

Board of Governors of the Federal Reserve System

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



OFFICE OF INSPECTOR GENERAL



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

OFFICE OF INSPECTOR GENERAL

September 29, 2003

The Honorable Mark W. Olson
Chairman, Committee on Board Affairs
Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Governor Olson:

We are pleased to present our *Report on the Audit of the Board's Information Security Program* (A0302). We performed this audit pursuant to requirements in the Federal Information Security Management Act (FISMA). FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act (GISRA) which expired in November 2002. FISMA requires each agency Inspector General to conduct an annual independent evaluation of the agency's information security program and practices. This was the third year that such evaluations were required; our first two evaluations were conducted pursuant to an identical requirement in GISRA. 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.

To test security controls and techniques, we selected four applications for review. We performed our control tests using a modified version of the National Institute of Standards and Technology Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*. Our tests did not identify any major security control weaknesses, although we found several areas where controls need to be strengthened. Given the sensitivity of the issues involved with these reviews, we are providing the results to management under separate restricted cover. We plan to follow up on implementation of our recommendations as part of our future audit and evaluation activities related to the Board's information security program. We also followed up on recommendations made during prior year's control reviews and found that sufficient actions had been taken to close all recommendations; however, we identified one broader issue pertaining to documenting and tracking remedial actions which we have included as part of our compliance discussions below.

To evaluate the Board's compliance with FISMA and related policies and procedures, we followed up on the open recommendations in our 2002 information security audit report.¹ These recommendations were designed to help bring the Board into compliance with GISRA's requirements and further enhance the Board's information security program. Since FISMA contains most of the requirements and provisions set forth by GISRA, implementing our prior recommendations would also bring the Board into compliance with the new information security legislation. Our follow-up work showed that the Board continues to make progress in developing a structured information security program as envisioned by both FISMA and GISRA. Specifically, we found that the Board's Chief Information Officer (CIO) established a direct reporting relationship for security matters between his position and the Information Security Officer (ISO). We also found that the ISO has developed a high-level Boardwide security plan and issued security incident guidance. In addition, Board staff completed additional application security plans and related security control reviews and all Board divisions and offices updated their risk assessments.

Notwithstanding the actions described above, however, the Board has not achieved full compliance with FISMA's requirements and issues remain open related to five of the seven recommendations from our original 2001 information security report. These issues pertain to properly positioning the CIO and ISO to effectively carry out their responsibilities, finalizing the Boardwide security program document and the application inventory, conducting security control reviews, developing a comprehensive information security awareness program, and identifying control weaknesses and documenting corrective actions. We recognize that the Board, along with other government agencies, is still transitioning from implementing the requirements outlined in GISRA to those contained in FISMA and that guidance from the Office of Management and Budget (OMB) was only recently provided. The new legislation, however, establishes essentially the same requirements for information security, and we continue to believe that fully addressing the open issues from our prior report is essential to firmly establish the necessary managerial responsibilities, oversight structure, and clear, consistent guidance related to the Board's information security program; to bring the Board into compliance with the security legislation's requirements; and to establish the organization and programmatic framework that is intended by the legislation. To help the Board achieve these objectives, the attached report updates our prior recommendations using the concepts, terms, and requirements contained in FISMA.

We believe that one of the reasons the Board has not achieved full compliance with FISMA's requirements is that the Board's decentralized, collegial operating environment differs from the structured, top-down framework for information security management envisioned by the security legislation. Implementing our first two recommendations regarding the responsibilities and authorities of the CIO and ISO will be essential to establishing this framework. We also note that one of the new provisions in FISMA is that agency information security programs apply to all information systems that support the operations and assets of the

¹ Our 2002 information security report (*Report on the Audit of the Board's Information Security Program* (A0205), dated September 2002) reported on the status of our original 2001 information security report (*Report on the Audit of the Board's Information Security Program* (A0106), dated September 2001). Our report contained seven recommendations. During 2002, we fully closed one recommendation and partially closed three other recommendations.

agency, including those provided or managed by another agency, contractor, or other organization. The ISO has been working with the Board's Legal Division to determine how this requirement applies to contractors and Reserve Banks that operate information systems supporting Board programs and operations. Resolving this issue will impact implementing the remainder of our recommendations since each recommendation addresses an element of the Board's information security program that will need to be applied to these other organizations.

We provided our draft report to the Staff Director for Management, who serves as the Board's CIO, for review and comment. In his response, the Staff Director partially concurred with recommendations 1 and 2. The Staff Director noted that the Board, like other small federal agencies, is challenged by the prescriptive standards contained in FISMA and that outside reviews of the Board's security program by an OMB representative and by a contractor working for NIST did not have any issues with the Board's governance structure for information security. Nevertheless, the Staff Director indicated that he plans to strengthen the Boardwide emphasis regarding FISMA and look for alternative methods for meeting policy, compliance, and review responsibilities. We are encouraged by these actions and by other recent efforts to finalize the security program, identify the CIO's responsibilities as enumerated in various statutes, delegate the CIO's responsibilities to someone other than the Staff Director, and create more of a direct relationship between the CIO and the ISO. We believe that implementing the legislation's requirements is good business practice which can be achieved with a risk-based, cost-effective approach. The Staff Director's response also concurred with our remaining five recommendations and identified actions that he will take or has already taken to implement the recommendations.

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

Enclosure

cc: Governor Edward M. Gramlich
Governor Donald L. Kohn

Board of Governors of the Federal Reserve System

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



OFFICE OF INSPECTOR GENERAL

(A0302)

September 2003

TABLE OF CONTENTS

	Page
Background.....	1
Objectives, Scope and Methodology	4
Findings, Conclusions and Recommendations	5
Analysis of Comments.....	16
Appendixes	17
Appendix 1 – Division’s Comments.....	19
Appendix 2 – Principal Contributors to this Report	21

BACKGROUND

Legislative Requirements

On December 17, 2002, the President signed into law the E-Government Act of 2002 (P.L. 107-347) which includes Title III, the Federal Information Security Management Act of 2002 (FISMA).¹ FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act (GISRA) which expired in November 2002. GISRA codified existing information security requirements found in the Office of Management and Budget (OMB) Circular A-130, Appendix III, and reiterated security responsibilities outlined in other legislation.²

FISMA contains most of the requirements and provisions set forth by GISRA. Specifically, FISMA requires that each agency develop and implement an agencywide security program to provide information security throughout the life cycle of all systems supporting the agency's operations and assets. FISMA reiterates the Chief Information Officer's (CIO) strategic agencywide security responsibilities and places responsibility on agency officials for assessing the information security risks of the operations and assets for the programs and systems over which they have control. Officials are to determine, based on their risk assessments, the level of information security appropriate to protect such operations and assets and to periodically test and evaluate information security controls and techniques.

