

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

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



---

**OFFICE OF INSPECTOR GENERAL**

---

October 2005





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

OFFICE OF INSPECTOR GENERAL

October 6, 2005

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 three applications running primarily on the Board's Unix and Linux platforms and followed up on open issues from our 2004 application control reviews. Because this year's reporting guidance from the Office of Management and Budget (OMB) requires IGs to include applications operated by contractors or other sources in their sample of systems selected for control reviews, we also reviewed controls over one application maintained by the Federal Reserve Bank of Philadelphia in support of the Board's Supervision and Regulation (S&R) function. We performed our application control testing based on criteria in the National Institute of Standards and Technology (NIST) Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems* (SP 800-26). We also reviewed configuration settings for selected Board-maintained hardware such as servers, workstations, and routers.

Our control tests did not identify any significant security control deficiencies, although we found areas where controls could be strengthened. Given the sensitivity of the issues involved with these reviews, we have provided the specific results to management under separate restricted cover. Follow-up work on our 2004 application control reviews allowed us to close all outstanding recommendations. Our review of security settings found that the Board has enhanced the processes for establishing, monitoring, and remediating security settings. However, we identified additional improvement opportunities which we are also providing to management under separate restricted cover.

To evaluate the Board's compliance with FISMA and related policies and procedures, we followed up on the open recommendations in our 2004 information security audit report.<sup>1</sup> We also compiled information on, and reviewed the Board's processes related to, areas for which 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, remedial action monitoring, and incident response. FISMA also 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. Consequently, we also incorporated the results from our earlier audit of the Federal Reserve System's (System) efforts to implement FISMA requirements for applications operated by the Reserve Banks in support of the Board's delegated S&R function.<sup>2</sup>

Our follow-up work showed that, over the past year, the Board has continued to make progress in developing and implementing a structured information security program as outlined by FISMA and has taken actions to address the areas discussed in our 2004 audit report. Specifically, we found that the Board has developed a process to evaluate the effectiveness of its security awareness and training program and has identified system interfaces as part of the Board's application inventory; as a result, we are closing our related recommendations. The Board has also made improvements in tracking remedial actions and conducting application security reviews. Because several of these improvements are still in process, we are leaving our remaining recommendations open and will continue to review actions taken as part of our ongoing work related to information security. More specific information regarding each of our prior year recommendations can be found at appendix 1.

Despite this progress, however, we found that the Board has not yet identified all information and information systems supporting its operations and assets, or fully implemented information security requirements for applications maintained by third parties. We also found that the Board's overall governance structure for information security has been ineffective in establishing, monitoring, and enforcing compliance with information security requirements. Each of these areas, and our associated recommendations, are addressed below. As part of our audit work, we also reviewed recent NIST guidance and the Board's progress towards incorporating this guidance into its revised information security program. While we do not have any specific recommendations at this time, the final section of our report discusses several areas of concern for the Board to consider as it continues to implement the revised security program.

- 1. 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.**

---

<sup>1</sup> See our *Report on the Audit of the Board's Information Security Program*, dated September 2004.

<sup>2</sup> 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.

FISMA applies to information and information systems used or operated by the agency, or by contractors and other organizations and sources on behalf of an agency. Other organizations could include contractors, grantees, state and local governments, and industry partners.

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, including those not operated by or under the control of the agency. 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.

In 2004, the Board reported an application inventory of 145 systems, including 65 systems maintained by the Reserve Banks. The Reserve Bank systems were identified through an initiative of the Division of Banking Supervision and Regulation to work with the Reserve Banks to implement FISMA for systems supporting the Board's S&R mission. Our audit report on these implementation efforts concluded that the Reserve Banks had not consistently followed guidance in identifying applications. We also found that the Reserve Banks' general support systems were excluded from the application inventory, even though the support systems provide baseline controls for the applications which they support. Our report contains a recommendation to establish a more consistent approach for identifying systems supporting the S&R function.

