

Board of Governors of the Federal Reserve System

**AUDIT OF THE SUPERVISION AND
REGULATION FUNCTION'S EFFORTS TO
IMPLEMENT REQUIREMENTS OF THE
FEDERAL INFORMATION SECURITY
MANAGEMENT ACT**



OFFICE OF INSPECTOR GENERAL

September 2005



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

OFFICE OF INSPECTOR GENERAL

September 9, 2005

Mr. Stephen Malphrus, Staff Director for Management
Mr. Richard Spillenkothen, Director
Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Messrs. Malphrus and Spillenkothen:

The Office of Inspector General (OIG) is pleased to present its *Report on the Audit of the Supervision and Regulation Function's Efforts to Implement Requirements of the Federal Information Security Management Act (FISMA)*. We began this audit as part of an effort to perform work throughout the year related to our independent evaluation responsibilities under FISMA. Our objectives were to evaluate (1) the policies and procedures established by the Division of Banking Supervision and Regulation (BS&R) and the Division of Information Technology (IT) to ensure applications owned or operated by Reserve Banks on behalf of the Board of Governors of the Federal Reserve System (Board) meet FISMA's requirements; and (2) the Reserve Banks' implementation of those policies and procedures, focusing specifically on how the application inventories were compiled. As you know, FISMA requires agencies to provide information security protections for information collected or maintained by or on behalf of the agency, as well as for information systems used or operated by an agency, by a contractor of an agency, or by another organization on behalf of an agency. The Reserve Banks perform functions on behalf of, or under delegated authority from, the Board and, in performing these functions, collect or maintain information and use or operate information systems on behalf of the Board. This information and these information systems are subject to FISMA compliance.

Overall, we found that the Federal Reserve System (System) has begun implementing FISMA's requirements for Supervision and Regulation (S&R) systems. During 2004, a project team established by BS&R to help the S&R business function at the Reserve Banks comply with the legislation conducted FISMA awareness training at the Reserve Banks. The project team also issued guidance for developing an inventory of applications, developed an application tracking mechanism, and established a process to track identified weaknesses and associated corrective actions. Based on the guidance provided, the Reserve Banks developed an initial inventory of 140 applications and completed eight security control reviews using a self-assessment questionnaire. The project team provided additional guidance in early 2005 for updating the inventory and conducting additional security control reviews.

Notwithstanding the progress made, however, we believe that further actions are required to ensure that all information and information systems used or operated by the Reserve Banks in support of S&R delegated functions meet FISMA's requirements. We found that the Reserve Banks did not follow a consistent approach to developing their application inventory, and the guidance issued to the Reserve Banks for developing the inventory was insufficient to address all security controls and properly establish system interfaces as required by FISMA. As a result, the Board lacks assurance that it has a complete and accurate inventory of all information and information systems supporting its programs and operations. In our opinion, establishing an accurate inventory is critical to effectively implementing other FISMA requirements. We also found that guidance issued to the Reserve Banks did not thoroughly address other aspects of the Board's current information security program (such as developing security plans, testing application security controls, and implementing corrective action plans).

Our report contains four recommendations designed to enhance guidance to the Reserve Banks, strengthen compliance with the legislation and the Board's security program, and establish greater consistency across the System. Because FISMA assigns to the Chief Information Officer (CIO) the responsibility for ensuring an agency complies with FISMA's requirements, we are addressing our recommendations to the Board's CIO rather than the project team. We believe that the Board's CIO should be the focal point for promulgating guidance to the Reserve Banks, although we recognize that the project team may ultimately implement the CIO's directives. Work on this audit also identified broader issues related to the Board's approach to, and progress towards, implementing portions of its information security program. Given that these broader issues go beyond the specific objectives of this audit, we plan to address our concerns as part of our annual evaluation of the Board's information security program.

We provided our report to the Director of IT, in her capacity as CIO for FISMA, and to BS&R's Chief Technology Officer for review and comment. The Director of IT and the Director of BS&R provided a joint response which is included as appendix 1. In their response, the directors partially concurred with our first recommendation, did not concur with our second recommendation, and generally concurred with the intent of recommendations three and four. For all four recommendations, the directors have identified actions that, if fully implemented, will generally satisfy the recommendations' intent. The directors' response also provides narrative context on FISMA and its implications for Board and Reserve Bank activities, as well as the Board's approach to implementing the legislation with respect to Reserve Bank systems.

While we agree with several of the directors' general observations, the response mischaracterizes our report's content in several areas. The response also highlights several areas of fundamental disagreement between the OIG and Board management regarding the legislation's requirements and the approach for implementing those requirements for Reserve Bank systems. To more closely align our analysis with the directors' specific comments, we have incorporated our perspective into the directors' response at appendix 1.

We are providing copies of this audit to Board management officials. The report will be added to our publicly-available web site at www.federalreserve.gov/oig and will be summarized on our next semiannual report to Congress. Please contact me if you would like to discuss the audit report or any related issues.