FISMA also restates the requirements for conducting annual independent evaluations of agency information security programs and practices. The independent evaluations are designed to test the effectiveness of security controls and techniques for a representative subset of an agency's information systems and to assess compliance with the requirements of FISMA. Responsibility for the independent evaluations has been given to the agency Inspector General (IG). Each agency head is to submit the results of the IG's independent evaluation, along with the agency's reports of the adequacy and effectiveness of information security policies, procedures, and practices, to the Director of OMB on an annual basis.

While FISMA reaffirms essentially all of the requirements included in GISRA, it also introduces some additional requirements to further strengthen the security of the Federal government's information and information systems. For example, FISMA requires that each agency provide information security for all information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other organization. This requirement has broader applicability than that of GISRA because agency

¹ An earlier version of FISMA was enacted as part of the Homeland Security Act (P.L. 107-296). However, as provided in 44 U.S.C. 3549 and as stated by the President in his signing statement for the E-Government Act, the version of FISMA included in the E-Government Act supersedes similar FISMA provisions in the Homeland Security Act.

²The Legal Division (Legal) of the Board of Governors of the Federal Reserve System (Board) has determined that the Board is subject to the E-Government Act since it adopts the definitions in the Paperwork Reduction Act which specifically includes the Board as an "agency". Legal had previously determined that the Board was subject to the requirements in GISRA.

information security programs now apply to all organizations that possess or use federal information—or which operate, use, or have access to federal information systems—on behalf of a federal agency. Such organizations may include contractors, grantees, state and local governments, and industry partners. Other expanded provisions in FISMA include a stronger role for the agency Information Security Officer (ISO), the development of an inventory of major information systems, and the annual testing of the management, operational, and technical controls for each system identified in the agency's inventory of information systems.

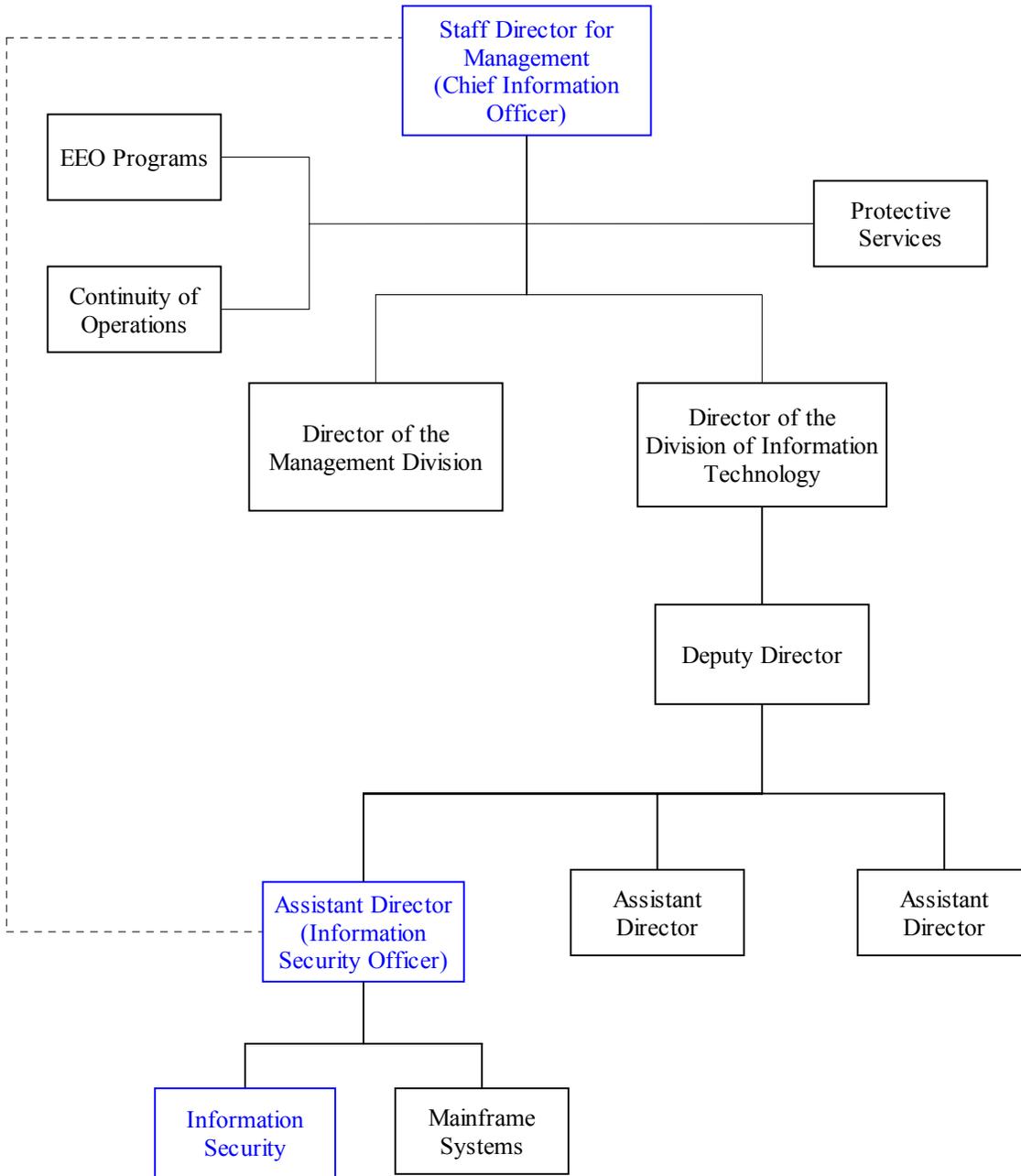
FISMA also reassigned the Director of OMB the responsibility for establishing government-wide policies for the management of information security programs. To assist agencies in fulfilling their FISMA evaluation and reporting responsibilities, OMB issued memorandum 03-19 in August 2003. The memorandum updates prior OMB reporting instructions and provides a consistent form and format for agencies to report back to OMB on topics that relate to agency responsibilities outlined in FISMA. Although the 2003 reporting instructions remain nearly identical to last year's instructions, there are two significant changes: an increased emphasis on previously established performance measures and additional guidance to IGs to assess whether agencies have an agencywide plan of action and milestones (POA&M) process that meets OMB criteria.