Beyond the concerns addressed in that report, however, we found that the Board has yet to fully identify the scope of information and information systems within the Federal Reserve System—other than the S&R business function—to which the legislation applies. Because FISMA applies to information systems used or operated by a contractor or another organization on behalf of an agency, all systems meeting this definition must be included in the agency's information security program. Thus, the Board's information security program should be applied to information and information systems that support the Board's other functional areas, including the monetary policy function, research activities, or the Reserve Bank oversight function. As we have noted in previous FISMA reports, establishing an accurate application inventory is critical to effectively implementing other FISMA requirements, such as control reviews and certifications and accreditations. Beyond just identifying systems, however, establishing a complete inventory also requires accurately identifying the system boundaries and all interfaces with other systems to provide proper end-to-end coverage of security requirements.

Once the inventory is established, the Board must apply the components of its information security program—to include establishing requirements for performing risk assessments, developing security plans, testing security controls, and tracking corrective actions—to those systems, as it has with Board-operated applications. Our audit report regarding FISMA's implementation within the S&R function made recommendations in several of these areas.

FISMA requires each agency to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or maintained by another agency, contractor, or other source. In its 2005 reporting guidance, OMB clarified agency security responsibilities for contractors and other sources. For

example, OMB's guidance states that for contractors acting as service providers (i.e., outsourced operations), agencies are responsible for ensuring that all FISMA and related policy requirements are implemented and reviewed. The guidance also states that agencies must ensure that identical, not "equivalent," security procedures are implemented and that these procedures explicitly meet NIST guidance. The guidance provides similar requirements for contractor support and Government-Owned/Contractor-Operated facilities. We do not believe that the Board should impose any less of a standard on the Reserve Banks—which operate systems on behalf of the Board—than OMB expects from third-party service providers or other contractors.

To ensure that the requirements are understood by all affected parties throughout the System, the Board should revise its information security program document to communicate the agency's information security policies for all information systems supporting the Board's operations and assets. The revised security program document should clearly establish (1) the applications that are to be included on the Board's FISMA inventory, (2) the specific security expectations for all applications, and (3) the process for monitoring compliance with the information security program's requirements. We found that absent definitive Board policies, other System entities have issued guidance and direction. For example, both a working group involved with implementation of the new Information Security Manual and a legal working group have issued position papers on FISMA applicability at the Reserve Banks. In our opinion, the additional guidance and direction developed by these working groups fails to properly apply FISMA and the Board's information security program to Reserve Bank systems supporting Board activities. We believe that the Board, as the agency directly subject to FISMA and whose information and information systems are at risk, must be the decision-maker for establishing the applicability of FISMA to systems maintained in support of its operations and assets.

Until the Board establishes firm requirements for the Reserve Banks, we are concerned that the Banks will continue to use information security processes that do not provide the same level of assurance as the processes envisioned by FISMA and required by NIST guidance. While current Reserve Bank processes—such as the new Risk Management Process (RMP)—share similar objectives with FISMA, they differ in their approach to information security protection as well as the extent to which NIST standards are applied. For example, FISMA requires compliance with recommended security controls (a philosophy of risk avoidance) while the RMP permits Reserve Banks to select among security controls to mitigate risks (a philosophy of risk management). FISMA also requires the agency to test security controls at least annually, while the RMP has no similar requirement. Finally, NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (SP 800-37), requires that an independent certification agent test the operational, managerial, and technical controls protecting an application as part of the certification and accreditation process; this requirement is absent in the RMP. Taken together, we believe that the current Reserve Bank approach to information security provides a less robust process than the Board is required to apply to applications it maintains, thus failing to meet legislative requirements.