Sincerely,

/signed/

Barry R. Snyder
Inspector General

Enclosure

cc: Governor Mark Olson
Governor Susan Bies

Board of Governors of the Federal Reserve System

**AUDIT OF THE SUPERVISION AND
REGULATION FUNCTION'S EFFORTS TO
IMPLEMENT REQUIREMENTS OF THE
FEDERAL INFORMATION SECURITY
MANAGEMENT ACT**



OFFICE OF INSPECTOR GENERAL

September 2005

TABLE OF CONTENTS

	Page
BACKGROUND	1
OBJECTIVES, SCOPE, AND METHODOLOGY	2
FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS.....	3
ANALYSIS OF COMMENTS	8
APPENDIXES	11
Appendix 1 – Division Director’s Comments with OIG Analysis	13
Appendix 2 – Principal Contributors to this Report	21

BACKGROUND

Legislative Requirements

The Federal Information Security Management Act of 2002 (FISMA), Title III of Public Law 107—347, provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. FISMA expanded previous legislation and requires agencies to provide information security protections for (i) information collected or maintained by or on behalf of the agency, and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. FISMA assigns responsibility to the agency’s Chief Information Officer (CIO) to ensure compliance with the Act’s requirements, and requires the Office of Inspector General (OIG) to perform an annual independent evaluation of the agency’s information security program and practices.

To ensure the effectiveness of information security, FISMA requires that each agency develop and implement an agencywide information security program to provide information security for all agency systems, including systems managed on behalf of the agency by another agency, contractor, or other source. The agency’s program should include:

- conducting periodic risk assessments;
- developing security plans;
- establishing minimum security configuration requirements;
- providing security awareness training;
- conducting periodic control testing;
- establishing procedures for detecting, reporting, and responding to security incidents; and
- developing a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies.

FISMA also assigned to the director the Office of Management of Budget (OMB) the responsibility for establishing governmentwide policies for managing information security programs. In addition, FISMA tasked the National Institute of Standards and Technology (NIST) with developing related standards and guidelines.

Roles and Responsibilities

FISMA amends the Paperwork Reduction Act of 1995 (PRA) by enacting a new subchapter on “Information Security.” The Board of Governors of the Federal Reserve System (Board) is subject to PRA and is, therefore, subject to FISMA’s requirements. Because the Federal Reserve Banks (Reserve Banks) are not Federal agencies as defined in FISMA, they are not directly subject to the legislation. However, the Reserve Banks perform functions on behalf of, or under

delegated authority from, the Board, the U.S. Department of the Treasury (Treasury), and other federal agencies. For example, the Reserve Banks act under delegated authority from the Board to examine and supervise bank holding companies, state member banks, and all international banks and facilities located in the United States. The Reserve Banks also act as fiscal agents for the Treasury in the issuance and redemption of U.S. government securities and as repositories for federal tax payments. In performing these functions, the Reserve Banks collect or maintain information and use or operate information systems on behalf of these agencies. This information and these information systems are therefore subject to FISMA's requirements.

The Board has designated the Staff Director for Management as the Board's CIO. The Staff Director has delegated to the Director of the Division of Information Technology (IT) certain CIO functions pertaining to FISMA and E-Government. An IT assistant director serves as the Board's Information Security Officer (ISO) and is the focal point for the Board's information security activities. Within the Federal Reserve System (System), each Reserve Bank has IT staff responsible for the Bank's technology assets. IT staff at the Reserve Banks do not, however, have any direct reporting relationship to the Board's CIO or ISO.

In 2004, the Board's Division of Banking Supervision and Regulation (BS&R) established an initiative to help the supervision and regulation (S&R) business function at the Reserve Banks comply with FISMA's requirements.¹ The initial goals and objectives of the FISMA-compliance initiative were to coordinate and conduct FISMA awareness and security training; develop an accurate and complete systems inventory; conduct an initial assessment to determine whether existing security processes for S&R assets comply with NIST guidance; and develop a plan to identify information security weaknesses and track associated corrective actions. To implement this initiative, BS&R assigned a project team consisting of staff from the Board and Reserve Banks.

OBJECTIVES, SCOPE, AND METHODOLOGY

We began this audit as part of an effort to perform work throughout the year related to our independent evaluation responsibilities under FISMA. We conducted our audit fieldwork from November 2004 through March 2005. Our objectives were to evaluate (1) the policies and procedures established by BS&R and IT to ensure applications owned or operated by Reserve Banks on behalf of the Board meet FISMA's requirements and (2) the Reserve Banks' implementation of those policies and procedures, focusing specifically on how the application inventories were compiled.

To accomplish these objectives, we interviewed Board IT and BS&R management and staff and reviewed guidance issued to the Reserve Banks. We reviewed the work completed in 2004 by the project team and their plans for 2005. We also reviewed guidance provided to the Reserve Banks by the Treasury, although we did not evaluate implementation of Treasury's guidance.

¹S&R includes the Reserve Banks' BS&R function and the consumer compliance function.

