~~SENSITIVE BUT 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 Broadcasting Board of Governors

Report Number IT-I-06-04, September 2006

~~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.~~

~~SENSITIVE BUT UNCLASSIFIED~~

Table of Contents

Overview

The Federal Information Security Management Act (FISMA)[1] requires that all federal agencies develop and implement an agency-wide information security (INFOSEC) program designed to safeguard information technology (IT) assets and data of their respective agency. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of controls over IT that support federal operations and assets, and it provides a mechanism for improved oversight of the information security programs government-wide.

FISMA requires that each agency's information security program must include documentation of policies and procedures, and reports that document the following:

- Periodic risk assessments;
- Information security policies and procedures;
- An assessment of threats, including their likelihood and impact;
- Policies and procedures for detecting security vulnerabilities;
- Evaluation and periodic testing of how well security policies are working;
- An inventory of software and hardware assets;
- Security awareness training and expected rules of behavior for end users;
- An evaluation of the technical, management, and operational security controls;
- Procedures for reporting and responding to security incidents;
- A process for addressing any deficiencies identified; and
- Contingency plans to facilitate a continuity of operations in a disaster.

FISMA also requires that the Office of Inspector General (OIG) provide an annual independent evaluation of the effectiveness of the agency's INFOSEC programs and practices. FISMA provides a framework and approach designed to assist OIG with:

1) Determining the current status of agency security programs through the testing of management and technical controls;
2) Assessing management, policies, and guidelines; and
3) Providing feedback to agency management through the annual evaluation process that will better assist with establishing and achieving improvement goals for INFOSEC.

Details including the scope and methodology of the review are discussed in Appendix A. Appendix B lists open recommendations from the OIG 2005 FISMA review that still require action and compliance from the Broadcasting Board of Governors (BBG) Office of the Chief Information Officer (CIO).

[1] 44 U.S.C. § 3541 et seq.

Results In Brief

OIG's 2006 FISMA review focused on the fundamental structure to support the implementation of the Clinger Cohen Act (CCA) of 1996[2], the Paperwork Reduction Act (PRA) of 1995[3], FISMA, and Office of Management and Budget (OMB) Circular A-130. The OIG team found programmatic and systemic issues that are traceable to a condition of organizational structure and authority and underlie BBG's continuing struggle to adequately address many of OIG's previous FISMA recommendations.

In brief, CIO position has not been assigned agency-wide authority for implementation and oversight of information management, technology, and security initiatives. The CIO, therefore, does not have sufficient authority to fully implement the requirements of FISMA.

BBG has established an ambiguous reporting chain for the CIO, effectively negating the capacity of the CIO to act as direct adviser to the head of the agency on IT matters. The structure also hampers the perceived authority of the CIO, negatively affecting his ability to effectively implement INFOSEC requirements. BBG management has not sufficiently involved the CIO in its strategic planning process or defined CIO responsibilities and authorities within the process. BBG views the CIO position as limited to overseeing administrative IT management within the International Broadcasting Bureau's Office of Engineering and Technical Services (IBB/E). By having vested the CIO with insufficient authority to implement requirements, BBG fails to comply with numerous statutory responsibilities regarding INFOSEC and the management of information resources.

In the 2004 and 2005 FISMA reports, OIG reported that BBG had not developed an agency-wide IT enterprise architecture. BBG has made progress regarding the enterprise architecture. (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)) (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)

BBG provided OIG with formal comments on the recommendations in this report, and they are included in their entirety in Appendix C. Overall, BBG agrees with all of the recommendations. The OIG will address the BBG's comments during the compliance process.

Background

The U.S. International Broadcasting Act of 1994[4] created BBG as a self-governing element within the former United States Information Agency, an entity that had provided limited administrative, technical, and management support to BBG. The Foreign Affairs Reform and

[2] The Clinger-Cohen Act of 1996, also known as the Information Technology Management Reform Act (P.L. 104-106)

[3] P.L. 104-13.

[4] P.L. 103-236.

Restructuring Act of 1998[5] granted BBG independence from United States Information Agency on October 1, 1999. BBG is led by a nine-member Board of Directors that serves collectively as the head of the agency and by an Executive Director, all of whom are Presidential appointees.

BBG is responsible for overseeing all U.S. government- and government-funded, non-military, international broadcasting, including the Voice of America (VOA) and the Office of Cuba Broadcasting. BBG also oversees three grantee organizations: Radio Free Europe/Radio Liberty, Radio Free Asia, and the Middle East Broadcasting Network.

INFOSEC is important to any organization that depends on information systems and information networks. 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 communicates and conducts business. However, without proper safeguards, this widespread interconnectivity poses significant risks to the infrastructure it supports by increasing the methods available to those seeking sensitive information or wish to commit fraud, disrupt operations, or attack information networks and systems.