- 2. 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.**

In June 1999, the Administrative Governor designated the Staff Director for Management as the Board's CIO. In our 2003 *Report on the Audit of the Board's Information Security Program*, we recommended that the Administrative Governor establish a full-time CIO position and clearly articulate the CIO's wide array of responsibilities, including those related to information security. In response, the Staff Director delegated to the Director of the Division of Information Technology (IT) certain functions pertaining to FISMA and E-Government. Although we closed our recommendation based on the executed delegation, we raised concerns in our 2003 report as to whether a partial delegation would be effective or whether it would create confusion as to who had responsibility for which particular CIO-related functions. We also questioned whether the IT director was the most effective position for establishing Boardwide policies and ensuring compliance with FISMA, given that the director's operational responsibilities could create the appearance of a conflict of interest with the broader oversight role.

Based on our ongoing audit work related to information security, we believe the Board's current FISMA governance structure has been, and will continue to be, an ineffective structure for implementing the Board's information security program and complying with legislative requirements. In our opinion, the Board's CIO for FISMA and the ISO (an assistant IT director) lack the organizational placement, authority, and independence necessary to effectively establish, implement, monitor, and enforce information security requirements for all information and information systems supporting Board operations and assets, including systems maintained by the Reserve Banks. While we believe that the legislation provides sufficient authority for the Board's CIO for FISMA and the ISO to establish these requirements, we recognize that the Board's decentralized, collegial operating environment differs from the structured, top-down framework for information security management envisioned by FISMA, and that the structure of the Federal Reserve System—in which System IT staff and resources do not directly report to the Board—further complicates establishing such a framework. However, implementing the first recommendation in this report can, in our opinion, only be accomplished by establishing an effective governance framework.

We are also concerned about the ongoing workload requirements of the current CIO for FISMA and the ISO, and the conflict that their operational duties creates with the broader FISMA policy and enforcement responsibilities. As division director, the CIO for FISMA has significant responsibilities for managing the Board's infrastructure, overseeing application development, managing the IT division budget, and providing other information technology-related services. The ISO currently has the policy and enforcement activities outlined in FISMA, as well as day-to-day operational information security responsibilities. In our opinion, ongoing information security requirements—from an operational perspective—are likely to increase as technology evolves and the corresponding threats continue to mature. In addition, responses from the CIO for FISMA and the ISO to recent audit recommendations regarding information

security compliance have highlighted the conflict between establishing security requirements and the operational obligation (budget, staffing, time) of implementing such requirements.

We note that the issue of information security responsibilities was recently discussed within the System. Specifically, a work group formed under the System's Information Technology Oversight Committee recently contracted for a study of information technology governance. The study, which did not address FISMA requirements or include Board activities, concluded that there is a general lack of clarity regarding information technology governance within the System. In our opinion, this conclusion would have been even more pronounced if the difficulties of implementing FISMA (e.g., defining requirements and monitoring compliance) had been included in the study's scope.

To address these concerns, we believe the Board should establish an independent, full-time CIO and ISO to provide the organizational stature necessary to overcome cultural and operational hurdles in implementing FISMA's requirements throughout the System. The Board should clearly define the information security responsibilities for these individuals related to all technology resources and activities supporting Board operations and assets, regardless of whether the resources and activities belong to a Board division, a Reserve Bank, or another third party. We believe the Board should also delegate to the newly-established CIO any additional CIO responsibilities currently retained by the Staff Director in order to place with one individual all related functions stemming from various laws, regulations, and executive orders. In addition, the Board should ensure that the CIO and the ISO have the resources and authority necessary to establish policy, provide guidance, and enforce compliance. In establishing an independent CIO and ISO, however, we believe the Board should leave any day-to-day operational responsibilities related to information security within IT to provide an appropriate separation of duties.