To evaluate the Reserve Banks' implementation of the Board's policies and procedures, we visited three Reserve Banks. We selected two Reserve Banks that had major applications and that had completed security control reviews during 2004. We selected the third Reserve Bank because it had the most applications on the inventory. During our visits, we interviewed Reserve Bank IT and S&R management and staff, and reviewed processes for developing the inventory, performing security control reviews, and correcting identified weaknesses. Our audit was conducted in accordance with generally accepted government auditing standards.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

Overall, we found that the project team and the Reserve Banks have begun implementing FISMA's requirements for S&R systems. During 2004, the project team conducted FISMA awareness training at the Reserve Banks, issued guidance for developing an inventory of applications, and established an application tracking mechanism. Based on the guidance provided, the Reserve Banks developed an initial inventory of 140 applications and completed eight security control reviews using a self-assessment questionnaire. The project team independently reviewed the assessments and concluded that each application substantially complied with FISMA. The project team also established a process to track identified weaknesses and associated corrective actions. The project team's guidance for 2005 directed the Reserve Banks to update the inventory and to complete security reviews for all major and moderate-risk applications. In addition, the project team plans to conduct additional FISMA awareness training and perform additional independent assessments of the security control reviews completed by the Reserve Banks during the year.

Notwithstanding the progress made, however, we believe that further actions are required to ensure that all information and information systems used or operated by the Reserve Banks in support of S&R delegated functions meet FISMA's requirements. We found that the Reserve Banks did not follow a consistent approach to developing their application inventory. We identified applications on the inventory that were not supporting a delegated S&R function and our fieldwork showed that the Reserve Banks followed inconsistent approaches to including administrative applications and internal S&R websites. We also found that the guidance issued to the Reserve Banks for developing the inventory was insufficient to address all security controls and properly establish system interfaces as required by FISMA. As a result, the Board lacks assurance that it has a complete and accurate inventory. In our opinion, establishing an accurate inventory is critical to effectively implementing other FISMA requirements, such as control reviews and certifications and accreditations. During our audit, we also found that guidance issued to the Reserve Banks did not thoroughly address all aspects of the Board's current program (such as developing security plans, testing application security controls, and implementing corrective action plans).

Our report contains four recommendations designed to enhance guidance to the Reserve Banks, strengthen compliance with the legislation and the Board's security program, and establish greater consistency across the System. Because FISMA assigns to the CIO the responsibility for

ensuring an agency complies with FISMA's requirements, we are addressing our recommendations to the Board's CIO rather than the project team. We believe that the Board's CIO should be the focal point for promulgating guidance to the Reserve Banks, although we recognize that the project team may ultimately implement the CIO's directives. We also recognize that the Board's ISO has been a liaison to the project team and is therefore aware of the project team's efforts. However, the ISO is conducting a pilot effort as part of revising the Board's information security program and informed us that he is waiting for that effort to conclude before incorporating the Reserve Banks into the Board's security program. We disagree with that approach and believe the CIO should issue additional guidance now to address the issues discussed in our report. The project team plans to continue working with Reserve Banks during 2005; definitive guidance issued by the CIO would help ensure that actions completed by the Reserve Banks are consistent with the Board's information security program and meet legislative requirements.

Work on this audit also identified broader issues regarding the Board's approach to, and progress towards, implementing portions of its information security program. Given that these broader issues go beyond the specific objectives of this audit, we plan to address our concerns in our annual evaluation of the Board's information security program.

1. 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.

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

One of the initial objectives of the S&R FISMA compliance initiative was to develop a complete and accurate inventory. To achieve this objective, the project team provided guidance to the Reserve Banks for developing their application inventory. The guidance instructed the Reserve Banks to include applications and systems that are supported at the Banks and that use S&R data to directly support an S&R business function. The guidance also directed the Reserve Banks to exclude general support systems; static web sites; programming development tools; customized office solutions such as spreadsheets; and Reserve Bank operational systems such as human resources/personnel systems, budget systems, and accounting systems. Based on this guidance, the Reserve Banks developed an initial inventory of 140 applications.

We found that the Reserve Banks did not consistently implement the guidance provided by the project team; as a result, the 140 applications do not represent a complete and accurate inventory of applications supporting the S&R function. Specifically, we found that the inventory for some Reserve Banks included applications supporting non-S&R functions such as discount window and credit risk. The Reserve Banks included these applications because these functional areas report to the same senior official as the S&R function. At the time of our audit, however, the

applicability of FISMA to functional areas other than S&R had not been definitively established. We also noted that some Reserve Banks included S&R internal websites as well as “administrative systems” such as time keeping and training databases.

We are also concerned that because the 2004 guidance specifically excluded the Reserve Banks’ general support systems (GSS), the Board is not accurately reporting the inventory in its annual FISMA submission to the OMB and that the Reserve Banks are not assessing the security controls for all applications.² In 2004, the Board reported only 64 of the 140 applications identified by the Reserve Banks. The Board did not report applications identified as having low risk or no risk and that did not contain restricted data. These applications generally rely on a GSS for their security controls. By not including either the low/no-risk applications or the Reserve Bank support systems, the Board may have underreported the total number of information resources supporting its programs and operations. Excluding these resources also means that controls over some applications will not be reviewed. While we recognize that the Reserve Banks may have implemented other processes for identifying and reviewing security controls over these applications, the processes differ from FISMA in several key respects such as the identification of minimum controls and periodic control testing. We believe the most efficient approach is to include the Reserve Bank support systems as part of FISMA reporting and implement the associated processes. An alternative to including the support systems would be to include all applications on the inventory and ensure that the required processes and associated documentation (such as securing plans, controls reviews, and certification and accreditation) are completed for every application.