In April 2004 Congress approved, and on May 30, 2004, BBG implemented a reorganization that consolidated all IT functions into a common program area, the Information Technology Directorate, within IBB/E. The Board designated the director of IBB/E as the chief technology officer with responsibility for all engineering and transmission service functions. The Board appointed a CIO to direct and oversee a broad range of statutory functions, including meeting FISMA requirements. Lastly, the Board created and filled a Chief Information Security Officer (CISO) position that reports directly to the CIO.

BBG Progress in Implementing FISMA Requirements

Authority of the Chief Information Officer

BBG's CIO does not have sufficient authority to fully implement the requirements of FISMA. The CCA directs the head of an agency, in consultation with the CIO and Chief Financial Officer (CFO), to develop and implement policies and procedures that provide assurance for information systems, as well as mechanisms for developing performance measures and conducting program reviews. FISMA, CCA, and PRA have the CIO reporting directly to the agency head and responsible for the agency's INFOSEC program and for advising the agency head on acquisition and management of information resources. Further, FISMA charges the agency head with making sure that INFOSEC management processes are integrated with agency strategic and operational planning processes. Given the CIO's responsibility for overall compliance with FISMA requirements, there is a need for a strong relationship between the agency head and CIO, encompassing strategic, operational, and capital and budgetary planning processes.

[5] P.L.105-277.

Ineffective Organizational Structure

The BBG organizational structure does not allow the CIO to have the authority to effectively implement INFOSEC. The Board has established an ambiguous reporting chain and organizational structure for the CIO. Although BBG's organizational chart (see Appendix E) indeed shows a direct line to the Board, a "dotted line" on the chart indicates the actual reporting responsibility to IBB/E, which has made the CIO operationally subordinate to the IBB/E director. Under this organizational structure, the IBB/E director reviews the CIO's performance. In fact, the CIO's performance should be reviewed by the Executive Director or the Board, because 44 USC § 3506 establishes a direct reporting requirement between the CIO and the agency head. The CIO's current positioning in the organizational structure does not allow for effective oversight of these organizations.

Furthermore, the current organizational environment has given the CIO unequal standing with the CFO in making decisions on IT investments for the agency, despite statutory and regulatory requirements that the heads of agencies must make such decisions in joint consultation with the CIO and CFO. The CCA requires the head of each agency to consult with the CIO and CFO to establish policies and procedures to ensure that major IT initiatives are integrated with organizational planning, budget, financial management, human resources management, and program decisions. These costs are captured in the system or program's annual OMB Circular A-11 Exhibit 300 and in the enterprise-wide Exhibit 53, the funding vehicles submitted to OMB to secure an operating budget. The National Institute of Standards and Technology's guidance to agencies on the implementation model of this process is shown in Figure 1 of Appendix D.

Currently, the CFO works closely with the Executive Director—their offices are collocated. The CIO, however, is generally not part of this interaction. The Executive Director's only interaction with the CIO is from a strategic mission perspective that is limited to IBB. As a result, although the CFO has always been involved in IT investment decision-making, the CIO is unable to approve or disapprove IT investments or advise the agency head regarding whether to continue, modify, or terminate IT programs or projects.

Organizational Culture and Understanding of FISMA Requirements

The position of CIO has insufficient standing within the BBG organizational culture to project the authority necessary to implement FISMA. The CIO is a relatively new position. Historically, BBG has been a radio-engineering operation, and questions related to technical issues and IT have been seen as responsibilities of the engineering offices. BBG has no true "Office of the CIO," in terms of either physical office space or as an entity that controls information or IT resources. Despite adding a deputy CIO position, the office still has only three employees to fulfill a tremendous number of statutory requirements. Yet the CIO has historically had little power, beyond his title and personal relationships, to use to influence or compel cooperation and compliance.

There is a lack of awareness and understanding of the CIO's role in driving the use of IT and of the CIO's statutory responsibilities to report to Congress and OMB on BBG's progress in implementing E-Government initiatives and the President's Management Agenda. This lack of awareness pervades even the highest levels of senior BBG management, some of whom believe the CIO's responsibility lies only in oversight of IT operations within IBB, rather than the agency as a whole.

Noncompliance with FISMA

BBG fails to comply with numerous mandates regarding INFOSEC and the management of information resources. BBG has:

- Ineffective processes for IT strategic planning and capital planning and investment control;
- No complete enterprise architecture[6];

Ineffective Processes for IT Strategic Planning and Capital Planning and Investment Control

BBG management has not included the CIO in its strategic planning process. BBG views the CIO position as limited to overseeing information resources management within IBB/E. The CIO's responsibilities and authorities within the strategic planning processes have not been defined.