## CONTINUING CHALLENGES

Our 2004 information security audit report discussed guidance developed by NIST that we believed would require the Board to fundamentally redesign many of its information security processes to remain consistent with applicable standards.<sup>3</sup> Since then, the Board's ISO has developed a new information security program and related processes based on NIST guidelines and standards; the revised program covers each of the areas discussed in our 2004 report. As a first step in implementing the program, the ISO has worked with divisions and offices to identify and categorize Board information and the related information systems as outlined in NIST's Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. Agencies must categorize their information and information systems as either high, moderate, or low in order to determine which security controls should be implemented. The FIPS 199 assessment thus forms the basis of ensuring information and information systems are provided the appropriate level of information security. The Board completed the FIPS 199 impact assessments for all Board information and

---

<sup>3</sup> FISMA assigned to the Director of OMB the responsibility for establishing government-wide policies for the management of information security programs. FISMA also tasked NIST to develop related standards and guidelines.

information systems in September 2005. Additional phases of the ISO's revised program include updated security plans, risk assessments, and certifications and accreditations. The current implementation timeline projects that the revised program will be fully implemented for major applications by September 2006; the ISO has projected that all non-major systems will be transitioned by 2007.

In our opinion, the ISO's implementation timeline fails to meet OMB and NIST expectations. Statements by OMB officials, for example, indicate that FIPS 199—which was issued with an effective date of February 2004—should have been implemented one year after issuance. The Board began planning for FIPS 199 implementation in late 2004 and completed the assessment last month. In addition, the NIST guidance for performing system certifications and accreditations (SP 800-37) is effective for all systems placed into production after the publication's effective date of May 2004. The Board, however, has not yet adopted the NIST process; certifications and accreditations for major applications are currently scheduled to be performed between September 2005 and the end of 2006. Our informal discussions with other agencies found that while they are also in the process of implementing FIPS 199, they have already adopted certification and accreditation processes more closely aligned with NIST guidance. In addition, OMB's reporting guidance requires agencies to report performance metrics—including metrics for systems maintained by third parties—not only in terms of FIPS 199 categories, but also in terms of statistics for system certification and accreditation.

Based on our review of the Board's implementation schedule, we are also concerned that the timetable does not include any Reserve Bank applications. According to the Board's CIO for FISMA, the Board has adopted a phased-in approach to applying FISMA's requirements to the Reserve Banks. The ISO told us that he plans to focus on implementing the program at the Board before incorporating the Reserve Banks into the program. Since Reserve Bank applications that support the Board's S&R function comprised about 50 percent of the Board's reported inventory as of August 2005, we believe it is important that the Board ensure Reserve Bank systems on the Board's inventory are incorporated into the process as it develops, rather than waiting until the revised program is fully implemented at the Board. In our opinion, including the Reserve Banks in the implementation process now will help gain broader acceptance of adopting new requirements and processes as the program's implementation progresses, as well as identify any implementation hurdles at the Banks.

## **ANALYSIS OF COMMENTS**

We provided our draft report to the Director of IT in her capacity as CIO for FISMA for review and comment. Her response is included at appendix 2. The director shares our belief that the Board should identify all information collected and maintained and all information systems used or operated by the Board or on its behalf. The director also recognizes that the appropriate authority and controls need to be in place to facilitate the effective implementation and continued compliance with FISMA. The director's response generally agrees with the intent of our recommendations and identifies actions that the Board plans to implement as part of its information security activities. Specifically, the director's response states that the Board plans to perform a more comprehensive review to identify all information and information systems used

by the Board and determine whether or not that usage falls within FISMA's legislative requirements. Once that analysis is complete, the director indicates that the Board will reevaluate our recommendation regarding information security governance and make changes as appropriate in light of the final inventory and any additional developments from OMB. We will review these actions as part of our ongoing 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/*

Barry R. Snyder  
Inspector General

Enclosures

cc: Mr. Stephen Malphrus  
Ms. Marianne Emerson  
Mr. Raymond Romero

## **APPENDIXES**



## **Appendix 1 – Analysis of Action Taken on 2004 Audit Recommendations**

### **Original Recommendation 1.**

**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.**

#### **Basis for the Original Recommendation**

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 (GAO) 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 update to OMB.

In analyzing the Board’s POA&M process during our 2004 audit, we found that the information provided by the divisions was insufficient to ensure that all weaknesses had been identified, were properly tracked, and were corrected in accordance with established milestones. During our audit, we also found that weaknesses and corrective actions in the divisions’ POA&Ms—when the weaknesses and actions were identified—were not included in the Board’s overall POA&M. In addition, we found that weaknesses identified on reviews other than FISMA-related control reviews or other information security efforts, such as penetration tests, vulnerability scanning, emergency preparedness initiatives, and infrastructure protection issues were not included in the Board’s POA&M.