We also believe that guidance in other areas related to the inventory can be improved. The Reserve Bank inventory does not include the interfaces between each S&R related system and all other systems or networks. Although the application tracking tool used by the project team contains fields for this information, the guidance provided to the Reserve Banks did not require these fields be populated. In our opinion, identifying system boundaries and interfaces is essential to accurately complete risk assessments and comply with FISMA requirements. Accurately identifying the interfaces is also necessary for completing system certifications and accreditations. The NIST *Guide for the Security Certification and Accreditation of Federal Information Systems (Special Publication 800-37)* recognizes that system interconnections, if not appropriately protected, may result in compromises of all connected systems and the data they store, process, or transmit.

Clearly identifying system boundaries will, in our opinion, also help to ensure the effective development of security plans, review of controls, and performance of certifications and accreditations. During our audit, for example, we found that the input and display modules of a Board application were listed as two separate applications on a Reserve Bank’s inventory. It was unclear whether prior control reviews of the Board application included these other modules, or whether the modules were to be reviewed separate and apart from the application they support. By not clearly defining an application’s boundaries and interfaces, the overall security of the application cannot be addressed from end to end. This may lead to omissions of key components

²GSS is an interconnected set of information resources under the same direct management control which shares common functionality.

when identifying controls and developing security plans, and to a duplication of effort by performing multiple security control reviews on components of the same system.

We recognize that during 2005, the Reserve Banks have continued to refine the application inventory based on additional guidance provided by the project team. Over the past year, however, we also found that various groups within the System have issued guidance for identifying applications that are subject to FISMA's requirements and for completing security-related processes related to those applications. We believe that the Board's CIO, who has the legislative responsibility for the agency's information security program, needs to establish firm requirements for including or excluding an application from the inventory. The CIO should also ensure that guidance provided to the Reserve Banks is consistently followed so that the Board's annual reporting accurately reflects the inventory of systems supporting its programs and operations.

2. We recommend that the CIO issue guidance to clearly define the requirements for a system security plan.

FISMA requires that each agency develop, document, and implement an agencywide security program. The agency's program should include the development of subordinate security plans to provide information security for networks, facilities, systems, or groups of systems that support the operations and assets of the agency. 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 also delineate the responsibilities, expected behavior, and required training of all individuals who access the system, and describe appropriate controls for interconnection with other systems. Security plans are also needed to comply with NIST guidance which requires information system owners to confirm during the certification and accreditation process that potential threats which could exploit information system flaws or weaknesses have been properly identified and documented.

System-specific security plans have been part of the Board's security program since 2002. Guidance provided to the Reserve Banks, however, has not yet addressed requirements for developing security plans consistent with the Board's program. During 2004, four Reserve Banks completed eight self-assessment questionnaires as part of reviewing application security controls; we reviewed six of the eight completed questionnaires. The questionnaires asked whether a security plan had been developed for the application being reviewed. Although each of the questionnaires reviewed indicated a security plan was in place, we assessed the supporting documentation and interviewed responsible Reserve Bank staff and found that none of the applications had a security plan that was consistent with the Board's program or NIST guidance. The questionnaires instead referenced other documents and processes such as software security certifications, risk assessments, and the system development life cycle. None of these documents and processes, however, contains all the pieces of a security plan.

The Board's security plan template is based on existing OMB guidance and, in our opinion, could be implemented at the Reserve Banks. We recognize that the ISO plans to revise the template during 2005 as part of ongoing revisions to the Board's security program, but we are

concerned that plans for the revised program do not presently include Reserve Bank S&R-related applications. We believe the CIO should incorporate the Reserve Banks into the process for revising the security plan document to ensure that any System concerns are addressed and provide sufficient guidance to help Reserve Bank staff implement this requirement. We also note that including the Reserve Banks in plans for revising the Board's information security program will be equally important for other program areas, such as performing risk assessments and certifications and accreditations.

3. We recommend that the CIO issue guidance for conducting information security reviews that includes specific requirements for control testing.

FISMA requires periodic testing and evaluation of the effectiveness of an agency's information security policies, procedures, and practices. The evaluation should include testing of the management, operational, and technical controls for every system identified in the agency's inventory and should be performed with a frequency depending on risk, but not less than annually. The depth and breadth of these annual reviews depend on the potential risk and magnitude of harm as well as the relative comprehensiveness of the prior year's review and the adequacy and successful implementation of the agency's process for identifying and remediating weaknesses in the system. FISMA looks to NIST to develop the standards and guidelines necessary to assist agency officials in fulfilling this responsibility.