The Government Performance and Results Act (GPRA) of 1993 [7] requires that agencies set strategic goals, measure performance toward those goals, and report on their progress. Effective implementation of GPRA hinges on agencies' ability to produce meaningfully integrated information to manage performance and measure results. Furthermore, amendments to Section 3506 of the Paperwork Reduction Act require agencies to indicate in strategic information resources management plans how they are applying information resources to improve the productivity, efficiency, and effectiveness of government programs, including how they are improving the delivery of services to the public.

The CCA renamed and elevated several former federal agency senior information resources manager positions to executive-level CIO positions and specified that these officials report directly to the agency head and have information management as a primary responsibility. The new information management leaders are accountable for the range of information management activities outlined in the PRA and for more strategic IT functions such as developing architectures, managing portfolios, and measuring the performance of IT investments. The CCA also requires senior executive involvement in IT decision-making, imposes a more disciplined approach to acquiring and managing technology resources and

[6] Per OMB A-130, Enterprise Architecture is the practice of applying a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's processes, information systems, personnel and organizational sub-units, so that they align with the organization's core goals and strategic direction.

[7] P.L. 103-62.

requires the redesign of inefficient work processes before making an investment in technology.[8] As illustrated in Figure 2 in Appendix D, the capital investment process should effectively integrate IT security and capital planning to document resource and funding plans for IT security. It requires that agencies incorporate IT security into the lifecycle of their information systems.

BBG's CIO has not been involved in planning or project management for major IT investments. This has resulted in inadequate agency-wide oversight of IT planning and investment in major initiatives. IBB/E's Technical Directorate handles project planning for such endeavors, a recent example of which is the NewsFlow video server project to manage video acquisition, production, and distribution for VOA. VOA officials question BBG's $2.3 million contract with Technical Innovations, Inc. for NewsFlow and whether NewsFlow provides sufficient performance. This is a major IT investment, yet the CIO was not involved in a meaningful way during the planning or implementation of this project. Neither has the CIO been able to:

- Exercise his authority under Section 5125 of the CCA to advise the agency head whether to modify or terminate the project;
- Use his authority under Section 5127 to monitor the performance of the project based on significant deviations; or
- Take advantage of new technologies for final phases of the project.

Another example was the procurement of Macintosh laptop computers by BBG elements outside of the IT directorate. These machines were purchased with end-of-year funds, and the purchase order was never subject to the CIO's approval, despite the requirement in the BBG Manual of Operations and Administration. All consumers of IT hardware and software in the agency should be aware of the CIO's leadership in implementing the statute, which emphasizes an integrated framework of technology for efficiently performing business. BBG cannot operate efficiently by using hardware and software purchased on an ad-hoc basis and installed without a plan. According to the CCA, the CIO must lead the consideration of all facets of IT capital planning.

Lack of Enterprise Architecture

In the 2004 and 2005 FISMA reports, OIG reported that BBG had not developed an agency-wide IT enterprise architecture. In discussions with OIG, the new Deputy CIO acknowledged the continuing need and said BBG is determining how it will develop its enterprise architecture. BBG has made progress towards this goal by purchasing an enterprise architecture tool and developing an information resource management plan. In the spring of 2006, the CIO and Deputy CIO attended an enterprise architecture training course.

The CCA requires agencies to develop an enterprise-wide information systems architecture, a requirement reiterated in FISMA and OMB guidance. OMB's Federal Enterprise Architecture[9] (FEA) provides best practices and recommendations to promote the successful

[8] GAO-01-376G CIO Executive Guide – *Maximizing the Success of Chief Information Officers, Learning From Leading Organizations*, February 2001

[9] CIO Council, *A Practical Guide to Federal Enterprise Architecture*, February 2001.

incorporation of security and privacy into an organization's enterprise architecture and to ensure appropriate consideration of security and privacy requirements in agencies' strategic planning and investment-decision processes. FEA is a scaleable and repeatable methodology for addressing INFOSEC and privacy from a business-centric enterprise perspective. It integrates the disparate perspectives of program, security, privacy, and capital planning into a coherent process, using an organization's enterprise architecture efforts. Enterprise architecture provides a common language for discussing security and privacy in the context of agencies' business and performance goals, enabling better coordination and integration of efforts and investments across organizational or business activities.

