UNCLASSIFIED

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-A-04-07, September 2004

UNCLASSIFIED

Introduction

In response to the Federal Information Security Management Act of 2002 (FISMA),[1] the Office of Inspector General (OIG) performed an independent review and evaluation 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 met with BBG officials from the International Broadcasting Bureau (IBB), Radio Sawa, Office of Cuba Broadcasting (OCB), and two overseas transmitting stations in the Philippines. OIG did not conduct a detailed review of BBG's grantee organizations, Radio Free Europe/Radio Liberty (RFE/RL), Radio Free Asia (RFA), and Middle East Television Network, but did hold meetings and gathered relevant documentation to assess each organization's approach to handling IT information security. OIG also did not conduct a review of Radio Farda, a joint effort of RFE/RL and Voice of America. Grantees are private, nonprofit organizations that own and operate their own IT systems.

In addition to discussions with BBG management and staff, OIG performed a detailed analysis of BBG's system risk assessments and general support system and major application security plans. OIG collected other relevant supporting IT documentation as appropriate. OIG's IT staff performed this review from April 2004 through the first week of September 2004. Major contributors to this report were Lynn Allen, James Davies, Mary Heard, Anthony Carbone, and Brandon Carter. Comments or questions about the report may be directed to Mr. Davies at daviesj@state.gov or (703) 284-2673.

[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 reorganizing its IT program. As of May 30, 2004, BBG had appointed a Chief Technology Officer (CTO), a new Chief Information Officer (CIO), and a Chief Information Security Officer (CISO). Additionally, BBG defined 24 major systems; performed risk assessments; and developed general support system and major application system security plans, operating system security configuration standards, patch management policies, an incident response plan, and a user IT security training program. BBG has developed POA&Ms for 10 of its 24 systems and is working on completing the remaining 14 POA&Ms as required. The first FY 2004 quarterly report to OMB under the new reorganization structure in July identified 20 information security weaknesses within the 10 completed POA&Ms, of which two weaknesses were corrected.

Despite this progress, several key areas of information security still require management attention. BBG's CIO has not developed an agency-wide enterprise architecture as required by FISMA implementation guidance and the earlier enacted Clinger-Cohen Act.[2] Also, BBG's transmitting stations need headquarters guidance to meet information security requirements.

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

Background

The U.S. International Broadcasting Act of 1994[3] 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[4] 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 Voice of America, and OCB. BBG also oversees three grantee organizations: RFE/RL, RFA, and Middle East Television Network. Additionally, BBG oversees Radio Sawa, which is to be converted to grantee status during October 2004, and Radio Farda, a joint effort of RFE/RL and Voice of America that complements Voice of America'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 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. U.S. broadcasting initiatives, which use information systems and information networks to complete their mission, counter the efforts of local 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 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;

[3] P.L. 103-236, Title III, Sec. 301 et seq.
[4] P.L. 105-277.

- 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 CIO; and
- send annual reports to OMB and various congressional committees.

Overview of BBG's Information Security Program

OIG saw in February 2001 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 POA&M to OMB. In OIG's 2003 FISMA evaluation,[6] OIG reported that BBG had made limited progress in complying with the requirements of FISMA.

OIG closed five of its nine recommendations from the GISRA 2002 and FISMA 2003 evaluations. BBG continues to work toward closing the remaining recommendations by implementing actions designed to develop system security plans and functional-level contingency plans, complete an agency-wide information security program plan and timeline for completion of FISMA requirements, and provide each functional area with guidance to develop POA&Ms, system-level security plans, and self-assessments.

In April 2004, Congress approved and on May 30, 2004, BBG implemented a reorganization of its IT functions into a common program area, Engineering and Technical Services Directorate, which incorporated OCB, Voice of America, and IBB activities. BBG assigned the director of Engineering and Technical Services Directorate as the CTO and appointed a CISO.

