**United States Department of State
and the Broadcasting Board of Governors
Office of Inspector General**

Information Technology Memorandum Report

Review of the Information Security Program at the Broadcasting Board of Governors

Report Number IT-I-05-10, September 2005

~~IMPORTANT NOTICE~~

~~This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies or organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

United States Department of State
and the Broadcasting Board of Governors

Inspector General

PREFACE

This report was prepared by the Office of Inspector General (OIG) pursuant to the Inspector General Act of 1978, as amended, and Section 209 of the Foreign Service Act of 1980, as amended. It is one of a series of audit, inspection, investigative, and special reports prepared by OIG periodically as part of its responsibility to promote effective management, accountability, and positive change in the Department of State and the Broadcasting Board of Governors.

This report is the result of an assessment of the strengths and weaknesses of the office, post, or function under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

The recommendations therein have been developed on the basis of the best knowledge available to the OIG and, as appropriate, have been discussed in draft with those responsible for implementation. It is my hope that these recommendations will result in more effective, efficient, and/or economical operations.

I express my appreciation to all of those who contributed to the preparation of this report.

Howard J Krongard
Howard J. Krongard
Inspector General

Introduction

In response to the Federal Information Security Management Act of 2002 (FISMA),[1] the Office of Inspector General (OIG) performed an independent review of the information security program of the Broadcasting Board of Governors (BBG). FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of controls over information technology (IT) resources that support federal operations and assets and a mechanism for improved oversight of federal agency information security programs. In addition, Office of Management and Budget (OMB) implementation guidance for FISMA requires OIGs to assess development, implementation, and management of the agency-wide plan of action and milestones (POA&M) process and to focus on performance measures. The specific objectives of OIG's review were to assess BBG's progress in developing its information security program and practices as they relate to FISMA and determine BBG's processes for implementing the requirements of the law.

To fulfill the review objectives, OIG held discussions with BBG officials from the International Broadcasting Bureau (IBB), Office of Cuba Broadcasting (OCB), and the transmitting station in Botswana. OIG did not conduct a review of BBG's grantee organizations: Radio Free Europe/Radio Liberty (RFE/RL), Radio Free Asia (RFA), Middle East Broadcasting Networks (MBN), and Radio Farda—a special project in conjunction with Voice of America (VOA).

In addition to discussions with BBG management and staff, OIG selected a subset of systems and performed a detailed analysis of risk assessments and security plans as well as POA&M documentation and certification and accreditation packages. The subset consisted of the Central Infrastructure Domain, Central Services Domain, Central Extranet Domain, Cuba Broadcasting Headquarters Network, Botswana Transmitting Station Network, and the Public Internet Web Site. OIG held discussions with the managers of these systems to verify the processes and procedures employed in development and submission of FISMA documentation. OIG collected other relevant supporting IT documentation as appropriate.

OIG's Office of Information Technology performed this review from July 2005 through the first week of September 2005. Major contributors to this report were Mary S. Heard and Matthew J. Ragnetti. Comments or questions about the report may be directed to Ms. Heard at heardm@state.gov or (703) 284-2656.

[1] P.L. 107-347, Title III; 44 U.S.C. 3541 et seq.

Results in Brief

OIG's evaluation of the BBG's information security program concluded that BBG has made progress in the past year in meeting FISMA requirements and is adjusting well to last year's reorganization of IT operations (see Appendix A). BBG added a 25th system to its major systems inventory and categorized all of the systems based on risk impact levels as required by Federal Information Processing Standards (FIPS) Publication 199. BBG completed certification and accreditation for 28 percent (7 of 25) of its major systems. Ninety-two percent (23 of 25) of the major systems have risk assessments, system security plans, and POA&Ms. Also, BBG developed agency-wide POA&Ms to address findings reported in previous OIG FISMA reviews and site inspections. Lastly, BBG deployed a new security awareness training program for FY 2005 that has had positive reviews.

[redacted] BBG's method of tracking POA&Ms is cumbersome and has resulted in lapsed milestones. Finally, BBG has not completed development of an agency-wide enterprise architecture, a recommendation from last year's OIG report and a requirement since 2002. BBG concurred with OIG's recommendations and is moving forward to implement the recommendations. BBG's comments on a draft of the report are reproduced in Appendix B.