Section 207(d) of the E-Government Act of 2002[10] requires OMB to issue policies and requires agencies to use standards, "which are open to the maximum extent feasible to enable the organization and categorization of government information." According to BBG officials, the BBG's mission falls under one line of business: "knowledge dissemination." BBG maintains 11 "key systems" that are not integrated or fully automated since they require user intervention at multiple stages of the workflow process. For example, news might be acquired from one publicly available news wire, but this information must be saved and transferred to another system for manipulation before it can be retransmitted, requiring additional systems. Employees in BBG's language services operation might have to work on up to six different applications to complete a project because the systems are not integrated. Information cannot flow through these systems in an integrated workflow process because the business process was not redesigned for efficiency prior to the investment in technology, despite the requirement of Executive Order 13011[11]. Although it may not be possible to fully integrate all systems, it is important that BBG takes steps towards phasing out legacy systems.

Some of BBG's IT architecture processes are defined, but many do not link to the strategic planning process. There is no unified architecture process across technologies or business processes. Success depends on individual efforts. Documentation and standards are established for the technical architecture of broadcast operations but do not provide a linkage to business strategies or business drivers. Senior BBG management has limited awareness or involvement in the architecture process, and there is little or no involvement of acquisition management in the enterprise architecture process.

BBG's CIO should continue to develop an enterprise architecture that includes the agency's lines of business processes, information flows, hardware and software, data descriptions, and the IT infrastructure. BBG should integrate IT security into its capital planning and enterprise architecture processes. It should also conduct annual IT security reviews and report the results of those reviews to OMB. The resulting agency-level enterprise architecture should be linked throughout all operations to provide value to internal operational decision-making and in identifying government-wide solutions for improved services. An earlier OIG report call for development of an enterprise architecture. This <u>recommendation</u> remains open and is listed in Appendix B.

[10] P.L. 107-347.

[11] Executive Order 13011, *Federal Information Technology*, provides policy guidance for significantly improving the acquisition and management of IT by implementing the CCA and PRA.

[redacted]

[redacted]

[redacted]

[redacted]

[12] OMB Circular A-130, *Management of Federal Information Resources.*

Under FISMA, the agency CISO must effectively implement an agency-wide information security program, while BBG's program managers are responsible for INFOSEC duties. OIG sent a questionnaire to 20 BBG managers responsible for FISMA reporting, to evaluate the effectiveness of the INFOSEC programs.

[redacted]

[redacted] As part of an agency-wide INFOSEC program, FISMA requires that all personnel with access to information and information systems receive annual security awareness training. All BBG personnel must take the security awareness training, and statistics should are kept of those trained. Although security awareness training is mandated by FISMA, [redacted]

Meeting the Requirements

Recommendation 1: The Broadcasting Board of Governors should provide the Chief Information Officer with agency-level authority that encompasses, at a minimum, all components of the International Broadcasting Bureau and grantees to ensure compliance with statutes regarding the implementation and oversight of information management and information security requirements. (Action: BBG)

Once BBG gives the CIO sufficient authority, the CIO must develop processes to meet the statutory requirements. This effort will require resources and may require significant outsourcing. To date, the CIO has submitted to the executive director a status report of second quarter activities for FY 2006, outlining the roles and responsibilities, challenges, and plans.

Recommendation 2: The Chief Information Officer should develop and present to the Broadcasting Board of Governors a comprehensive plan of action to ensure the full implementation of the requirements of the Federal Information Security Management Act, Clinger-Cohen Act, and Paperwork Reduction Act, enumerating the necessary activities and the financial and personnel resources required to perform and maintain those activities. (Action: BBG)

Recommendations

Recommendation 1: The Broadcasting Board of Governors should provide the Chief Information Officer with agency-level authority that encompasses, at a minimum, all components of the International Broadcasting Bureau to ensure compliance with statutes regarding the implementation and oversight of information management and information security requirements. (Action: BBG)

Recommendation 2: The Chief Information Officer should develop and present to the Broadcasting Board of Governors a comprehensive plan of action to ensure the full implementation of the requirements of the Federal Information Security Management Act, Clinger-Cohen Act, and Paperwork Reduction Act, enumerating the necessary activities and the financial and personnel resources required to perform and maintain those activities. (Action: BBG)

Abbreviations

BBG	Broadcasting Board of Governors
CCA	Clinger-Cohen Act of 1996
CFO	Chief financial officer
CIO	Chief Information officer
CISO	Chief Information security officer
GPRA	Government Performance and Results Act of 1993
FEA	Federal Enterprise Architecture
FISMA	Federal Information Security Management Act of 2002
IBB	International Broadcasting Bureau
IBB/E	Office of Engineering and Technical Services
INFOSEC	Information security
IT	Information technology
OMB	Office of Management and Budget
OIG	Office of Inspector General
POA&M	Plan of action and milestones
PRA	Paperwork Reduction Act
VOA	Voice of America

Appendix A

Objectives, Scope and Methodology

OIG reviewed and evaluated BBG's INFOSEC program. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of controls over IT resources that support federal operations and assets and a mechanism for improved oversight of federal agency INFOSEC programs. In addition, OMB implementation guidance for FISMA requires agencies' offices of inspector general to assess development, implementation, and management of their agency's agency-wide POA&M process, focusing on performance measures. OIG's review assessed BBG's progress in developing its INFOSEC program and practices regarding FISMA and on determining BBG's processes for implementing FISMA's requirements.