Information Security Roles and Responsibilities

The Board of Governors of the Federal Reserve System (Board) has designated the Staff Director for Management as the Board's CIO. The Board's Information Security Unit (ISU), in the Division of Information Technology (IT), is responsible for monitoring the security of the Board's mainframe, public web sites, and local area networks. The unit is also responsible for intervening, as required, to address security exposures and for acting as liaison to Federal Reserve System (System) groups coordinating Systemwide security issues. The ISU reports to an IT assistant director who serves as the Board's ISO and is the focal point for the Board's information security activities. A reporting relationship has also been established between the ISO and the CIO for security matters. (See the organizational chart that follows.)

Because much of the information technology at the Board is decentralized, divisions and offices also have information security responsibilities. Specifically, network administrators are responsible for configuring, maintaining, and protecting the systems under their control to ensure a secure distributed operating environment. Information owners are responsible for assessing the degree of business risk associated with their systems and applications, classifying and authorizing access to information, and ensuring proper security controls are in place. To help coordinate these responsibilities, the Board has established an Information Security Committee (ISC) comprised of representatives from each division and office. The ISC functions as a Boardwide coordinating body with responsibility for advising management regarding System information security strategic direction and initiatives. The ISC is also responsible for the local application of policies and procedures in support of System information security policies and safeguards.

Board Organizational Chart for IT and Information Security



Information Security Guidance

To provide policy direction regarding the protection of its information assets, the System developed the *Information Security Manual (ISM)*. The ISM defines policies and safeguards for information security and is applicable to all automated platforms and manual information processes used throughout the System. The ISM is built on three security principles: confidentiality (assurance that information is disclosed only to authorized entities), integrity (assurance that information has not been improperly altered), and continuity of operations (assurance that correct information is available when needed). Two other manuals, the *Distributed Processing Security Support Manual* and the *Mainframe and FEDNET Security Support Manual*, contain policies and procedures specifically related to those information technology environments and support the general guidance provided by the ISM.³ Board divisions and offices are required to comply with the policies and safeguards in these manuals.

OBJECTIVES, SCOPE, AND METHODOLOGY

We conducted our audit fieldwork from May to September 2003. Our audit objectives, based on FISMA's requirements for conducting independent evaluations, were to evaluate the effectiveness of security controls and techniques for selected information systems and to evaluate the Board's compliance with FISMA and related information security policies, procedures, standards, and guidelines.

To achieve our objectives, we reviewed Board and System documentation pertaining to information security and met with officers and staff with information security responsibilities throughout the Board. To test security controls and techniques, we selected four applications for review and evaluation that provided representative coverage across the Board's information technology platforms and divisions/offices. The table below shows the platform and division or office for each application included in our review. We performed our control tests using a modified version of the National Institute of Standards and Technology (NIST) Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*. We also followed up on open issues from prior control reviews.

³The *Distributed Processing Security Support Manual* contains safeguards specific to distributed processing environments, such as personal computers, external network connectivity, local area networks, wide area networks, and telephonic systems. The *Mainframe and FEDNET Security Support Manual* contains safeguards specific to mainframe computers and FEDNET Communications equipment.

Applications Included in Office of Inspector General (OIG) Control Testing

APPLICATION	PLATFORM	DIVISION/OFFICE
Currency Ordering System (COS)	Mainframe	Reserve Bank Operations and Payment Systems
Restricted-Controlled Information Transmission System (RITS)	Distributed	Office of the Secretary
Home Mortgage Disclosure Act (HMDA)	Mainframe	Consumer and Community Affairs ⁴
Research, Statistics, Supervision, and Discount (RSSD)	Mainframe	Banking Supervision and Regulation

To evaluate the Board's compliance with FISMA, we followed up on the status of the recommendations made in our prior independent evaluations of the Board's information security program and practices.⁵ We also reviewed the methodologies developed by Board staff and independent Board consultants for performing system control reviews. Finally, we compiled information on those areas for which OMB requested a specific response as part of the agency's annual FISMA reporting. Our audit was conducted in accordance with generally accepted government auditing standards.

FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

Overall, we found that the Board's information security practices are generally effective. Our security control tests of four applications and our follow up work on the recommendations of prior control tests did not identify any major security control weaknesses. All of the applications we reviewed had completed security plans, risk certifications, and contingency plans; and, the business areas supported by these applications had completed updated risk assessments. The documentation we reviewed was thoroughly prepared and we identified several examples (such as the documentation for COS and HMDA) that could be used as models for other applications at the Board in addressing the requirements for FISMA.

Although our testing did not identify any major weaknesses, we found several areas where controls needed to be strengthened. Given the sensitivity of the issues involved, we are providing the results to management under separate restricted cover. We plan to follow up on our recommendations as part of our future information security audit activities. Because several

⁴ HMDA is maintained by the Board on behalf of the Federal Financial Institutions Examinations Council. The Division of Consumer and Community Affairs is the primary user of the system at the Board.

⁵ See our *Report on the Audit of the Board's Information Security Program* (A0205), dated September 2002.

of the issues were systemic across the applications we reviewed this year and in prior years, we are developing a separate restricted summary report for management with recommendations to address these issues from a Boardwide perspective. We also may include these areas in future audit or evaluation work that compliments our annual FISMA independent evaluation. Our follow-up work on prior control tests allowed us to close all outstanding recommendations although we identified one broader issue pertaining to documenting and tracking remedial actions which we have included as part of our compliance discussions below (see recommendation 7).

We also found that the Board continues to make progress in developing a structured information security program as envisioned by the previous and current security-related legislation. Specifically, a direct reporting relationship has been established between the ISO and the CIO for security matters, although the ISO remains within IT. The ISO developed a high-level Boardwide security plan that outlines the security program's purpose, scope, and objectives and describes the principles and practices used by the Board to secure information. During the past year, the Board has completed additional application security plans and related security control reviews. In addition, the ISO has issued security incident guidance and ensured that updated risk assessments have been completed by all Board divisions and offices.