Background

The U.S. International Broadcasting Act of 1994[2] created BBG as a self-governing element within the former United States Information Agency, which provided limited administrative, technical, and management support to BBG. The Foreign Affairs Reform and Restructuring Act of 1998[3] granted BBG independence from United States Information Agency on October 1, 1999. With the exception of limited Department of State broadcasting, BBG is responsible for overseeing all U.S. government-funded civilian broadcasting, including the operations of IBB, which includes VOA and OCB. BBG also oversees four grantee organizations: RFE/RL, RFA, MBN, and Radio Farda, a joint effort of RFE/RL and VOA that complements VOA's Persian-language radio and television broadcasts into Iran.

Information security is an important consideration for any organization that depends on information systems and information networks to carry out its mission. The dramatic expansion and rapid increase in the use of the Internet has changed the way the U.S. government, private sector, and much of the world communicate and conduct business. However, without proper safeguards, this widespread interconnectivity poses significant risks to the infrastructure it supports and makes it easier and relatively inexpensive for individuals and groups to eavesdrop on government operations, obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other information networks and systems. The war on terrorism and recent

[2] P.L. 103-236, Title III, Sec. 301 et seq.

[3] P.L. 105-277.

terrorist attacks underscore the need to maintain information security in order to continue program broadcasting to BBG audiences relying on impartial reports via satellite television and radio. These transmissions can be direct to home, to affiliates for rebroadcast, or to IBB-owned stations and frequencies for broadcasting. U.S. broadcasting initiatives, which use information systems and information networks to complete their mission, counter the efforts of local and state-sponsored newspapers and broadcasters that portray the United States as anti-Muslim.

Faced with continued concerns about information security risks to the federal government, Congress passed and the President signed FISMA into law in December 2002. The law provides a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support federal operations and assets and a mechanism for improving oversight of federal agency information security programs. Also, FISMA and OMB implementation guidance specifically:

- require agency OIGs to assess the development, implementation, and management of the agency POA&M process;
- require agency development of minimum standards for agency systems;
- introduce a statutory definition for information security;
- define agency IT security responsibilities; and
- broaden the scope of the Clinger-Cohen Act[4] to include federal information systems used or operated by contractors acquired for use on federal contracts.

FISMA and OMB implementation guidance also require that each agency:

- develop and maintain a major information systems inventory;
- develop system configuration requirements;
- perform annual periodic testing and evaluation of systems;
- include provisions for continuity of operations in its security program;
- have a qualified senior agency information security officer report to the Chief Information Officer (CIO); and
- send annual reports to OMB and various congressional committees.

Overview of BBG's Information Security Program

In February 2001, OIG found that BBG did not have a documented information security program or written policies and procedures covering information security. During 2001, BBG's senior management began taking actions to develop its IT security program by appointing a CIO who drafted a framework for the BBG information security program and started developing security plans to protect BBG's mission-critical systems. During its 2002 Government Information Security Reform Act (GISRA) evaluation,[5] OIG noted that BBG was making progress in developing its agency-wide information security program by completing program-level self-assessments and documenting the results in its quarterly reporting of the agency's

[4] Information Technology Management Reform Act of 1996, P.L. 104-106, Div. E; 40 U.S.C. 11101 et seq.

[5] *Information Security Program Evaluation: Broadcasting Board of Governors* (IT-A-02-07, Sept. 2002).

POA&M to OMB. OIG's 2003 FISMA evaluation[6] reported that BBG had made limited progress in complying with the requirements of FISMA.

In April 2004, Congress approved, and on May 30, 2004, BBG implemented, a reorganization consolidating all IT functions into a common program area, the Office of Engineering and Technical Services. BBG designated the director of this office as the Chief Technology Officer (CTO) and appointed a Chief Information Security Officer (CISO). To meet 2004 FISMA requirements, BBG defined 24 major systems, performed risk assessments, and developed general support system and major application system security plans, operating system security configuration standards, and patch management policies. Additionally, BBG developed an agency-wide incident response plan, an IT security awareness training program, and POA&Ms for ten of its 24 major systems. Despite the progress, OIG found that BBG did not have an enterprise architecture or capital planning and investment control process in place, and transmitting stations overseas were not receiving sufficient guidance for meeting FISMA requirements.