#### **Actions Taken**

The ISO has taken steps to provide divisions with additional guidance regarding the tracking and reporting of security-related issues. The new guidelines were finalized and implemented in November 2004. A separate section was also added to the POA&M form for tracking enhancement efforts, in addition to reporting security-related issues.

#### **Analysis of Actions Taken**

The additional guidance issued by the ISO is sufficient to address the first part of our recommendation. Although divisions and offices have improved processes for prioritizing, tracking, and addressing information security issues via the POA&Ms, we identified several exceptions:

- FISMA application review issues were not reflected on the applicable POA&Ms for two divisions.
- A security weakness identified outside the FISMA-control review process was never reflected on the division's POA&M.
- Division-level reporting of POA&M 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.

We believe more time is needed for the process to mature so that divisions and offices accurately report all security-related issues and consistently report quarterly performance metrics. The ISO may want to establish a follow-up process to ensure this requirement is accomplished.

### **Status of the Recommendation**

**Partially Closed**

---

### **Original Recommendation 2.**

**We recommend the CIO establish a process to develop feedback on the effectiveness of the Board's security awareness and training program.**

### **Basis for the Original Recommendation**

FISMA requires an agency's information security program to 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.

Although the Board had established a security awareness and training program in compliance with FISMA requirements, we believed the program could be enhanced by developing and implementing a monitoring and feedback process to ensure the program is working as intended. As noted in NIST guidance on building an information technology security awareness and training program, continuous improvement should always be the theme for security awareness and training initiatives. Once a program has been implemented, processes must be put into place to monitor compliance and effectiveness. Formal evaluation and feedback mechanisms are critical components of any education program. We felt that a feedback mechanism would provide the ISO with information to fine-tune training requirements, add or delete material, and modify the implementation method as required. The feedback might also identify courses which could become baseline requirements for all individuals with particular security responsibilities (e.g., network administrators or application developers).

### **Actions Taken**

Since our previous audit, IT has issued fourteen information security articles and alerts to assist Board employees and contractors with information security awareness. Questions on the annual security quiz relate to the information security articles posted on the Board's intranet, and the ISO established an automated process to capture metrics for the quiz such as the percentage of employees who answered each question correctly. In addition, the ISO added survey questions to capture employee and contractor input on whether the quiz was useful. The ISO told us that he also assessed the security awareness component of the Board's new employee orientation process and identified potential changes. For example, he is working with the Management Division to test new employees on the information security training provided during orientation. The ISO has also proposed a "take away" package for new employees, including items such as the Board's permissible use and privacy policies, to reinforce training.

### **Analysis of Actions Taken**

The continued release of security awareness articles, the new security quiz tracking process, and the proposed new employee training activities are sufficient to close this recommendation.

### **Status of the Recommendation**

**Closed**

---

### **Original Recommendation 3.**

**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.**

### **Basis for the Original Recommendation**

Our analysis of control reviews performed by consultants hired by IT found that the reviews did not include detailed testing. Rather, the consultants primarily reviewed system documentation and interviewed system owners and technical support staff. During our audit last year, we also reviewed the process for conducting control reviews by Board staff in divisions other than IT. For these reviews, we found an inconsistent level of reporting or retention of supporting documentation. For example, staff performing the reviews in one division did not document the steps performed or produce a report at the completion of the control review. Instead, they simply made notes on any security weaknesses identified and then held the reviews open until any issues identified were resolved. Although the process outlined by these individuals was consistent with OMB and NIST requirements, without adequate supporting documentation, the CIO for FISMA and ISO have no assurance that the reviews are properly or consistently conducted. In our opinion, holding a review open until all issues are resolved precluded the division from providing timely feedback to the ISO. The lack of a formal report—identifying weaknesses found and corrective actions taken—also reduced the ISO's ability to effectively identify security issues on a Boardwide basis and minimized the effectiveness of the POA&M process for tracking and prioritizing corrective actions.