To fulfill these objectives, OIG met with BBG's Executive Director, CFO, CIO, Deputy CIO, CISO, and BBG Board members. OIG did not conduct a detailed review of BBG's grantee organizations, but did hold meetings and gathered relevant documentation to assess each organization's approach to handling INFOSEC. OIG surveyed FISMA managers or their designated information systems security officers on issues pertaining to the implementation of FISMA requirements at overseas locations. Finally, OIG drew upon documentation and meetings from the concurrent OIG inspection of IBB/E.

OIG also 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, and examined reports of inspections performed during FY 2006. OIG's IT staff performed this review between May 2006 and September 2006. Major contributors to this report were Tim Fitzgerald, Matthew Ragnetti, and Michelle Wood. Comments or questions about the report may be directed to Richard Saunders, Director Office of Information Technology at saundersRS@state.gov.

Appendix B

Open Recommendations

BBG FISMA 2005 IT-I-05-10

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

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: (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)

Appendix C

Agency Comments

Enclosure

The Broadcasting Board of Governors (BBG) Response
to the Draft Memorandum Report
"Review of the Information Security Program at the
Broadcasting Board of Governors"
Report No. IT-I-06-04
September 2006

> **OIG Recommendation 1: The Broadcasting Board of Governors should provide the Chief Information Officer with agency-level authority that encompasses, at a minimum, all components of the International Broadcasting Bureau and grantees (Office of Management and Budget M-06-20) to ensure compliance with statutes regarding the implementation and oversight of information management and information security requirements.**

BBG Response: Developing mature and effective information technology programs is a complex task that requires transformational change throughout an organization. The BBG recognizes the value of IT planning and investment and therefore believes it has progressed beyond minimum maturity levels in these efforts. The Office of the Chief Information Officer has recently been staffed with individuals with the appropriate experience and knowledge to develop the programs necessary to effect this transformational change at BBG. Also, per the OIG recommendation, the BBG will clearly communicate to the organization the authoritative role the CIO has with respect to IT policy and investment decisions. The agency will also review the position of the CIO within the agency's organizational structure to develop a less "ambiguous" reporting and administrative structure.

With respect to grantee organizations, the BBG notes that FISMA only applies to information systems that store and process federal agency information. The agency interprets the intent of M-06-20 to cover information and information systems shared and/or managed by grantees on behalf of the federal government or vice versa. This type of information or information system sharing relationship does not exist between the agency and its grantees. The BBG grantees are atypical in that they are entirely independent stand alone non-profit organizations that do not use or otherwise have access to BBG's agency information systems, nor are grantees' information systems interconnected with this agency's information systems, but instead have entirely separate information systems and data storage, which they acquire and manage on their own, none of which are federal systems or agency information. The information processed and stored on the grantees' information system is the property of the grantees' and not federal information. Because of this, the BBG has no legal authority to control or advise the grantees on the use of their

information systems. The BBG can, however, give general guidance on the appropriate use of federal funds that the grantees receive. The CIO will investigate alternatives for providing IT investment guidance to grantees to ensure that
federal funds are being used to develop secure information systems and manage them according to industry best practices.

> **OIG Recommendation 2**: **The Chief Information Officer should develop and present to the Broadcasting Board of Governors a comprehensive plan of action to ensure the full implementation of the requirements of the Federal Information Security Management Act [FISMA], Clinger-Cohen Act [CCA], and Paperwork Reduction Act [PRA], enumerating the necessary activities and the financial and personnel resources required to perform and maintain those activities.**

BBG Response: The CIO is developing a set of interrelated programs to allow the agency to better manage its IT investments per the requirements of FISMA, CCA, PRA, and other federal statutes, and guidelines. The programs are modeled after the guidance presented by the Chief Information Officer Council in *A Practical Guide to Federal Enterprise Architecture* and consists of the following four subprograms: enterprise architecture (EA) program, IT capital investment and planning (CPIC) program, IT project management (PM) program, and IT security and privacy (INFOSEC) program. The EA, CPIC, and PM programs are tightly coupled to provide system lifecycle management from IT investment inception to retirement. The programs also ensure alignment of IT investments with the agency strategic mission, goals, and objectives. Each program is discussed in more detail below.