OIG closed 11 of its 12 recommendations from the GISRA 2002 and FISMA 2003 and 2004 evaluations. BBG continues to work toward closing the remaining recommendations by implementing actions designed to improve the overall information security program, including development of an agency-wide enterprise architecture.

Review Findings

BBG continues to make progress in developing its information security program to meet FISMA requirements after consolidating disparate units under one IT authority. BBG's continued efforts to respond to FISMA reporting requirements, as well as OIG's inspection work at the transmitting station in Botswana, have revealed additional areas where BBG is considering reorganizing IT operations to improve information security and compliance with FISMA. OIG supports BBG's progress in developing its information security program and encourages BBG senior management and staff to continue developing the program to comply with FISMA requirements and National Institute of Standards and Technology (NIST) guidance.

Progress in Meeting FISMA Requirements

In the FY 2002 GISRA evaluation, OIG disagreed with BBG's approach in grouping all systems within five functional areas because this organizational structure did not meet GISRA security requirements. During the FISMA evaluation of BBG in FY 2003, OIG reported that the BBG CIO had neither the time nor the IT qualifications to carry out the CIO's role and had not assigned a senior agency information security officer and information system security officers. Also during FY 2003, IBB's director noted several IT operational deficiencies and areas for improvement and hired a contractor to perform an independent review of BBG's IT services, management, and operations. The independent review identified a lack of effective communication and collaboration among program areas and recommended a restructuring of BBG's IT organization.

[6] *Review of the Information Security Program at Broadcasting Board of Governors* (IT-A-03-14, Sept. 2003).

In April 2004, Congress approved, and on May 30, 2004, BBG implemented, a reorganization of its IT management structure, responsibilities, and functions by consolidating overall IT program management under the Office of Engineering and Technical Services. BBG named the director of the Office of Engineering and Technical Services as the CTO, with responsibility for all engineering and transmission service functions, and added a new consolidated Information Technology Directorate. BBG appointed a qualified CIO and CTO to direct and oversee a broad range of statutory functions, including meeting the FISMA requirements. The CIO reports directly to the Board of Governors on all IT matters. Lastly, BBG created and the CIO filled the CISO position that reports directly to the CIO and is responsible for overseeing and participating in planning, assessing, and testing of IT operations and ensuring compliance with FISMA.

During FY 2004, BBG took steps to meet FISMA and NIST guidance for developing an agency-wide IT security program. BBG defined 24 major systems under the Office of Engineering and Technical Services. Additionally, BBG developed operating system security configuration management policy for many of its operating systems, an incident response plan for use at headquarters, and an IT security awareness training program. BBG performed risk assessments and developed security plans and POA&Ms for ten of its 24 major systems. BBG developed a program action plan to address the lack of documentation at transmitting stations, continuity of operations plans, certification and accreditation, training of the IT support staff, POA&Ms, and vulnerability and penetration testing.

During FY 2005, BBG added a system to its list of major systems to bring the total to 25, and made significant progress in meeting FISMA requirements, as shown in Appendix A. BBG assessed and categorized all of its systems based on risk impact levels as required by FIPS 199. BBG completed certification and accreditation for seven of the 25 major systems. Risk assessments, system security plans, and POA&Ms were completed for 23 of the 25 major systems. BBG developed an agency-wide POA&M to address findings reported in previous OIG FISMA reviews and site inspections. Lastly, BBG deployed a new security awareness training program for FY 2005 that has had positive reviews.

Centralizing Management of Transmitting Station Systems

Despite the progress made toward improving its overall information security program and meeting FISMA requirements, (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)

System managers perform the risk assessments that identify potential vulnerabilities and create the system security plans and POA&Ms that outline their methodology for mitigating identified risks. The resulting documentation, as well as an independent security assessment, is included in system managers' application packages for certification and accreditation. If the information that is input into this process from the initial stages is inaccurate or incomplete, the CTO will be making an uninformed decision when accrediting systems. [redacted]

Recommendation 1: The Chairman, Broadcasting Board of Governors should direct the Chief Technology Officer to centralize, at Washington, DC headquarters, the management of computer networks located at transmitting stations overseas.