Notwithstanding the actions above, the Board has not achieved full compliance with FISMA's requirements and issues remain open on five of the seven recommendations from our original 2001 information security report. Specifically:

- The roles and responsibilities of the CIO and ISO have not been clearly defined and documented, and given the responsibilities established by FISMA for these individuals, we are concerned that the CIO and ISO are not properly positioned to carry out their responsibilities effectively.
- The Boardwide security program, although drafted, has not been issued by the CIO and its applicability to information systems maintained by contractors and other organizations, to including the Reserve Banks, has not been clearly established.
- The Board lacks a consistent process for identifying major information systems and the Board's application inventory has not been finalized.
- Although additional control reviews have been completed, we believe there are other more cost-effective approaches to conducting these reviews.
- The Board still lacks a comprehensive information security awareness program.
- Although a framework has been established for tracking corrective actions on control weaknesses, there is no process to ensure that all weaknesses are identified or that sufficient documentation is maintained to substantiate actions taken.

We recognize that the Board, along with other government agencies, is still transitioning from implementing the requirements outlined in GISRA to those contained in FISMA and that

guidance from OMB was only recently provided. The new legislation, however, establishes essentially the same requirements for information security and we are concerned that sufficient action has not been taken over the past year to close more of the recommendations from our prior information security reports. We believe that one of the reasons the Board has not achieved full compliance with FISMA's requirements is that the Board's decentralized, collegial operating environment differs from the structured, top-down framework for information security management envisioned by the security legislation.

This report updates our prior recommendations using the concepts, terms, and requirements contained in FISMA. In our opinion, fully implementing these recommendations is essential for the Board to firmly establish the necessary managerial responsibilities, oversight structure, and clear, consistent guidance related to the Board's information security program; to bring itself into compliance with the security legislation's requirements; and to establish the organization and programmatic framework that is intended by the legislation.

1. We recommend that the Administrative Governor (a) establish a full-time CIO; and (b) clearly define the roles and responsibilities of the CIO to ensure that all security responsibilities under FISMA are addressed.

FISMA reiterates GISRA's requirements that the CIO have responsibility for providing a strategic view of the agency's architecture and crosscutting security needs. FISMA continues to direct agency CIOs to develop, implement, and maintain an agencywide information security program; assist senior agency officials concerning their responsibilities; and describe the security program in detail in an agencywide security plan. The CIO is to participate in developing agency performance plans to establish the budget, staffing, training resources, and time periods required to implement the security program. The CIO must also ensure that the agency's security programs are fully integrated into the agency's enterprise architecture and capital planning and investment control processes. In addition, the CIO is to work with the agency's program officials in reviewing the information security program on an annual basis.

The CIO's responsibilities, originally enumerated in the Clinger-Cohen Act of 1996, have evolved to encompass requirements stemming from various laws, regulations, and executive orders. These include responsibility for electronic government from the E-Government Act; responsibility for defining agency information needs from the Paperwork Reduction Act; and responsibility for protecting critical infrastructure from Presidential Decision Directive 63.

The Staff Director for Management is currently fulfilling the CIO function for the Board. In that role, he has taken steps to implement the requirements of FISMA and the legislation and executive order cited above. However, the Staff Director also has responsibility for all Board administrative functions, including human resources, finance and accounting, information technology, equal employment opportunity, and continuity of operations planning. We are concerned that the myriad of responsibilities assigned to the Staff Director preclude him from effectively carrying out the broad responsibilities invested in the CIO by FISMA and other legislation. The lack of a full-time CIO has, in our opinion, contributed to key elements of

FISMA not yet being fully implemented and could inhibit a consistent Boardwide approach to complying with FISMA's requirements.

We understand that the Staff Director is considering delegating to the director of IT certain CIO responsibilities to the director of IT, including the CIO's responsibilities under FISMA as well as the responsibility to review privacy impact assessments required by the Paperwork Reduction Act. While we support the Staff Director's divestiture of CIO responsibilities, we are concerned whether a partial delegation will be effective or whether it will create confusion as to who has responsibility for which particular CIO-related functions. We also question whether the IT director's organizational position is the most effective position for establishing Boardwide policies and ensuring compliance with FISMA. The director's operational responsibilities could also create the appearance of a conflict of interest with the broader oversight role. We believe the Administrative Governor should thoroughly review all of the CIO's responsibilities and decide how best to delegate the function to achieve maximum efficiency and effectiveness.

As stated in our previous reports on the Board's information security program, we also believe that the Administrative Governor needs to clearly define all of the roles and responsibilities of the CIO, given the significant, agencywide responsibilities that FISMA and other legislation establish for this position. This will help ensure that the requirements of the position and the interrelationships with other senior officials (such as the chief information assurance officer) are understood by all concerned. We note that the ISO recently completed a draft Information Security Program (as discussed in recommendation 3) which describes the Staff Director's role as the Board's CIO. Although the description is at a high level and provides few details, we found that the Legal staff is in the process of reviewing pertinent legislation to identify all CIO responsibilities. We believe that using the two documents together would enable the Board to clearly articulate the CIO's wide array of responsibilities, including those related to information security. This would also provide a better foundation for deciding what responsibilities should be delegated and to whom. Properly positioning the Board's CIO and clearly defining the expectations of the position are, in our opinion, requirements to effectively implementing our other recommendations.

2. We recommend the Staff Director (a) establish a direct reporting relationship between the CIO and the ISO; (b) establish a separate policy and compliance function reporting to the ISO; and (c) clarify the associated roles and responsibilities.

GISRA directed the CIO to designate a senior agency information security official that reported to the CIO or a comparable individual within the agency. The official's responsibilities were to include reporting to the CIO on the implementation and maintenance of the agency's information security program and policies. FISMA broadens these requirements by providing additional expectations regarding the ISO. Specifically, FISMA requires agencies to designate a senior agency information security officer to carry out the CIO's responsibilities under the legislation, have information security duties as that official's primary duty, and head an office with the mission and resources to assist in ensuring agency compliance.