## **Actions Taken**

As we noted in our report last year, the ISO hired an analyst whose responsibilities include performing security reviews. The analyst developed review programs based on NIST SP 800-26; the programs include the seventeen critical element categories contained in NIST SP 800-26. The analyst also established testing requirements to be performed during the reviews. The programs and testing requirements were distributed to those divisions that perform their own security control reviews.

## **Analysis of Actions Taken**

The guidance issued by the ISO for conducting control testing is sufficient to address the first part of our recommendation. We examined six reviews completed by the IT security analyst and found that the review program was followed and that documentation was retained. However, those divisions that perform their own reviews were finalizing their reviews as of the completion of our audit fieldwork. Although division representatives informed the ISO that they were following the appropriate review programs, we were unable to substantiate the process or determine whether adequate documentation was prepared. We plan to evaluate the completed reviews to ensure that established guidance was consistently followed; based on that evaluation, we anticipate closing this recommendation.

## **Status of the Recommendation**

### **Partially Closed**

---

## **Original Recommendation 4.**

**We recommend that the CIO (1) expand the inventory of applications and systems to include the identification of the interfaces between each system and (2) coordinate the reporting of applications for FISMA purposes with other reporting responsibilities.**

## **Basis for the Original Recommendation**

The Board's ISO worked with representatives of the Information Security Committee to refine and update the inventory for Board-maintained applications. He also expanded the inventory to include third-party systems maintained by contractors as well as systems maintained by the Reserve Banks in support of the Board's delegated S&R function. We found, however, that the Board's inventory did not include the interfaces between each system and all other systems or networks as required by FISMA. While we noted that this information may be contained in other security-related documents such as application security plans, we believed that the information should be consolidated on the Board's application inventory not only to achieve compliance with FISMA and OMB requirements, but also to facilitate upcoming changes to the Board's risk assessment and certification processes.

Our 2004 review of the Board's inventory also found that not all applications listed as "critical assets" for either critical infrastructure protection or contingency planning purposes were classified as major applications on the FISMA inventory. For example, one application listed as

mission-critical for critical infrastructure reporting is classified as “other” in the Board’s inventory; the “other” classification means the application has no security requirements beyond those provided by its general support system. Similarly, we found applications designated in divisions’ continuity of operations plans as critical assets for contingency recovery purposes were classified as “other” applications for FISMA reporting purposes. While we recognized that the definition of a system’s criticality varies depending on the controlling law or implementing guidance, we believed that there needed to be a rationalization and harmonization between the Board’s FISMA inventory, its critical infrastructure protection plan, and the divisions’ contingency plans to accurately comply with the OMB requirement of appropriately identifying system criticality and risk levels.

### **Actions Taken**

The ISO updated the Board’s FISMA inventory template for divisions to identify internal and external system interconnections. The ISO told us that interface information should be updated based on the annual security control reviews. Regarding the coordination of reporting for FISMA with other reporting responsibilities, the CIO for FISMA did not agree that further coordination was needed. The ISO reviewed possible exceptions to the FISMA reporting and did not identify any required changes.

### **Analysis of Actions Taken**

Information security staff updated the inventory with interconnection information based on completed control reviews and analysis of application security plans. Our review of information provided by the ISO showed that the inventory has been substantially updated. We are therefore closing this portion of the recommendation.

Although the CIO for FISMA did not agree with our recommendation on coordinating the reporting of applications for FISMA purposes with other reporting responsibilities, the ISO nevertheless reviewed the various reporting requirements and determined that changes to the inventory were not required. One of our concerns last year was that applications identified as critical from a contingency or infrastructure perspective may require availability controls beyond those provided by the general support system. Although no inventory changes were made based on the ISO’s review, we note that the Board recently performed impact assessments for all of its information and information systems based on confidentiality, integrity, and availability; the resulting rating of high, moderate, or low in each of these categories will guide the selection of controls required for each application. Because controls will now be identified and reviewed for all applications based on FIPS guidance, we are also closing this portion of the recommendation.