Implementing Minimum Standard Security Controls

BBG's current agency-wide security configuration policy is established and available to system managers on the computer security portion of their intranet site, which includes security configuration guides for the operating systems in use at BBG, except for Windows Server 2003, which is under development. BBG's security configuration methodology establishes a minimum baseline for security controls, with the expectation that system managers are to implement additional controls as necessary to ensure adequate protection of information systems.

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

NIST has issued a draft version of FIPS Publication 200, which will require federal agencies to implement the minimum security configuration standards recommended in NIST Special Publication 800-53. In light of this, BBG is reevaluating its information security and FISMA efforts to create a more systematic approach. The resulting documentation, including risk assessments, system security plans, and POA&Ms, should become more thorough and meaningful, thus aiding in the certification and accreditation process. OIG supports BBG in its efforts to use FISMA requirements more effectively to secure its information systems.

Recommendation 2: The Chairman, Broadcasting Board of Governors should direct the Chief Information Officer to implement information system security controls in accordance with National Institute of Standards and Technology Special Publication 800-53.

Implementing an Automated FISMA Reporting Tool

BBG currently has no automated tool for reporting progress in meeting FISMA requirements. The CISO manages the agency-wide POA&M process and has distributed reporting guidance and organized the updates. The CISO and system managers use electronic mail for updating and reporting POA&M progress. However, as more systems now have the required documentation completed and require updates, this process has become cumbersome to keep track of and has resulted in lapsed milestones.

The CISO cannot compel system managers to submit updates. BBG officials have discussed obtaining an automated FISMA reporting tool that would track submissions and automatically send reminders to system managers of impending deadlines, with copies sent to the managers' supervisors as well. OIG supports BBG in its efforts to ensure effective management of the POA&M process.

> **Recommendation 3:** The Chairman, Broadcasting Board of Governors should direct the Chief Information Officer to procure and implement an automated tool to facilitate reporting and tracking of progress in implementing Federal Information Security Management Act requirements and Office of Management and Budget reporting guidelines.

Developing an Enterprise Architecture

OIG's 2004 FISMA report stated that BBG had not developed an agency-wide IT enterprise architecture or capital planning and investment control process. BBG now has a capital planning and investment control process in place but has not fully developed an enterprise architecture. Disparate elements that comprise an enterprise architecture have been developed, such as outlining business processes and network topologies, but they have not been integrated sufficiently to satisfy the requirements of the Clinger-Cohen Act.

Reinforced by FISMA and OMB guidance, the Clinger-Cohen Act requires that agency CIOs, at a minimum, develop an enterprise architecture that includes the agency's business processes, information flows, hardware and software, data descriptions, and the IT infrastructure. The enterprise architecture will help ensure that BBG aligns its information system requirements with its business processes and provides adequate interoperability between systems, desired redundancy of systems, and necessary systems security.

> **Recommendation 4**: The Chairman, Broadcasting Board of Governors should direct the Chief Information Officer to develop an enterprise architecture that will align its information system requirements with its mission processes and provide adequate interoperability between systems, redundancy of systems, and systems security.

Recommendations

Recommendation 1: The Chairman, Broadcasting Board of Governors should direct the Chief Technology Officer to centralize, at Washington, DC headquarters, the management of computer networks located at transmitting stations overseas.

Recommendation 2: The Chairman, Broadcasting Board of Governors should direct the Chief Information Officer to implement information system security controls in accordance with National Institute of Standards and Technology Special Publication 800-53.

Recommendation 3: The Chairman, Broadcasting Board of Governors should direct the Chief Information Officer to procure and implement an automated tool to facilitate reporting and tracking of progress in implementing Federal Information Security Management Act requirements and Office of Management and Budget reporting guidelines.

Recommendation 4: The Chairman, Broadcasting Board of Governors should direct the Chief Information Officer to develop an enterprise architecture that will align its information system requirements with its mission processes and provide adequate interoperability between systems, redundancy of systems, and systems security.