As indicated above, staff at four Reserve Banks completed eight information security reviews in 2004 using a self-assessment questionnaire. These reviews involved five major applications, two non-major applications, and one system support center.³ The project team, along with an independent contractor, also conducted independent evaluations of the security reviews to serve as a quality assurance check, provide feedback to Reserve Bank management, and develop guidance for future reviews. We reviewed documentation supporting the security reviews and subsequent evaluations. Our review showed that the Reserve Banks used a self-assessment questionnaire that was consistent with the NIST self-assessment guide as required by OMB. We found, however, that neither the Reserve Banks nor the project team performed any detailed testing of security controls as required by FISMA. Rather, the Reserve Banks and the project team reviewed system documentation and interviewed system owners and technical support staff. While this may provide a level of assurance that the systems have appropriate documentation and that responsible staff understand information security policies, procedures, and practices, it does not ensure all security controls are functioning as intended. We raised similar concerns during our 2004 audit of the Board's information security program and made a recommendation that the CIO provide guidance to Board staff for conducting security reviews that included specific requirements for control testing. The CIO needs to ensure that guidance issued to the Reserve Banks regarding control testing is consistent with any requirements established for Board applications.

³The support center is not part of the Reserve Bank application inventory. However, it provides general system information and architecture support to Lotus Notes based applications used throughout the Federal Reserve System.

4. We recommend that the CIO issue guidance that clearly defines the roles and responsibilities for implementing corrective actions.

FISMA requires agencies to establish a process for addressing any deficiencies in information security policies, procedures, and practices. To implement this requirement, OMB guidance requires agencies to develop, implement, and manage a Plan of Action and Milestones (POA&M) for all programs and systems where an information technology weakness has been found. The POA&M should include all security weaknesses found during any review done by, for, or on behalf of the agency. The plans should be the authoritative agency-wide management tool for identifying the specific tasks required to address identified weaknesses, as well as the associated resources and anticipated milestones. In addition, agency officials should regularly update the agency CIO on their progress in implementing corrective actions to enable the CIO to monitor agency-wide remediation efforts and provide the agency's quarterly update to OMB.

The project team included deficiencies identified during Reserve Bank security reviews on BS&R's POA&M, which was submitted to the Board's ISO as part of the Board's POA&M process. During 2004, the project team also conducted POA&M awareness training. We found, however, that the team provided insufficient guidance to ensure that the Reserve Banks effectively tracked and remediated identified weaknesses. We interviewed several Reserve Bank staff whom the POA&M identified as contact persons for correcting weaknesses and found that staff were generally unaware that they had been assigned this responsibility. We recognize that this is the first year that the process has been implemented at the Reserve Banks and that it will continue to evolve as Reserve Bank staff become more familiar with FISMA. However, we believe it is necessary to clearly define the roles and responsibilities of individuals responsible for implementing corrective actions in order to maintain accountability at the proper level and help to ensure that weaknesses related to applications on the Reserve Bank's inventory are tracked and resolved in a consistent and timely manner.

ANALYSIS OF COMMENTS

We provided our report to the Director of IT, in her capacity as CIO for FISMA, and to BS&R's Chief Technology Officer for review and comment. The Director of IT and the Director of BS&R provided a joint response which is included as appendix 1. In their response, the directors partially concurred with our first recommendation, did not concur with our second recommendation, and generally concurred with the intent of recommendations three and four. For all four recommendations, the directors have identified actions that, if fully implemented, will generally satisfy the recommendations' intent. The directors' response also provides narrative context on FISMA and its implications for Board and Reserve Bank activities, as well as the Board's approach to implementing the legislation with respect to Reserve Bank systems. Specifically, the directors refer to the "evolving" requirements of FISMA and the changes brought about by OMB's June 2005 reporting guidance. The directors also reiterate that FISMA does not directly apply to the Reserve Banks since the Banks are not federal agencies. In addition, the directors note that the Reserve Banks already have strong risk-based information security programs, and that the Board adopted a phased approach to implementing FISMA's requirements for applicable Reserve Bank systems.

While we agree with several of the directors' general observations, the response mischaracterizes our report's content in several areas. The response also highlights several areas of fundamental disagreement between the OIG and Board management regarding the legislation's requirements and the approach for implementing those requirements for Reserve Bank systems. We believe that our four recommendations address fundamental aspects of an information security program that the legislation envisions to be in place for all systems on an agency's inventory. Our audit fieldwork showed that while the System has begun implementing FISMA's requirements for S&R systems, further actions are required to ensure that all information and information systems used or operated by the Reserve Banks in support of Board programs and operations meet the legislative requirements. In our opinion, one of the contributing factors to the issues identified during this audit is the lack of clear guidance from the Board regarding FISMA's applicability to Reserve Bank information and information systems in terms of the legislation's breadth (i.e., to which systems) and depth (i.e., to what degree for areas such as security plans and control testing). We plan to address this concern as part of our overall evaluation of the Board's information security program.

To more closely align the directors' specific comments with our analysis, we have incorporated our perspective into the directors' response at appendix 1.