In our previous reports on the Board's information security program, we recommended that the CIO reevaluate the ISO's organizational placement within IT. We were concerned that the ISO was not properly positioned within the Board's organizational structure to effectively carry out his information systems security responsibilities, particularly since the ISO also had operational responsibilities. To address these concerns, the CIO established a reporting relationship between the CIO and the ISO regarding agencywide information security and FISMA compliance issues and he removed the data center operations from the ISO's span of control.

Despite these changes, we remain concerned that the ISO still lacks the organizational placement to properly fulfill his responsibilities. The ISO continues to report to IT management regarding day-to-day security administrative issues. Although the ISO no longer has ongoing day-to-day operational responsibilities for the data center, the Board's Mainframe Systems Unit still reports to him. This unit has responsibility for managing the operating systems, database and other environmental software on the Board's mainframe computer; the ISO estimated that oversight of this function occupies about fifteen to twenty percent of his time. As noted in our prior reports, operational responsibilities could create a conflict of interest with performing other information security activities as required by FISMA. In our opinion, these responsibilities also detract from the time required for the ISO to effectively perform his broader information security functions.

Our previous recommendation envisioned an independent information security function, headed by the ISO, with a reporting line to the CIO rather than to operational information technology management. We continue to believe this would enhance the ISO's ability to focus on security issues and ensure a more direct route to senior management on matters that have Boardwide implications. We recognize, however, that should the Staff Director decide to delegate some of his CIO responsibilities (including the security-related responsibilities under FISMA) to the director of IT, the delegation will complicate moving the ISO outside of IT. Having the ISO report directly to the director of IT (now in her capacity as CIO) is not, in our opinion, ideal, especially given the delegation-related concerns identified in our first recommendation. This relationship would, however, at least establish the direct linkage between the CIO and ISO that we believe is essential. As discussed below, clearly defining the ISO's role from a Boardwide perspective will help ensure that the position is not viewed as an IT-centric function. The relationship must also provide for sufficient ISO independence to resolve conflicts between the IT director's divisional role of ensuring the availability of information systems and the rapid delivery of technology with the ISO's role for establishing and enforcing the proper controls to ensure confidentiality and integrity. The ISO's mainframe responsibilities should also be realigned with another IT manager, allowing the ISO to focus solely on information security issues.

To further enhance the abilities to carry out the responsibilities invested in the position under FISMA, we believe the ISO needs a dedicated policy and compliance function. The ISU, which reports directly to the ISO, presently has responsibility for monitoring the security of the Board's infrastructure, intervening as required to address security exposures, and acting as liaison to the System groups coordinating Systemwide security issues. Although the ISU has worked with the ISO to take a more proactive role in providing guidance to divisions and offices on information systems security matters, such as providing guidance for control reviews and risk assessments, we found that the unit's activities over the past year have focused more on operational issues

such as virus response, patch management, network scanning, and password cracking. We are also concerned that the unit's functions related to virus control and patch management could easily increase going forward, thus taking time away from assisting with the higher-level policy and oversight responsibilities. The day-to-day operational responsibilities could also pose a conflict of interest with the responsibility for enforcing compliance with established policies and guidance.

We believe that establishing a separate policy and compliance function underneath the ISO would assist the ISO in fulfilling his responsibilities under FISMA. The function could help develop policy and guidance and enforce consistent security requirements Boardwide. Establishing this function would also provide an alternate means of conducting security control reviews, thus reducing the Board's reliance on outside consultants.⁶ The compliance function should remain separate from the ISU's operational function (although both can report to the ISO) to provide a sufficient level of independence.

As noted in our previous reports, the CIO needs to clarify the ISO's responsibilities, authority, and accountability. Our review of the draft Information Security Program showed that it lists many of the functions the ISO performs. What is lacking, however, is the unambiguous language in the security legislation that the ISO has been designated by the CIO to carry out the CIO's FISMA responsibilities, including ensuring agency compliance with the law's requirements. We believe that clearly establishing that the ISO's authority derives from the CIO (as required by FISMA) and that such authority is agencywide is necessary to invest the ISO (and any policy and compliance staff reporting to him) with the responsibility for providing guidance and direction Boardwide, for ensuring that FISMA's requirements are implemented in accordance with established guidelines, and to be in full compliance with the legislation. This could be accomplished by adding additional detail to the Information Security Program, ensuring that job descriptions are updated with these requirements, or developing more detailed guidance documents. Whatever mechanism is selected, clearly communicating the requirements across the Board will help ensure that all staff understand the expectations that have been placed on the ISO and ISU, as well as reinforcing their authority for providing information systems security guidance across the Board.

3. We recommend that the CIO finalize the Boardwide security program and clearly establish the program's scope regarding third parties such as contractors, the Reserve Banks, and other organizations.

GISRA and subsequent OMB guidance directed agency CIOs to develop, implement, and maintain an agencywide security program that assessed risk and provided adequate security for the operations and assets of all agency programs and systems. FISMA reinforces this requirement and directs that the program provide information security for all information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other organization.

⁶ Recommendation 5 provides additional information regarding the Board's approach to conducting these reviews.

The ISO recently completed a high-level Boardwide security plan that outlines the security program's purpose, scope, and objectives and describes the principles and practices used by the Board to secure information. We encourage the CIO to finalize and distribute the plan to all users of Board applications and systems to firmly establish the framework for the Board's information security program and to ensure that the program's requirements are clearly understood by everyone. Because the plan is at a high level, the CIO will also need to establish a process to provide more detailed information to support the overall program. Areas where additional information would be helpful include guidance on how to define major applications and major information systems, conduct security control reviews, define individuals with significant security responsibilities, and document corrective actions taken on identified weaknesses and vulnerabilities. Detailed guidance will be especially important if the Board transitions from following guidance established by the ISM to guidance provided by NIST and related sources. More detailed guidance will help in applying the new security requirements to the Board's information technology and cultural environment.