### **Status of the Recommendation**

**Closed**

---

**Original Recommendation 5.**

**We recommend the CIO expand the Board's reporting of security incidents to include all four incident priority levels as well as incidents that occur at the Reserve Banks and other third-party contractors.**

### **Basis for the Original Recommendation**

FISMA requires agencies to develop procedures for detecting, reporting, and responding to security incidents. The procedures should include mitigating risks associated with such incidents before substantial damage is done; notifying and consulting with the Federal Computer Incident Response Center (FedCIRC)/United States Computer Emergency Readiness Team (US-CERT); and notifying and consulting with appropriate law enforcement agencies and relevant OIGs. FedCIRC/US-CERT has also established requirements for incident reporting, to include priority levels for categories of incidents and the timeframes for reporting each priority level.

Although the Board's incident reporting process included procedures for escalating incident reporting within the Board as well as for reporting to the appropriate government agencies, law enforcement agencies, and the OIG, we found that the Board was only tracking and reporting incidents for two of the four priority levels established by FedCIRC/US-CERT. The ISO told us that the Board's process is based on NIST guidance which provides a narrower definition of an incident than FedCIRC/US-CERT. We believed, however, that incorporating the remaining priority levels into the Board's reporting process was necessary to be in compliance with current reporting requirements; OMB stated they expected all incidents to be tracked and reported. Although FISMA tasked NIST to provide definitions and guidance on identifying and handling security incidents, the reporting requirements at the time of our audit had been established by FedCIRC/US-CERT. We also believed the CIO needed to develop a mechanism for coordinating incident reporting with contractors or other third parties, especially for any Reserve Bank systems processing information on behalf of the Board.

### **Actions Taken**

During 2005, US-CERT revised their reporting guidelines to be consistent with NIST and established five reportable categories. The ISO has continued to track security incidents, but only those in categories 1, 2 and 3. (Category 4 covers incidents related to "improper use" and category 5 is for "Scans/Probes/Attempted Access.") The ISO feels that category 4 is very broad and that not all violations of acceptable computing use policies rise to the level of a security incident. In the case of category 5, the ISO feels that collecting and reporting all unsuccessful attempts to access systems, scans, and probes would be very costly. The ISO recommended alternative approaches to the Department of Homeland Security, which is responsible for US-CERT. The ISO also informed us that he has not yet issued formal instructions for incident reporting to the Reserve Banks or other third-party contractors and service providers, although he receives daily logs from the System's National Incident Response Team identifying incidents throughout the Federal Reserve System.

### **Analysis of Actions Taken**

GAO recently reported that governmentwide guidance has not been issued to clarify which incidents agencies should report, and how and to whom the report should be made. Our preliminary contact with US-CERT, however, found that US-CERT expects agencies to report incidents in categories 1 through 4. Our contact also indicated that reporting category 5 is voluntary, although US-CERT encourages agencies to report incidents in this category to identify emerging cyber-security threats and raise federal cyber-situational awareness. We will continue to work with US-CERT and other government officials to identify definitive reporting requirements and ensure that the Board is complying with those requirements. In addition, the ISO needs to issue formal instructions or procedures for third-party contractors and service providers covering incident reporting.