APPENDIXES

Appendix 1 – Division Director’s Comments with OIG Analysis

MEMO

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DATE: August 10, 2005
TO: Mr. Barry R. Snyder
FROM: Rich Spillenkothen and Marianne Emerson */signed/*
SUBJECT: Comments on the Audit of the Supervision and Regulation (S&R) Function’s Efforts to Implement Requirements of the Federal Information Security Management Act (FISMA)

Thank you for the opportunity to comment on the OIG’s audit of the efforts of the Board’s S&R function to implement the evolving requirements of FISMA at the Reserve Bank level. As you are aware, the Reserve Banks themselves are not subject to FISMA because they are not federal “agencies” as defined by FISMA. The Reserve Banks are separate corporations whose shares are owned by commercial member banks in each District. The supervision function itself, of course, is the legal responsibility of the Board and is carried out by the Reserve Banks under delegated authority from the Board. Because the Reserve Banks collect and maintain Board information and operate and use information systems on behalf of the Board in the course of performing supervisory activities delegated by the Board, the Reserve Banks are indirectly affected by FISMA. The Board is required to ensure that the Reserve Banks collect and maintain Board information and use and operate information systems on behalf of the Board consistent with the FISMA standards applied by the Board. It is for this reason that S&R, in collaboration with the Board’s CIO and ISO, initiated a review under FISMA standards of the manner in which Reserve Banks apply information security to S&R information collected and maintained and information systems used or operated on behalf of Board S&R.

OIG Analysis:

Our report never uses the term “evolving” when referring to FISMA’s requirements. Although OMB has modified the specific reporting requirements over the past four years and although NIST has continued to develop new guidance, the underlying legislative requirements have remained the same.

The Background Section of our report clearly states that the Reserve Banks are not federal agencies and thus not subject to FISMA’s requirements. However, to the extent that the Reserve Banks will need to change processes and procedures to comply with the Board’s information security program, they are more directly affected by the legislation than the directors’ comments would indicate. Our audit fieldwork found that the Reserve Banks have not yet fully

Appendix 1 – Division Director’s Comments with OIG Analysis

implemented portions of the Board’s information security program in accordance with “FISMA standards.”

At the outset, we believe it is important to recognize that 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. As was stated in this audit’s closing meeting on July 7, 2005, we believe the audit conducted by the OIG should acknowledge the effectiveness of the Reserve Banks’ information security programs to give a complete picture of the actual status of Reserve Bank information security programs as they relate to the Board S&R function.

OIG Analysis:

Under FISMA, we are required to evaluate the Board’s information security program, to include reviewing controls over the systems included in the Board’s inventory and evaluating the Board’s compliance with the legislation. During our audit, we found that the current Reserve Bank processes—such as those in the new Information Security Manual and the Risk Management Process (RMP)—may share similar objectives with FISMA, but that 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 requires the use of an independent certification agent to 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. In our opinion, an information security program that doesn’t require detailed control testing or certification is not providing the same level of assurance as the processes envisioned by FISMA and required by the implementing NIST guidance.

While the objectives, scope and methodology section of the audit states that the fieldwork took place between November 2004 and March 2005, we believe that the report should highlight that the audit covers two different FISMA compliance periods: 2004 and 2005. S&R FISMA guidance for both years consciously provided for a phasing in of important elements based upon a careful consideration of priorities. Certain elements cited in the report were not overlooked in 2004; rather they were judged to be of lower priority. Moreover, this approach took into account the evolving nature of the government-wide FISMA guidance promulgated by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) and, consequently, the evolving Board information security program. Our philosophy of a rational phase-in, based upon priorities, reflected a careful assessment of the rate at which Reserve Banks could absorb FISMA requirements as they concurrently implement a new information security manual. Knowing that Reserve Banks had to deal with changing requirements from OMB, NIST and the Board information security program, we continue to

Appendix 1 – Division Director’s Comments with OIG Analysis

believe this phase-in approach is the most effective means to assure S&R information systems operate in a manner consistent with FISMA standards applied by the Board.

OIG Analysis:

Since the Board must report to OMB at the end of September/beginning of October each year, the “FISMA compliance period” for agency reporting purposes has generally been from October to September (to coincide with the standard government fiscal year). Our audit fieldwork therefore covered a single FISMA reporting period. While the S&R project team may have issued guidance in separate calendar years, there is nothing to suggest that the Reserve Banks should be on different FISMA reporting cycles than the Board.

Throughout our report, when referring to the guidance issued by the S&R project team, we generally use language such as “the guidance was insufficient” or “the guidance did not thoroughly consider.” Whether this was by design or omission doesn’t change the fact that elements of the Board’s program were not in place at the Reserve Banks at the time of our audit. One of our report’s fundamental conclusions is that despite progress made, all information and information systems used or operated by the Reserve Banks in support of S&R delegated functions do not yet fully comply with the legislation, even though FISMA was passed over two years ago. We believe that the directors’ comments minimize the capabilities of the Reserve Banks to adapt to new requirements. Reserve Bank staff we spoke with during the audit seemed willing to incorporate whatever requirements were necessary, as long as those requirements were clearly communicated.

We believe the audit also would benefit from a delineation between those systems at the Reserve Banks that support the operations and assets of the Board and are operated by the Reserve Banks on behalf of the Board, versus those that do not meet these criteria. This distinction is critical for assessing the scope of the Board’s obligation under FISMA to review and evaluate the information systems of the Reserve Banks. In this respect, and based on the advice of the Board’s Legal Division, we believe the audit is inaccurate in its assessment of the scope of FISMA and should be amended to recognize that FISMA applies only to the Board (and not the Reserve Banks directly) and that it requires the Board to make various assessments of Reserve Bank information and information systems only to the extent that the information or information systems “support the operations and assets” of the Board.