In finalizing the Board's information security program, the CIO also needs to clearly establish the program's scope regarding contractors, the Reserve Banks, and other agencies. As presently drafted, the program states that it ". . . is applicable to all systems used and operated by third parties for the Board and to all information collected or maintained by a third party for the Board." We note, however, that there is limited guidance in the remainder of the document on how to apply components of the program (such as risk assessments, security plans, and control testing) to systems maintained by third parties. The document also states that ". . . although it may impact the Reserve Banks insofar as Reserve Bank activities support the operations and assets of the Board, the program is not intended to affect the operations of the Reserve Banks generally. In this regard, while the Board and Reserve Banks share information about security and assistance in, among other areas, security testing, except in the context of the Board's exercise of its power of general supervision, they do not share, transfer or assign any responsibility, authority or liability for the security of their respective information technology." We believe the latter statement creates confusion as to the applicability of FISMA to Reserve Bank systems and applications, particularly those supporting the Board's delegated supervision and regulation program which we believe fall under FISMA's definition as directly supporting the Board's programs and operations. We know that the ISO has begun working with Legal to more clearly define FISMA's broader applicability and that the program document will evolve as the scope becomes clearer. As the program evolves, the CIO should ensure that either the program or the more detailed guidance is updated to reflect the program's requirements for contractors, Reserve Banks, and other organizations.

4. We recommend that the CIO (a) clearly define and communicate the requirements for major and nonmajor information systems and (b) ensure all information systems operated and maintained on behalf of the Board are included on the Board's inventory.

FISMA requires each agency to develop and maintain an inventory of major information systems operated by or under the control of the agency. An inventory of each agency's major information systems has been required for many years by the Paperwork Reduction Act. The inventory forms the basis for FISMA's periodic testing requirements, and is to include the identification of

interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency.

The Board's ISO has developed an inventory of 123 Board applications and systems. The list includes major applications, general support systems, and other applications with varying degrees of security requirements. The ISO recently worked with the ISC representatives to refine the inventory and identify any additional applications which should be designated as major. We found, however, that neither the CIO nor the ISO have established clear requirements for defining a major application or system. The ISO told us that he considers factors such as contingency recovery timeframes and the application's availability, confidentiality, and integrity risks in deciding which applications or systems should be designated as major. This approach is consistent with recent OMB guidance which provides a definition of "major application" (based on relative risk and security concerns) as well as a definition of "major information system" (based on development cost, importance to agency mission, or support of an item on the President's Management Agenda). We believe the CIO should include the ISO's approach for updating the Board's inventory in the Information Security Program to ensure the guidance is consistently implemented Boardwide. The CIO should also ensure the guidance incorporates all factors in OMB's guidance regarding major applications and major information systems (including cost and importance to the Board's primary mission areas) to provide a robust definition for all divisions and offices to use. A clear distinction as to which applications or systems are considered major will also facilitate the scheduling of security control reviews by establishing those which must be reviewed every year.

The current inventory also does not include applications or systems maintained by contractors, Reserve Banks, or other agencies. As noted in recommendation 3, the ISO has been working with Legal to develop an approach for determining which systems maintained by third parties are subject to the Board's information security program. Because these systems may also have interfaces with other Board systems and applications, completing this portion of the inventory should be a priority in the coming year. Having a complete inventory will also assist the CIO and ISO in understanding the effort involved to ensure the Board's information security program is properly applied to these applications.

5. We recommend that the CIO develop alternative methods for conducting information security reviews and provide additional guidance for conducting the reviews.

FISMA, like GISRA, requires agency program officials to periodically test and evaluate information security controls and techniques to ensure they are effectively employed. FISMA also looks to NIST to develop the standards and guidelines necessary to assist agency officials in fulfilling this responsibility. Over the past three years, the Board has employed various approaches for conducting control reviews. Several divisions have performed the reviews in-house, using managers in one business function to review applications in another function. Conversely, although ISU staff performed some reviews during the second year GISRA was in effect, IT has relied primarily on outside consultants to perform reviews of the applications that IT maintains. The in-house and external reviews have also employed differing methodologies,

although our review showed that the basic elements of the NIST guidance were addressed in the review programs.

We believe the CIO should review the Board's current approach of contracting for the majority of the control reviews and determine if an alternative, more cost-effective approach can be employed. OMB guidance notes that the depth and breadth of FISMA reviews depends on several factors, including risk, the level of documentation and monitoring, and the relative completeness of the most recent past review. Guidance on conducting reviews in OMB Circular A-130, Appendix III, states only that the review should be independent of the manager responsible for the application; there is no requirement that it be performed by an external party.

While the use of outside consultants may have assisted the Board in establishing a baseline of reviews for compliance with GISRA and FISMA, by the end of September 2003, the Board will have spent over \$800,000 during the past three years for a total of thirty-seven reviews from two consulting firms.⁷ We found that the consultant initially used by the Board provided limited documentation, other than a final report, in support of the work performed. Although the ISO has a closer working relationship with the current consultant conducting reviews, the consultant's contract is silent as to the level of documentation to be provided. We are concerned that insufficient support can hinder the effective implementation of corrective actions and precludes the retention by Board staff of knowledge gained during the reviews.

To address these concerns, the CIO should determine if additional reviews could be conducted with Board staff. This would potentially reduce the cost of conducting the reviews and ensure that information gained during the review remained within the Board. Establishing a separate compliance function under the ISO would be one means to implement this recommendation. The CIO could also look to IT's quality assurance staff since these individuals are already tasked with ensuring compliance with established quality policies, standards, procedures, and guidelines and with conducting system testing as part of application development efforts. In addition, the CIO could task IT managers in one business area to review applications maintained by a different manager. The reviews could even be performed by business-line managers with sufficient guidance provided by the CIO and ISO.

Our discussions with the ISO showed that he was generally aware of the approaches being used by divisions conducting their own reviews, but that he had not provided guidance to (1) ensure that staff performing the reviews were sufficiently independent and possessed the necessary skills or (2) establish the level of detail required (such as basic documentation) to support the conclusions reached and substantiate that the methodology was followed. We believe this is an important step to ensure reviews meet the requirements established by NIST. If additional reviews are brought in-house and a greater number of individuals are performing reviews, the ISO's approval of review methodologies and his follow-up on the implementation of those methodologies will be even more important to achieve consistency across all divisions/offices and applications.

⁷ This includes ten separate reports on the Board's general support system.

6. We recommend that the CIO establish additional proactive measures to promote security awareness and enhance the security training program for individuals with significant security responsibilities.

FISMA tasks the head of each agency with ensuring that the agency has trained personnel sufficient to assist the agency in complying with FISMA and related policies, procedures, standards, and guidelines. Specifically, FISMA requires the agencywide information security program to include security awareness training to inform 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 the CIO to train and oversee personnel with significant responsibilities for information security.