Abbreviations

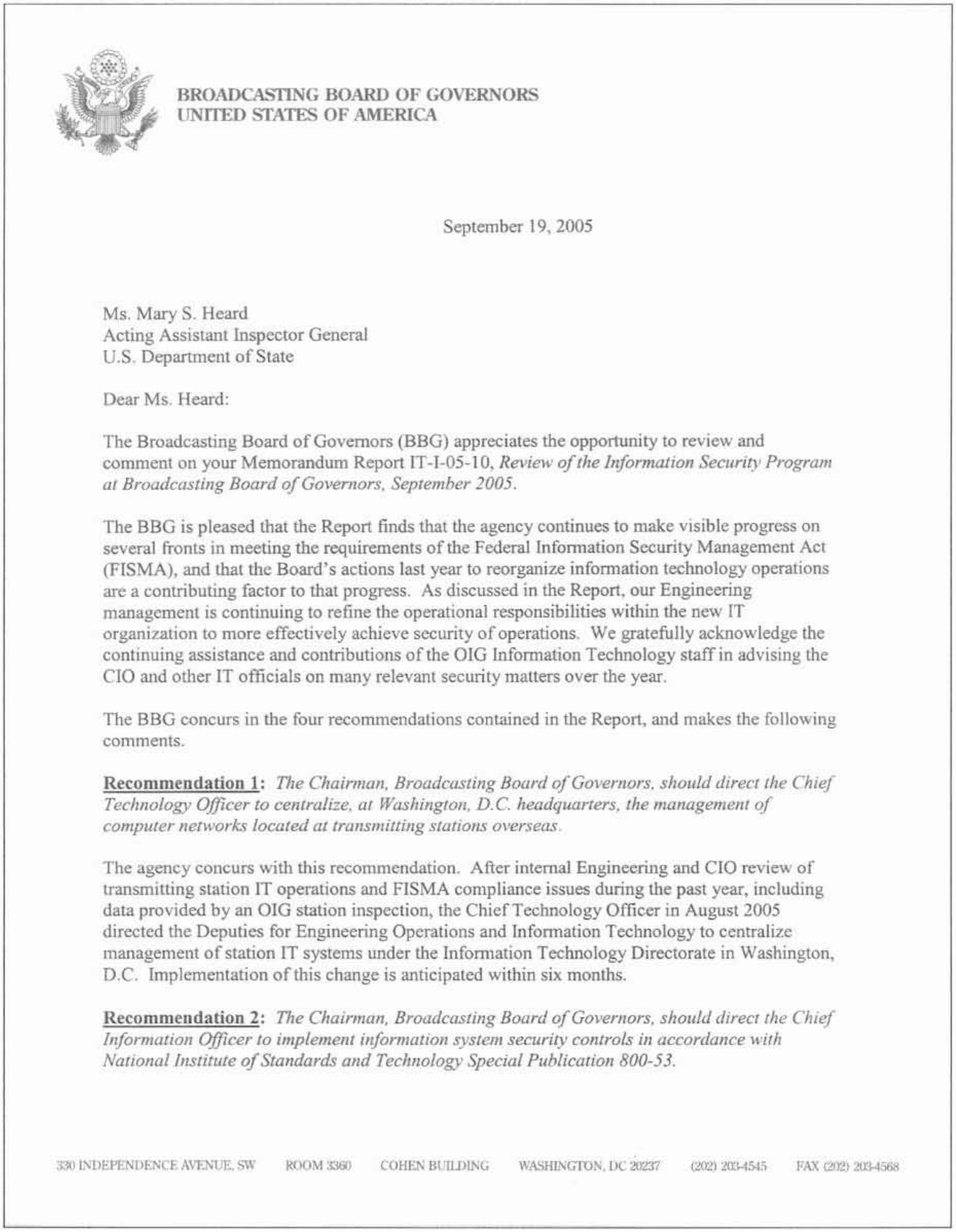
BBG	Broadcasting Board of Governors
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CTO	Chief Technical Officer
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
GISRA	Government Information Security Reform Act
IBB	International Broadcasting Bureau
IT	Information technology
MBN	Middle East Broadcasting Networks
NIST	National Institute of Standards and Technology
OCB	Office of Cuba Broadcasting
OMB	Office of Management and Budget
OIG	Office of Inspector General
POA&M	Plan of action and milestones
RFA	Radio Free Asia
RFE/RL	Radio Free Europe/Radio Liberty
VOA	Voice of America