OIG Analysis:

In the Background Section of the report, we make the very delineation described above. However, and more significantly, the Board itself has yet to make a clear distinction between those systems (outside the S&R function) which are subject to FISMA and those which are not. The failure to **clearly establish** the “breadth” of FISMA’s applicability to Reserve Bank systems supporting Board programs and operations is, in our opinion, a significant deficiency in the Board’s implementation of the legislation and an issue that

Appendix 1 – Division Director’s Comments with OIG Analysis

we plan to address in our annual assessment of the Board’s information security program. We also note that the legislation does not require the Board “to make various assessments of Reserve Bank information and information systems.” Rather, FISMA requires agencies to “...provide information security protections for information collected or maintained by or on behalf of the agency, and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency”.

Further, to the extent the audit includes a discussion of information or information systems operated by the Reserve Banks for other federal agencies, those activities are not and should not be part of the Board’s Information Security Program subject to FISMA. The particular federal agency on whose behalf the Reserve Bank operates or uses the system is responsible for implementing any FISMA information security requirements including all testing and evaluations of those systems.

OIG Analysis:

We never discussed the systems operated by the Reserve Banks for other federal agencies, other than to note that the Reserve Banks do, in fact, perform functions on behalf of the Treasury and other agencies. In our Objectives, Scope, and Methodology section, we make it very clear that we reviewed guidance issued by the Treasury but that we did not evaluate the guidance. There was never any intent to state or infer that activities conducted for another agency are part of the Board’s information security program, and we do not believe the report makes such a statement or inference.

We believe it is important to note that while the Board’s information security program covers S&R applications operated by the Reserve Banks on behalf of the Board, the same cannot be said of the Reserve Bank’s infrastructure (servers, network operations, telecommunications and other managed services) that the Reserve Banks operate or use on their own behalf. Accordingly, we believe the Reserve Banks’ infrastructure does not have to be separately included in the Board’s inventory as an information system operated or used by a third party on behalf of the Board.

OIG Analysis:

We have a fundamental disagreement with Board management regarding the proper approach to including or excluding Reserve Bank general support systems. In our opinion, and as addressed in our report, the Board needs to either (1) include all systems supporting the S&R function (from high-risk to low-risk) on the Board’s inventory and complete all required processes and associated documentation for every system, or (2) fold the lower-risk systems under the appropriate general support systems and subject those platforms to FISMA’s requirements. Whether the general support systems are explicitly included on the inventory or not, however, evaluating the controls of any system will by necessity include a review of the controls provided by the infrastructure.

Appendix 1 – Division Director’s Comments with OIG Analysis

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.

1. 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.

We partially concur. The recommendation implies that to date the CIO has not provided guidance. However, as the audit itself acknowledges, guidance provided to Reserve Banks has been developed with the involvement of the Board’s CIO. The OIG stated that they found no applications missing from the original inventory. The CIO’s 2004 guidance concentrated on ensuring that there were no omissions, and that every application that was associated with the supervision function was reported. Board S&R staff then reviewed, analyzed, and refined the inventory, eliminating applications to which FISMA did not apply. Because of the priority of application approach (discussed above), low risk applications to which FISMA does apply were also temporarily omitted in order to focus limited resources on the higher risk applications as quickly as possible.

OIG Analysis:

Our report notes that the ISO was a liaison to the S&R project team and was therefore aware of their efforts. However, we found no evidence of the CIO’s involvement in the guidance that was issued or of the “collaboration” referred to in the opening paragraph of the directors’ response and our perception was that the S&R project team felt they received limited guidance from the CIO and the ISO. In addition, the ISO himself stated that he wasn’t going to provide direction to the S&R project team until he finished revising the Board’s information security program.

FISMA requires agencies to develop and maintain an inventory of major information systems, which forms the basis of FISMA’s periodic testing requirement. At the closing meeting, we stated that we found no applications missing from the inventory at the three Reserve Banks we visited; we made no representations, however, about the entire S&R portfolio. While we don’t disagree with prioritizing review resources on higher-risk applications, this is not consistent with our understanding of the reasons the ISO left the lower-risk applications off of the OMB reporting, nor was our understanding that these applications were only “temporarily omitted.” Rather, our understanding was that the ISO had adopted an approach consistent with the treatment of Board-operated applications; i.e., applications listed in the Board’s inventory as “other” are not reported to OMB and are not subject to all of the procedures and documentation required by FISMA because these applications rely on one of the Board’s general support systems for their controls. In contrast to the

Appendix 1 – Division Director’s Comments with OIG Analysis

Reserve Banks, however, the Board’s general support systems are included on the Board’s inventory and are subject to all of the associated processes.

Further, we are not at all certain that the most efficient approach to handling the low risk applications is to include Reserve Bank general support systems (infrastructure), which are otherwise not subject to review under FISMA. FISMA regulations contain a high degree of paperwork burden. As noted in the audit, the Reserve Banks may have implemented other processes for identifying and reviewing security controls over these low-risk applications. Board staff will carefully evaluate the benefits and costs associated with alternative methods of handling the low-risk applications before deciding on the best approach. It is likely that more clearly defining the boundaries between S&R systems used or operated on behalf of the Board and general support systems used or operated by the Reserve Banks for themselves will be a more efficient method for meeting the Board’s FISMA requirements. Moreover, new guidance from NIST recommends that agencies group minor applications into major applications for reporting purposes.