Enterprise Architecture (EA) Program:

The EA program defines the roadmap for reaching an IT investment goal three to five years in the future that supports the agency's strategic mission. The EA documents the current state of IT investments, called the "as is" state, the future state, called the "to be" state, and a transition plan for getting from the "as is" to the "to be" state through rational IT investments. The *portfolio* of IT investments identified in the transition plan is prioritized based on importance to the agency mission and technology dependencies. The EA is also used to validate proposed investments with the architecture and mission of the agency. Proposed investments must undergo both a business and technical review and be approved by an executive board and a technical board, respectively.

Developing an enterprise-wide EA is a very complex and time-consuming task. Consequently, the CIO is using a segmented approach to develop the EA. A segmented approach focuses on a single business area and documents the IT architecture as described earlier. The CIO has selected VOA's video production

Agency Comments (Continued)

business segment as the first area for EA development. Video production is a critical tool for meeting the agency's multimedia oriented strategic goals and was identified by the OIG as an investment in need of guidance by the CIO.

IT Capital Planning and Investment Control (CPIC) Program

The IT Capital Planning and Investment Program shepherds IT investments through the IT acquisition process. Investments that have been approved by the EA boards are submitted to the CPIC program to develop Congressional funding requests. The CIO plans to develop an IT CPIC program where IT investment requests are assessed for funding throughout the year, not just in reaction to the annual budget call. The CIO believes a more effective IT funding process can be developed by focusing investment justification and documentation efforts on investments that truly serve the agency mission and are in alignment with the EA.

IT Project Management (PM) Program

The IT project management program is designed to provide lifecycle support to IT investments. A properly managed project requires structure to be successful. At initiation, a project needs a business justification statement that meshes with the EA, a sponsor who will champion the project through implementation, and a charter or agreement of the ground rules for the investment's implementation, a well-defined requirements definition, and a project manager who follows IT project management best practices. BBG is committed to a sound IT project management program that will keep IT projects within scope, on time, and within budget, by avoiding the pitfalls of poorly managed projects. The PM program is closely coordinated with the EA and CPIC programs. Coordination with the EA program ensures that the investment serves the agency mission. The PM program also provides feedback to the CPIC program to identify if additional funding for a particular investment should be pursued or abandoned.

[redacted]

[redacted].

Agency Comments (Continued)

Likewise, the CPIC program will ensure that information assurance is built into all IT investment funding requests in a manner identified by the EA. Finally, the IT project management program will manage information assurance throughout the lifecycle of IT investments. Information assurance requirements must be clearly stated in all acquisition and implementation documents and monitored for compliance, and FISMA Certifications and Accreditation and Privacy Impact Assessments must be performed in accordance with applicable law and regulations.

Program Summary:

The programs proposed in response to Recommendation 2 provide a framework for successful IT investment The agency recognizes that successful implementation of these programs will require a cooperative commitment by agency management, the CIO, IT systems managers, and end-users. Some of these programs will require additional resources to implement; however, the agency is committed to supporting the CIO's outreach and governance efforts to initiate and sustain these programs.

General Comments about the Report:

While the BBG recognizes that additional work is required, we continue to make progress in integrating CIO input in agency IT decisions. The report does not mention the agency's efforts to improve coordination with the CIO. For example, in FY 2005, the Capital Planning Process was modified to incorporate the CIO function. While in FY 2006 the CIO only participated in the initial Capital Planning kickoff meeting in preparation for the FY 2008 budget request due to transition and coordination issues in the Office of the CIO and the Office of Engineering, the agency plans to continue to refine and strengthen the CFO-CIO relationship as well as implement the CIO programs described above to improve the effectiveness of IT investments. For FY 2005 and 2006, the CIO coordinated and prepared the Exhibit 53.

In addition, in FY 2006 the CIO has been actively involved in the evaluation and selection of the BBG's financial management system and services provider. In prior years, the CFO has included the CIO's input in the e-government initiative to implement a new payroll system.

Also, the OIG report mentions the procurement of Macintosh laptops by BBG elements outside of the IT directorates as an example of the lack of CIO involvement in budget decisions. These laptops were purchased within the CIO/IT guidance at the time of the purchase. The current CIO has drafted a revised IT purchasing and contracting policy that is intended to provide broader oversight of IT purchases. The policy is awaiting final approval by management. In an effort to prevent year-

Agency Comments (Continued**)**

end spending on IT items without CIO approval, the CIO reviewed and cleared on the proposed FY 2006 fourth quarter IT-related purchases for VOA and IBB.