### **Status of the Recommendation**

**Open**



## Appendix 2 – Division Director’s Comments

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

# MEMO

DATE: October 3, 2005  
TO: Mr. Barry R. Snyder  
FROM: Marianne Emerson /signed/  
SUBJECT: Comments on the Office of the Inspector General’s 2005 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 concur with your view that we have a strong program without any significant security control deficiencies. Indeed, there have been no intrusions, security breaches or unauthorized use of Board information or services during the reporting period. We continue to strengthen our automated configuration and patch management processes to protect our systems from viruses and unauthorized use. We continue to add new security safeguards, such as intrusion prevention systems, to protect our systems from evolving threats. Also, as you noted, we strengthened our security awareness program, helping to ensure that all Board employees and contractors know what to do to protect the Board’s information. Further, we are taking steps to implement the recent Office of Management and Budget (OMB) requirements to assure that the Reserve Banks protect Board information and information systems. In this respect, the Reserve Banks have strong risk-based information security programs that, among other elements, include periodic assessments of risk, awareness training, contingency planning, periodic vulnerability and penetration testing, and processes for remedial action. For example, federal intelligence agencies have characterized Fedwire security as “best corporate practice.”

In evaluating the effectiveness of a security program, we believe it is important to recognize that FISMA includes cost as a consideration in the risk decision. FISMA as well as the National Institute for Standards and Technology (NIST) guidance, allows for making prudent, cost-effective information security risk decisions for information systems. For example, FISMA states that federal agencies are responsible for “providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information...”. Further, the guidance permits the agency to consider risk on a broader perspective. NIST 800-53, which provides guidance on information security control selection, states that “...The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program that involves the management of organizational risk—that is, the

risk associated with the operation of an information system. The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system—the security controls necessary to protect the operations and assets of the organization.”

In addition, we believe it is important to recognize the changing nature of OMB's direction for implementing FISMA. In this regard, on June 13, 2005, OMB made a significant change between the rules published for comment and its final rules that fundamentally altered the requirements applicable to third party contractors. When OMB stated that it requires that “identical” not “equivalent” processes be applied to systems operated on behalf of agencies, we had already completed most of our third party evaluations. For clarity of communication and to make a more cost-effective implementation of FISMA, the Board defines its year for FISMA purposes as starting on October 1 of a year and ending on September 30 of the next year. This approach allows us to implement the complex and pervasive systems and processes required by FISMA in a deliberate and efficient manner that enhances the quality of our security program. To avoid confusion and disruption, we implement changes in OMB guidance at the start of the next operational year. Thus, OMB's June 2005 guidance on third party contractors, which was issued nearly three-quarters through our 2005 operational cycle, will be implemented beginning in October 2005. To have implemented the changes immediately would have caused confusion and disruption of planned program implementation already underway.

Following are our responses and comments for the audit report's specific recommendations. Each recommendation is set forth in bold face below, accompanied by our comments, which refer not only to the recommendations themselves, but also to the accompanying justification language in the audit.

**Recommendation 1: We recommend that the Board identify all information and information systems supporting its operations and assets, including those at the Reserve Banks and other third parties, and ensure full and timely compliance with FISMA's legislative requirements and related information security policy and guidance.**

Response: We share the belief that the Board needs to identify all information collected and maintained and all information systems used or operated by the Board or on its behalf. While we already have a complete inventory of information and information systems that we operate at the Board and those operated on our behalf at the Reserve Banks as part of the bank supervisory function, we will perform a more comprehensive review to identify all information and information systems used by the Board and perform an analysis to determine whether or not that usage falls within FISMA's legislative requirements, once the General Counsel issues his legal opinion regarding the applicability of FISMA to third parties.

**Recommendation 2: We recommend that the Board establish full-time independent 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.**

Response: We believe that the Board's assignment of management responsibilities is designed to facilitate the effective implementation and continued compliance with FISMA's requirements and recognize that the appropriate authority and controls need to be in place. As with all

developing programs, we will however continue to evaluate and make changes as appropriate to our organizational structure in light of the developments from OMB and progress on implementing the review and analysis of the inventory outlined in Recommendation 1. We will reevaluate this recommendation once the work on Recommendation 1 is complete.

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

**Appendix 3 – Principal Contributors to this Report**

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

Richard Allen, EDP Auditor

Gerald Edwards, Auditor

Timothy Rogers, Auditor

Peter Sheridan, Senior EDP Auditor

Alvaro Soto, Auditor

William Mitchell, Assistant Inspector General for Audits and Attestations