(b) (2)

[redacted]

Appendix B

Comments From the Broadcasting Board of Governors



BROADCASTING BOARD OF GOVERNORS
UNITED STATES OF AMERICA

September 19, 2005

Ms. Mary S. Heard
Acting Assistant Inspector General
U.S. Department of State

Dear Ms. Heard:

The Broadcasting Board of Governors (BBG) appreciates the opportunity to review and comment on your Memorandum Report IT-I-05-10, *Review of the Information Security Program at Broadcasting Board of Governors, September 2005.*

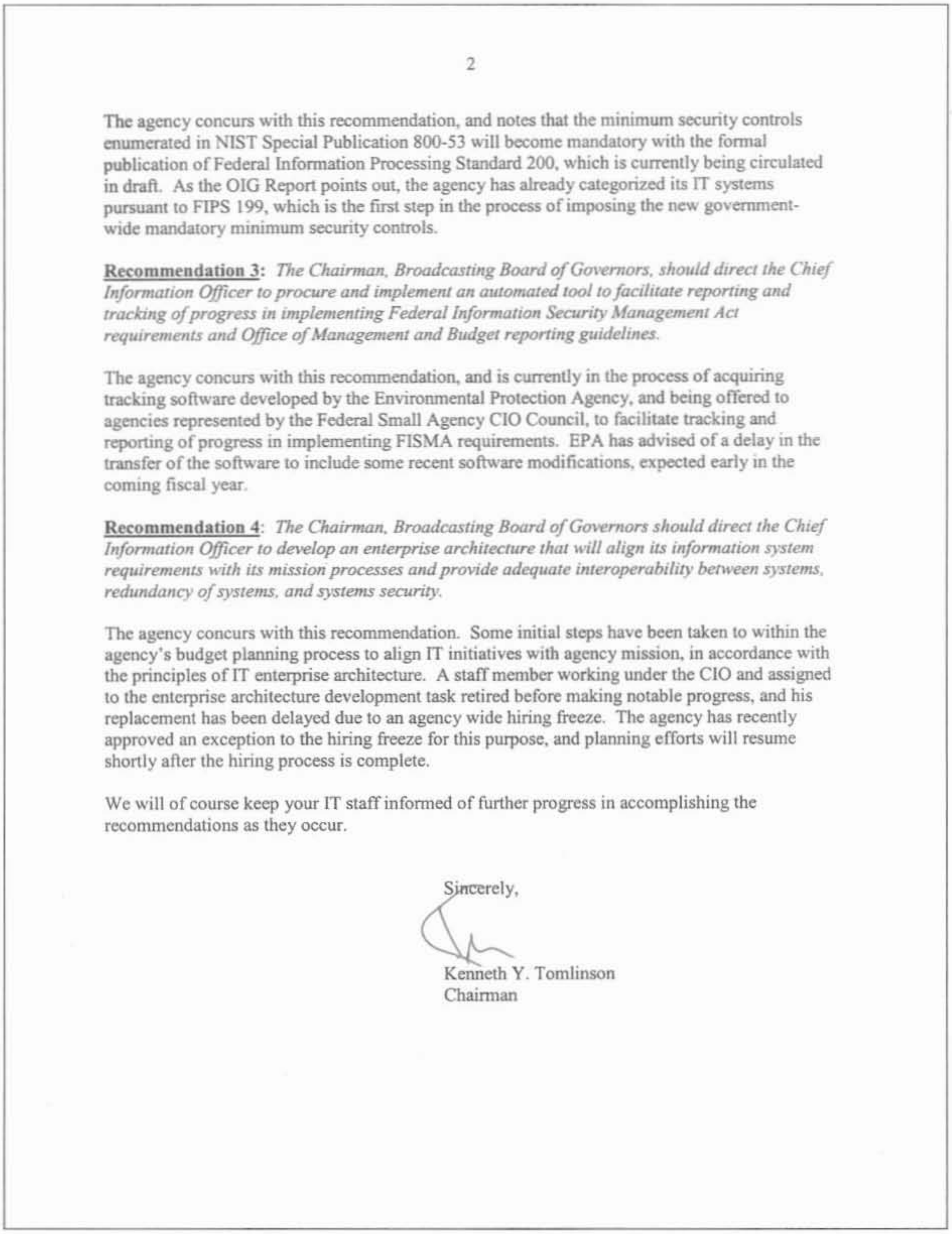
The BBG is pleased that the Report finds that the agency continues to make visible progress on several fronts in meeting the requirements of the Federal Information Security Management Act (FISMA), and that the Board's actions last year to reorganize information technology operations are a contributing factor to that progress. As discussed in the Report, our Engineering management is continuing to refine the operational responsibilities within the new IT organization to more effectively achieve security of operations. We gratefully acknowledge the continuing assistance and contributions of the OIG Information Technology staff in advising the CIO and other IT officials on many relevant security matters over the year.

