote access capabilities.

Work to Be Done:

We shared our observations from prior 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. 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 do not become too "routine" or that participants do not become complacent. We will continue to monitor the contingency tests as part of our ongoing FISMA work, and anticipate performing focused audit or evaluation work in this area over the coming year.

Appendix 2 – Updated Status of Prior OIG Information Security Audit Recommendations

The following tables list the recommendations that were not fully closed at the time of our 2007 audit. The first column lists the original recommendation(s) from each report cited. In the status column, we note the current status of each recommendation as discussed in appendix 1.

2004 *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.	Closed (see discussion in appendix 1, page 13)
We recommend 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]	Closed (see discussion in appendix 1, page 15)

2005 *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 (see discussion in appendix 1, page 8)
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 (see discussion in appendix 1, page 9)

[4] At the time of our audit recommendation in 2004, US-CERT had established only four priority levels. During 2005, 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 *Audit of the Supervision and Regulation Function's Efforts to Implement Requirements of the Federal Information Security Management Act*

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.	Closed (see discussion in appendix 1, page 9)
We recommend that the CIO issue guidance for conducting information security reviews that includes specific requirements for control testing.	Partially Closed (see discussion in appendix 1, page 13)

2005 *Review of the Board's Implementation of Software Security Reviews*

Original Recommendation	Status
We recommend the CIO develop guidance to ensure that single purpose software and other software products are evaluated as part of a general support system, as part of an application security review, or on an individual basis as appropriate.	Closed (see discussion in appendix 1, page 10)

2006 *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.	Closed (see discussion in appendix 1, page 10)

2006 *Audit of the Board's Information Security Program*

Original Recommendation	Status
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.	Closed (See discussion in Appendix 1, page 7)
We recommend that the CIO provide additional guidance for designating individuals with significant security responsibilities and identify specific training requirements.	Closed (see discussion in appendix 1, page 14)

Appendix 3 – Principal Contributors to this Report

Peter Sheridan, Senior IT Auditor and Auditor-in-Charge

Richard Allen, IT Auditor

Robert McMillon, Senior IT Auditor

Satynarayana-Setty Sriram, IT Auditor

William Mitchell, Assistant Inspector General for Audits and Attestations