Appendix D

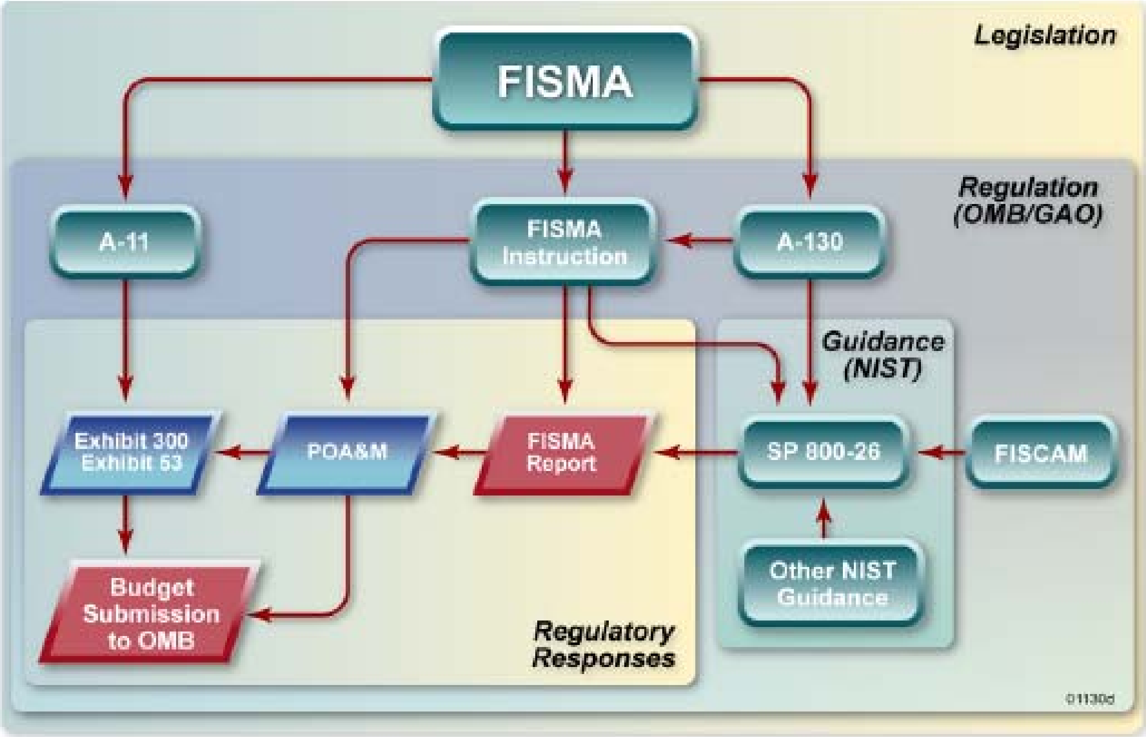


FIGURE 1 Source: *NIST Special Publication 800-65 Federal IT Security and Capital Planning Legislation, Regulations, and Guidance*