The BBG concurs in the four recommendations contained in the Report, and makes the following comments.

Recommendation 1: *The Chairman, Broadcasting Board of Governors, should direct the Chief Technology Officer to centralize, at Washington, D.C. headquarters, the management of computer networks located at transmitting stations overseas.*

The agency concurs with this recommendation. After internal Engineering and CIO review of transmitting station IT operations and FISMA compliance issues during the past year, including data provided by an OIG station inspection, the Chief Technology Officer in August 2005 directed the Deputies for Engineering Operations and Information Technology to centralize management of station IT systems under the Information Technology Directorate in Washington, D.C. Implementation of this change is anticipated within six months.

Recommendation 2: *The Chairman, Broadcasting Board of Governors, should direct the Chief Information Officer to implement information system security controls in accordance with National Institute of Standards and Technology Special Publication 800-53.*



The agency concurs with this recommendation, and notes that the minimum security controls enumerated in NIST Special Publication 800-53 will become mandatory with the formal publication of Federal Information Processing Standard 200, which is currently being circulated in draft. As the OIG Report points out, the agency has already categorized its IT systems pursuant to FIPS 199, which is the first step in the process of imposing the new government-wide mandatory minimum security controls.

Recommendation 3: *The Chairman, Broadcasting Board of Governors, should direct the Chief Information Officer to procure and implement an automated tool to facilitate reporting and tracking of progress in implementing Federal Information Security Management Act requirements and Office of Management and Budget reporting guidelines.*

The agency concurs with this recommendation, and is currently in the process of acquiring tracking software developed by the Environmental Protection Agency, and being offered to agencies represented by the Federal Small Agency CIO Council, to facilitate tracking and reporting of progress in implementing FISMA requirements. EPA has advised of a delay in the transfer of the software to include some recent software modifications, expected early in the coming fiscal year.

Recommendation 4: *The Chairman, Broadcasting Board of Governors should direct the Chief Information Officer to develop an enterprise architecture that will align its information system requirements with its mission processes and provide adequate interoperability between systems, redundancy of systems, and systems security.*

The agency concurs with this recommendation. Some initial steps have been taken to within the agency's budget planning process to align IT initiatives with agency mission, in accordance with the principles of IT enterprise architecture. A staff member working under the CIO and assigned to the enterprise architecture development task retired before making notable progress, and his replacement has been delayed due to an agency wide hiring freeze. The agency has recently approved an exception to the hiring freeze for this purpose, and planning efforts will resume shortly after the hiring process is complete.

We will of course keep your IT staff informed of further progress in accomplishing the recommendations as they occur.

Sincerely,

Kenneth Y. Tomlinson
Chairman

FRAUD, WASTE, ABUSE OR MISMANAGEMENT
of Federal programs
and resources hurts everyone.

Call the Office of Inspector General
HOTLINE
202/647-3320
or 1-800-409-9926
or e-mail oighotline@state.gov
to report illegal or wasteful activities.

You may also write to
Office of Inspector General
U.S. Department of State
Post Office Box 9778
Arlington, VA 22219
Please visit our website at oig.state.gov

Cables to the Inspector General
should be slugged "OIG Channel"
to ensure confidentiality.