We found that the Board has taken steps over the past year to develop a proactive security awareness program. The Board continues to train new employees and contractors during orientation and IT has developed an on-line security self-test for all staff and contractors with access to the Board's network. IT employs password cracking tools to identify weak passwords and, when weak passwords are identified, employees are notified and procedures for developing a strong password are explained. IT periodically posts articles on *Inside the Board* related to computer viruses and other information security issues, and the division developed an information security web page which includes information on policies, viruses, and security-related tips. We found, however, that the number of *Inside the Board* articles has actually declined from the previous year and the security awareness page has not been routinely updated. For example, the last update on the awareness page for viruses was in January 2003, and the last update regarding tips and national warnings was in July 2002. The lack of regular updates reduces the page's value in making security awareness more of an ongoing/continuous process.

The System is currently developing a Systemwide awareness program. The program will include internet-based employee training, security awareness videos, and a security newsletter. The ISO plans to utilize portions of this program although nothing will be available until second quarter of 2004. While we endorse the Board's participation in the Systemwide effort, we believe that, in the interim, the Board can adopt additional proactive measures. These measures would include routinely updating the Board's security awareness page, which could encompass information and tips that other agencies have typically placed on posters and various giveaways to sustain employee interest in security awareness. Another proactive measure that we previously recommended, and continue to endorse, is to require each employee to acknowledge, in writing, that they have read and that they understand the Board's information security requirements and that they are aware of the penalties for failing to comply. This could be incorporated into the annual on-line self test.

In addition to establishing a broader security awareness program for all staff, we believe the CIO should enhance the security training program for those individuals with specific information security responsibilities. The ISO has requested that each division and office identify staff with significant security responsibilities and, for each staff member identified, report the types of information security and technical classes, conferences, and seminars attended. The divisions and offices are responsible for identifying the training courses they believe are appropriate. We

believe that the CIO should use the information gathered from the divisions and offices to identify specific Boardwide training requirements. Establishing a benchmark will help promote consistency and ensure that the Board maintains a high-quality, security-conscious technology staff. The requirements could be in the form of recommended classes or the CIO could use the Board's training infrastructure to provide in-house information security training. For example, the ISU recently provided security training to one division and it was well received. We believe this could be a cost-effective measure for meeting the training requirements contained in FISMA. The CIO will also need to develop procedures to ensure contractors and other organizations that use or operate Board information systems are complying with FISMA requirements for security awareness and training.

7. We recommend that the CIO enhance the process of prioritizing, tracking, and managing security performance gaps on a consistent Boardwide basis by determining what information the divisions and offices should report and what documentation they should retain.

OMB guidance requires agencies to prepare and submit POA&Ms for all programs and systems where an information technology security weakness has been found. The guidance directs CIOs and program officials to develop, implement, and manage POA&Ms for all programs and systems they operate and control. The plans should include all security weaknesses found during any review done by, for, or on behalf of the agency, including General Accounting Office audits, financial system audits, and critical infrastructure vulnerability assessments. These plans should be the authoritative agencywide management tool. In addition, program officials should, at the direction of the CIO, regularly update the CIO on their progress implementing corrective actions to enable the CIO to monitor agencywide remediation efforts and provide the agency's quarterly update to OMB.

The Board submitted its initial POA&M to OMB in November 2001, and the ISO has established a process for updating the POA&M and submitting it to OMB on a quarterly basis. The process does not, however, ensure that all deficiencies are included on the POA&M and no specific guidance has been provided to divisions and offices as to what information should be tracked at the division level. For example, at least one division is not reporting issues identified during annual control reviews because the division takes corrective action as soon as the deficiencies are identified. While some minor deficiencies may not need to be included on the agency's POA&M, we believe the CIO needs to provide guidance to the divisions and offices on what issues to report, even if they simultaneously report that the problems have been corrected. This will help the ISO identify potential trends and establish a reference tool for identifying corrective actions should similar issues occur elsewhere at the Board. The CIO should also remind the divisions and offices that issues may arise not only from annual control tests, but through any review or evaluation. These changes will establish the POA&M as the agencywide management tool as envisioned by OMB and allow the CIO and ISO to better identify Boardwide security-related issues and to prioritize, track, and manage all Board efforts to identify and close security gaps.

We also believe the CIO needs to provide guidance on what documentation is required at the division level to track issues and substantiate that corrective actions have been taken. While OMB recognizes that the CIO or ISO will be the focal point for managing the agencywide corrective action plan, OMB also envisions that program officials will maintain POA&Ms for all systems under their control. We found that some divisions and offices maintain “action plans” which could be a starting point to maintain individual POA&Ms. However, divisions and offices are keeping very little documentation as to the steps they are taking to correct identified deficiencies. We believe that documentation is important to maintain an adequate audit trail of changes made to applications and systems and to substantiate the rationale for those changes. Documentation also provides the CIO and ISO with additional assurance that corrective actions have been taken.

ANALYSIS OF COMMENTS

We provided our report to the Staff Director for Management for comment and his response is included as appendix 1. In his response, the Staff Director partially concurred with recommendations 1 and 2. The Staff Director noted that the Board, like other small federal agencies, is challenged by the prescriptive standards contained in FISMA which he believes were written for the large, cabinet-level agencies. The Staff Director also indicated that outside reviews of the Board’s security program by an OMB representative and by a contractor working for NIST did not have any issues with the Board’s governance structure for information security. Nevertheless, the Staff Director indicated that he plans to strengthen the Boardwide emphasis regarding FISMA and look for alternative methods for meeting policy, compliance, and review responsibilities.

We agree that OMB’s emphasis on FISMA compliance has focused heretofore on the larger, cabinet-level agencies. However, we also believe that implementing the legislation’s requirements is good business practice which can be achieved with a risk-based, cost-effective approach. As the Staff Director notes in his response, and as we stated in our report, FISMA’s requirements run counter to traditional Board culture. For this reason, we continue to believe that clearly defining the CIO’s and the ISO’s central, Boardwide authority, accountability, and responsibilities is a key requirement to achieving compliance with the legislation. We are encouraged by recent efforts to finalize the security program, identify the CIO’s responsibilities as enumerated in various statutes, delegate the CIO’s responsibilities to someone other than the Staff Director, and create more of a direct relationship between the CIO and the ISO. These actions are all steps toward implementing our first two recommendations.