In FY 2004, to meet the requirements for developing an agency-wide security program, BBG defined 24 major systems under two program areas. Additionally, BBG performed risk assessments, and developed general support system and major application system security plans, operating system security configuration standards, patch management policies, an incident response plan, and a user IT security training program. Also, BBG developed POA&Ms for 10 of its 24 major systems and provided OIG with a program action plan, which addresses BBG's approach to creating an agency-wide continuity of operations plan, system-level risk assessments, security plans, and POA&Ms.

[5] *Information Security Program Evaluation: Broadcasting Board of Governors* (IT-A-02-07, Sept. 2002).
[6] *Review of the Information Security Program at Broadcasting Board of Governors* (IT-A-03-14, Sept. 2003).

Review Findings

Progress in Developing BBG's Information Security Program

BBG changed its IT organizational structure in FY 2004, establishing and filling senior-level IT management positions and consolidating disparate units under one IT authority. Under the revised structure, BBG is making progress in developing its information security program to meet FISMA requirements. OIG supports BBG's progress in developing its IT program and is not making recommendations where BBG management is taking action or developing plans to correct weaknesses and deficiencies. OIG encourages BBG senior management and staff to continue developing its IT program to meet 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 appear to meet GISRA security requirements. During the FISMA evaluation of BBG in FY 2003, OIG also 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. In addition, 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 the BBG IT services, management, and operations. The independent review identified BBG's lack of effective communication and collaboration among program areas. The independent review recommended a restructuring of BBG's IT organization.

In April 2004, Congress approved and on May 30, 2004, BBG implemented a reorganization of its IT management structure, responsibilities, and functions, establishing the Engineering and Technical Services Directorate for overall IT program management and for the IT functions in OCB, Voice of America, and IBB. BBG named the director of Engineering and Technical Services Directorate 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 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.

Since last year's FISMA report, the agency has taken steps to meet FISMA and NIST guidance for developing an agency-wide IT security program. (See Appendix A.) Specifically, BBG defined 24 major systems under the Engineering and Technical Services Directorate. OIG found that managers were still unsure of the number of major systems they were responsible for, and the CIO agreed to review the number of major systems before next year's FISMA evaluation. Additionally, BBG developed operating system security configuration management policy for many of its operating systems. Also, BBG developed a generic incident response plan for use at headquarters that it plans to

further refine for use at its transmitting stations and other field operations. Lastly, BBG's management effectively incorporated user IT security training into its overall IT security program.

BBG performed adequate risk assessments and developed general support systems and major application system security plans and POA&Ms for 10 of its 24 major systems. However, much of the documentation BBG developed is not at the individual system level. BBG lacks IT policies and procedures, but has 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. BBG management intends to complete the program action plan by mid-FY 2005.

Developing an Enterprise Architecture

BBG has not developed an agency-wide IT enterprise architecture or capital planning and investment control process. In discussions with OIG, the new CIO acknowledged the need for both and explained that BBG is determining how it will develop its enterprise architecture. Additionally, BBG has made limited progress in tying budget requests to the business case process. The new CIO said that BBG would address this requirement with its current FY 2006 budget cycle. 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.

The enterprise architecture is required by the Clinger-Cohen Act, and it is reinforced by FISMA and OMB guidance. Agency CIOs should, 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.

FISMA, Clinger-Cohen Act, and OMB guidance also make agencies responsible for developing and maintaining a capital planning and investment control process. This process requires agencies to have two separate and distinct plans. The Information Resources Management Strategic Plan, which includes all IT resources of the agency and the agency Strategic Plan required by OMB Circular A-11, which ensures that IT decisions are a part of organizational planning, budget decisions, and IT procurement.

> **Recommendation 1**: OIG recommends that the Chairman, Broadcasting Board of Governors direct the Chief Information Officer to develop an enterprise architecture that will help the Broadcasting Board of Governors align its information system requirements with its mission processes and provide adequate interoperability between systems, redundancy of systems, and systems security.

BBG Response

BBG concurred with this recommendation and said it has no comments regarding the recommendation, other than to note the matters cited have already been identified by the CIO and BBG IT management officials, who plan to address them more fully in the coming year.