OIG Analysis:

We question whether the additional “burden” as imposed by FISMA above and beyond the current processes at the Reserve Banks (the new Information Security Manual or the Risk Management Process) is really that onerous. The directors’ comments regarding the grouping of minor applications are consistent with our approach to group the low-risk applications under the Reserve Banks’ general support systems. It is unclear from the directors’ response how grouping “minor applications” into “major applications” would fundamentally differ from folding those applications under a general support system. The directors’ response also fails to account for those Reserve Banks where the S&R functional area maintains its own portion of the infrastructure, separate and apart from Reserve Bank IT.

Our focus in 2004 was to obtain a complete FISMA inventory. Our guidance for 2005 requested that system interfaces be included in the inventory. Interfaces are required to be identified for every major information system operated by or under the control of the Board. 44 U.S.C. 3505(c).

OIG Analysis:

We question how obtaining a complete inventory can be accomplished if the Board has not established how FISMA applies to the Reserve Banks outside of the S&R function.

2. We recommend that the CIO issue guidance to clearly define the requirements for a system security plan.

We do not concur with this recommendation to the extent that it implies a weakness in the Board’s information security efforts. It was only in June 2005 that OMB established the requirement that contractors (or third parties) are expected to have security programs that, at a minimum, meet NIST guidance. Prior to June 2005, and for the entire period covered

Appendix 1 – Division Director’s Comments with OIG Analysis

by the OIG audit, OMB had not required that agencies ensure that contractors have “identical not equivalent” security procedures. Going forward, we are reviewing OMB’s new guidance and will determine how best to implement it at the Reserve Banks. We are not convinced that the audit is correct when it asserts that the Board’s security template could easily be implemented at the Reserve Banks that have their own quality assurance processes and their own methods of incorporating information security expectations into applications.

OIG Analysis:

The legislation itself requires that agencies develop “...subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate...” One of OMB’s reporting measures since 2002 has been the percentage of applications with security plans. In its 2004 reporting guidelines, OMB stated that “...agency IT security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems – on behalf of a Federal agency.” OMB’s June 2005 guidance, in our opinion, merely clarified what we have believed all along: if the application is on the Board’s inventory, it needs to undergo the same processes, regardless of whether it is maintained by Board staff or Reserve Bank staff. The directors’ response also fails to note that the control reviews completed by the Reserve Banks during 2004, and reviewed by the S&R project team, stated that security plans were in place. Our audit showed this was not the case.

Based on concerns raised by the CIO and ISO at the closing meeting, we deleted the word “easily” from the final draft. However, one of the reasons that we believe implementing the template at the Reserve Banks would not be difficult is that the Banks have already completed many of the processes and developed much of the documentation referenced in the security plan template; preparing security plans would, in our opinion, be relatively straightforward. One of the benefits provided by a security plan is that it describes, in one place, an overview of the security requirements of a system, the controls in place or planned for meeting those requirements, and the responsibilities and expected behavior of all individuals who access the system. We note that the draft of NIST SP 800-18 *Guide for Developing Security Plans for Federal Information Systems* states that security plans are required for all major applications and general support systems. The guide notes that plans are not required for minor applications, since the controls for these applications are typically provided by the general support system or major application in which they operate. To properly apply this approach, however, the Board will need to carefully establish system boundaries to ensure that all applications are appropriately covered.

- 3. We recommend that the CIO issue guidance for conducting information security reviews that includes specific requirements for control testing.**

Appendix 1 – Division Director’s Comments with OIG Analysis

We concur with the ultimate need to test controls. By design, the 2004 S&R FISMA process focused first on obtaining an accurate inventory; 2005 focused on identifying existing Reserve Bank controls and testing processes; and, 2006 will focus on implementing a targeted control testing regimen consistent with FISMA requirements.

OIG Analysis:

Although the directors’ response indicates concurrence with the intent of the recommendation and identifies planned actions, it is unclear why implementation will take until 2006. Our discussions with the S&R project team indicated that actions to implement the recommendation were planned for 2005.

4. We recommend that the CIO issue guidance that clearly defines the roles and responsibilities for implementing corrective actions.

Our 2004 focus was to ensure we had a comprehensive Plan of Action and Milestones (POA&M). This was appropriately implemented and Board S&R staff appropriately identified and followed-up on corrective actions. We concur that Reserve Bank staff responsible for correcting weaknesses should also be aware of their responsibilities through a standard tracking mechanism. This will be implemented in 2006.

OIG Analysis:

Although the directors’ response indicates concurrence with the intent of the recommendation and identifies planned actions, it is unclear why implementation will take until 2006 since the Board has already implemented the standard tracking mechanism, for corrective actions at the Reserve Banks and Reserve Bank staff are already listed as points-of-contact. Our discussions with the S&R project team indicated that actions to implement the recommendation were planned for 2005.

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

Appendix 2 – Principal Contributors to this Report

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

Richard Allen, EDP Auditor

Gerald Edwards, Auditor

Silvia Vizcarra, Auditor

William Mitchell, Assistant Inspector General