The Staff Director concurred with our remaining recommendations and identified actions that he will take or has already taken. Specifically, the Staff Director stated that the Boardwide security program is in final draft and efforts are underway to ensure FISMA’s requirements, including the identification of all information systems, are met regarding contractors, the Reserve Banks, and other organizations supporting the Board’s operations. The Board has established an enterprise project for 2004/2005 for policy, compliance, and review activities. In addition, additional security awareness measures are already in progress and the process of prioritizing, tracking, and managing security performance gaps will continue to be enhanced.

APPENDIXES

Appendix 1 – Division’s Comments



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

STEPHEN R. MALPHRUS
STAFF DIRECTOR FOR MANAGEMENT

DATE: September 26, 2003
TO: Barry R. Snyder
FROM: Steve Malphrus (*Signed*)
SUBJECT: Audit of the Board’s Information Security Program (A0302)

The purpose of this memorandum is to respond to the Inspector General’s (IG) audit of the Board’s Information Security Program (A0302). We agree with the IG’s findings: (1) that the Board continues to make progress in developing a structured information security program as envisioned by the Federal Information Security Management Act (FISMA) and (2) that the Board’s information security practices are effective overall. We are also in general agreement with the report’s recommendations. The seven recommendations and our responses are listed below (the IG’s recommendations are in bold).

- 1. We recommend that the Administrative Governor (a) establish a full-time CIO; and (b) clearly define the roles and responsibilities of the CIO to ensure that all security responsibilities under FISMA are addressed.**

We concur in part with the recommendation. As the Inspector General points out, the Board, like other “small” federal agencies (6,000 or fewer employees), is challenged by two very prescriptive subchapters of FISMA, which were directed to the large, cabinet-level agencies. The Board has implemented a common model for governance employed by many small agencies to address FISMA. The Office of Management and Budget (OMB), which oversees implementation of FISMA, has focused almost entirely on the cabinet-level agencies for the past two years. Recently, OMB started to work more closely with small agencies. At a FISMA conference held earlier this month, we asked our OMB representative to comment on the Board’s CIO governance structure. He indicated that he agreed with the structure. Moreover, at the recommendation of the Federal Chief Information Officers Council, we sought an outside opinion by a firm that is working on FISMA standards for the National Institute of Standards and Technology. They commented that our governance structure was “nicely done.”

We believe that deficiencies in implementing FISMA requirements result from revisions in guidance from NIST and OMB, differences between the IG and Board officials in interpreting that guidance, and not governance per se. For example, in the recommendation, the IG states that “the CIO must also ensure that the agency’s security programs are fully integrated into the agency’s enterprise architecture and capital planning and investment control processes.” From our perspective, these interrelated processes have become more integrated in past two years. We also believe the Board has a well-defined enterprise IT architecture. For example, security must be addressed when new technology is implemented in the Board’s IT architecture. Similarly, security is considered in the Board’s capital planning and investment process. We agree that sufficient written guidance is not always developed, and the Director of Information Technology will work even harder in the coming year to strengthen Boardwide emphasis on FISMA.

- 2. We recommend the Staff Director (a) establish a direct reporting relationship between the CIO and the ISO; (b) establish a separate policy and compliance function reporting to the ISO; and (c) clarify the associated roles and responsibilities.**

We partially concur with the recommendation. The ISO currently has a separate policy and compliance function reporting to him consisting of two contractors. The function was established so that IT could meet commitments to its customers and comply with FISMA. We agree with the IG that alternative methods need to be developed for

Appendix 1 – Division’s Comments

policy, compliance, and review responsibilities so that Board staff retains knowledge gained through the reviews. Roles and responsibilities will be reviewed and clarified as necessary.

3. We recommend that the CIO finalize the Boardwide security program and clearly establish the program’s scope regarding third parties such as the Reserve Banks and other organizations.

We concur with the recommendation. The Boardwide security program is in final draft and will be published soon. The IT director raised the issue regarding the program’s scope with senior Reserve Bank officials in June 2003 as well as with the director responsible for Reserve Bank oversight. As the IG noted, the Legal Division recently issued an opinion that FISMA applies to the Board’s contract with Hewitt Associates who provide human resources IT services. In 2004, we will ensure that FISMA requirements are met when the Board contracts for IT services from the Reserve Banks and other organizations.

4. We recommend that the CIO (a) clearly define and communicate the requirements for major and nonmajor information systems and (b) ensure all information systems operated and maintained on behalf of the Board are included on the Board’s inventory.

Generally, we concur with the recommendation. We believe that the requirements are defined and have been communicated. The requirements for “major” and “non-major” information systems have been conveyed to divisions. We are aware that NIST has recently drafted and circulated a document that defines a matrix to assist agencies in classifying information systems as “major” or “non-major.” We will implement NIST guidance in our classification program. In connection with Recommendation 3, we will ensure that all information systems operated and maintained on behalf of the Board are included in the Board’s IT inventory.

5. We recommend that the CIO develop alternative methods for conducting information security reviews and provide additional guidance for conducting the reviews.

We concur and will implement the recommendation in the coming year.

6. We recommend that the CIO establish additional proactive measures to promote security awareness and enhance the security training program for individuals with significant security responsibilities.

We concur with the recommendation. In 2003, we created a benchmark for training Board employees with significant information security responsibilities. We also surveyed divisions to ensure they were performing the appropriate level of needs assessment and training. Moreover, information security training was provided to network administrators. We will review opportunities to implement additional awareness measures.

7. We recommend that the CIO enhance the process of prioritizing, tracking, and managing security performance gaps on a consistent Boardwide basis by determining what information the divisions and offices should report and what documentation they should retain.

We concur with the recommendation. We will continue to enhance the process of prioritizing, tracking, reporting, and managing performance gaps in information security as gaps are identified.

cc: Marianne Emerson
Ray Romero
Bill Mitchell
Don Robinson
Peter Sheridan

Appendix 2 – Principal Contributors to this Report

Peter Sheridan, EDP Auditor and Auditor-in-Charge

Gerald Edwards, Auditor

Ariane Ford, Auditor

Robert McMillon, EDP Auditor

Paul Sciannella, EDP Auditor

William Mitchell, Senior Program Manager