OIG Comment

OIG accepts BBG's response and considers this recommendation resolved. OIG will consider closing this recommendation when BBG provides documentation showing that it developed an enterprise architecture that aligns its information system requirements with its mission processes and provides adequate interoperability between systems, redundancy of systems, and systems security.

> **Recommendation 2**: OIG recommends that the Chairman, Broadcasting Board of Governors direct the Chief Information Officer to develop a capital planning and investment control process that includes all agency information technology resources and ensures that information technology decisions are included in the agency's organizational planning, budgeting, and procurement decisions.

BBG Response

BBG concurred with this recommendation and said it has no comments regarding the recommendation, other than to note the matters cited have already been identified by the CIO and BBG IT management officials, who plan to address them more fully in the coming year.

OIG Comment

OIG accepts BBG's response and considers this recommendation resolved. OIG will consider closing this recommendation when BBG provides documentation showing that it developed a capital planning and investment control process that includes all agency IT resources and ensures that IT decisions are included in the agency's organizational planning, budgeting, and procurement decisions.

Providing Guidance to Transmitting Stations

OIG found that transmitting station managers were generally aware of FISMA and, in some instances, had received some information on headquarters security plans, risk assessments, and incident response handling. However, at the two transmitting sites OIG reviewed in the Philippines, managers were not aware of their responsibilities for satisfying information security requirements at the stations. They had started receiving information from headquarters concerning information security, FISMA, and the NIST guidance in late May 2004, when BBG implemented its new organizational structure. The station managers were notified that they were to be the station FISMA program managers, but their responsibilities were not spelled out.

Station managers were aware of basic information security requirements, but lacked headquarters instructions and guidance on adapting generic plans, policies, and procedures for use at the stations and on conducting system self-assessments and developing POA&Ms as required by FISMA. Station managers were aware of the organizational IT changes and were looking forward to receiving headquarters guidance to put the necessary information security measures in place.

In OIG's opinion, much of the success of BBG's IT security program depends on station managers' having adequate headquarters instructions and guidance to meet their IT security

requirements as defined under FISMA. Failure to develop such guidance could adversely affect BBG's agency-wide security program.

> **Recommendation 3**: OIG recommends that the Chairman, Broadcasting Board of Governors direct the Chief Information Officer to provide station managers with instructions and guidance to adapt information technology security plans, policies, and procedures for use at transmitting stations.

BBG Response

BBG concurred with this recommendation and said it has no comments regarding the recommendation, other than to note the matters cited have already been identified by the CIO and BBG IT management officials, who plan to address them more fully in the coming year.

OIG Comment

OIG accepts BBG's response and considers this recommendation resolved. OIG will consider closing this recommendation when BBG provides documentation showing it provided instructions and guidance to station managers to adapt their IT security plans, policies, and procedures.

Recommendations

Recommendation 1: OIG recommends that the Chairman, Broadcasting Board of Governors direct the Chief Information Officer to develop an enterprise architecture that will help the Broadcasting Board of Governors align its information system requirements with its mission processes and provide adequate interoperability between systems, redundancy of systems, and systems security.

Recommendation 2: OIG recommends that the Chairman, Broadcasting Board of Governors direct the Chief Information Officer to develop a capital planning and investment control process that includes all agency information technology resources and ensures that information technology decisions are included in the agency's organizational planning, budgeting, and procurement decisions.

Recommendation 3: OIG recommends that the Chairman, Broadcasting Board of Governors direct the Chief Information Officer to provide station managers with instructions and guidance to adapt information technology security plans, policies, and procedures for use at transmitting stations.