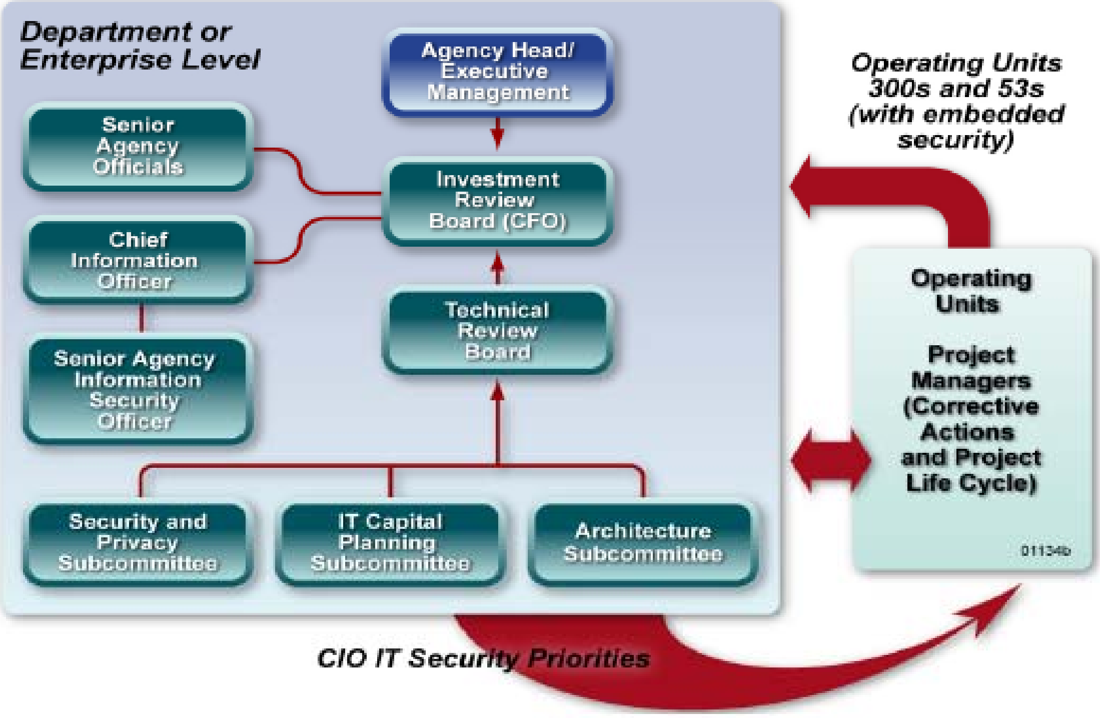
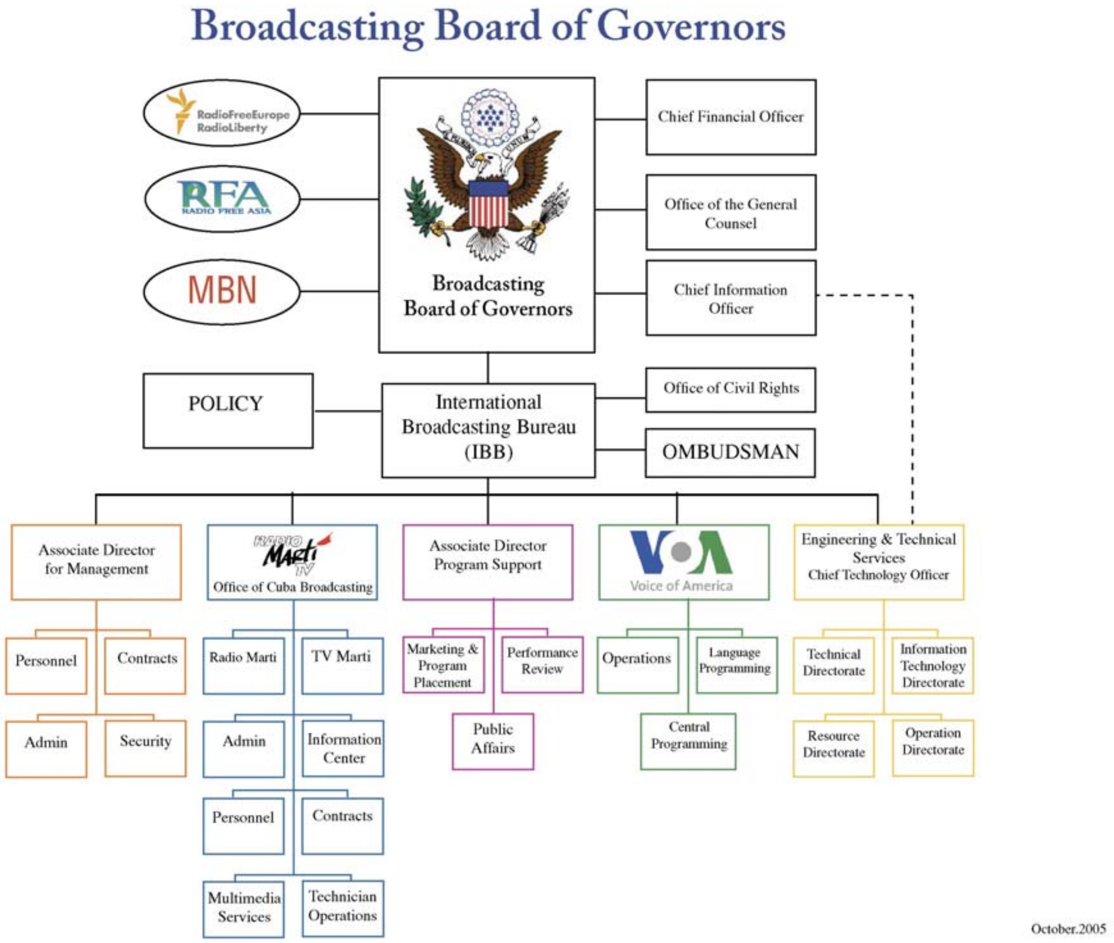

Department or Enterprise Level
Agency Head/ Executive Management
Senior Agency Officials
Investment Review Board (CFO)
Chief Information Officer
Technical Review Board
Senior Agency Information Security Officer
Security and Privacy Subcommittee
IT Capital Planning Subcommittee
Architecture Subcommittee
Operating Units 300s and 53s (with embedded security)
Operating Units
Project Managers (Corrective Actions and Project Life Cycle)
01134b
CIO IT Security Priorities

FIGURE 2 *Source: NIST Special Publication 800-65 Notional IT Management Hierarchy*

Appendix E



BBG Organization Chart