Abbreviations

BBG	Broadcasting Board of Governors
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CTO	Chief Technical Officer
FISMA	Federal Information Security Management Act of 2002
GISRA	Government Information Security Reform Act
IBB	International Broadcasting Bureau
IT	Information 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

Appendix A

BBG Progress in Developing a Security Program			
	BBG Planned and Completed GISRA/FISMA Work		
			FISMA 2004 Requirements
Enterprise Architecture	No	No	No
Agency-wide Information Security Program Plan	Partially	Partially	Partially[a]
Periodic Risk Assessments	Partially	Partially	Partially[b]
Policies and Procedures	No	Partially	Partially[c]
Systems Inventory	No	Partially	Partially[d]
System Security Plans	Partially	Partially	Partially[e]
Periodic Testing of Policies and Procedures	No	No	No
Plan of Action and Milestone (POA&M)	Partially	Partially	Partially[f]
Security Incident Reporting Procedures	No	Partially	Yes
Senior Agency Information Security Officer	No	No	Yes
Security Awareness Training	No	No	Yes
Contingency Plans	Partially	Partially	Partially[g]
Configuration Standard & Patch Manag. Policy	n/a	n/a	Partially[h]
Self-Assessments (NIST SP 800-26)	Partially	Partially	Partially[i]
System Certification & Accreditation	No	No	No[j]
OMB Executive Summary	Yes	Yes	Yes

Legend: **Yes** indicates BBG completed the requirement.
No indicates that the requirement was not started.
Partially indicates the task is in process but not completed.
n/a indicates requirement did not apply during this period.

[a] Pending OMB approval.
[b] For FY 2004, BBG reorganized its IT program from four domains to 24 major systems. It, however, has not yet completed periodic risk assessments for its 12 transmitting stations. Risk assessments are scheduled for completion in FY 2005.
[c] In FY 2003, BBG hired a contractor to develop policies and procedures for the Office of Computing Services. The policies and procedures would later be distributed throughout the agency. However, BBG has not yet distributed them.
[d] For FY 2004, BBG defined 24 major systems for FISMA purposes. However, it has not yet developed an enterprise architecture that would help it define all of its systems.
[e] For FY 2004, BBG has developed system security plans for 13 of its 24 major systems and is working to complete plans for the remaining 11.
[f] For FY 2004, BBG developed POA&Ms for 10 of its 24 major systems and intends to complete the remaining 14 in FY 2005.
[g] BBG has 2 of 24 major systems with contingency plans.
[h] BBG has written configuration standards and patch management policy for 5 of its 10 operating systems.
[i] BBG has not yet completed self-assessments for FY 2004.
[j] BBG started the system certification and accreditation process for its major systems. System certification and accreditation is scheduled for completion in FY 2005.

Appendix B

Comments From the Broadcasting Board of Governors

BROADCASTING BOARD OF GOVERNORS
UNITED STATES OF AMERICA

September 16, 2004

Mr. Lynn Allen
Assistant Inspector General
Department of State
2201 C. Street, N.W.
Washington, D.C. 20520

Dear Mr. Allen:

The Broadcasting Board of Governors appreciates the opportunity to review and comment on your Memorandum Report IT-A-04-07 titled, *Review of the Information Security Program at Broadcasting Board of Governors, September 2004*.

The BBG is pleased that the Report finds that several of its recent actions designed to strengthen information management operations have contributed to visible progress in the development of information security programs. These actions include a major re-organization of information technology functions and staff in the IBB, a clarification and re-emphasis of the role of the Chief Information Officer, and the appointment of a full-time Chief Information Security Officer. BBG anticipates that, as this new IT organization and management matures, we will make increasingly efficient progress in ensuring the security of our information operations and in complying with the extensive scope of information security regulations. We are pleased to acknowledge the continuing assistance of the OIG's Information Technology staff in advising the CIO and other IT officials regarding many relevant security matters.

The BBG concurs with the three recommendations contained in the Report. At this time we have no comments regarding the recommendations, other than to note the matters cited have already been identified by the CIO and IBB Information Technology management officials who plan to address them more fully in the coming year. Also some of the recommendations, those that address required development of IT plans and related compliance documentation, are resource intensive and may require more than a year to accomplish fully. We will of course keep your IT staff informed of progress in accomplishing the recommendations as they occur.

Sincerely,

Kenneth Y. Tomlinson
Chairman

330 INDEPENDENCE AVENUE, SW ROOM 3360 COHEN BUILDING WASHINGTON, DC 20237 (202) 401-3736 FAX (202) 401-6605