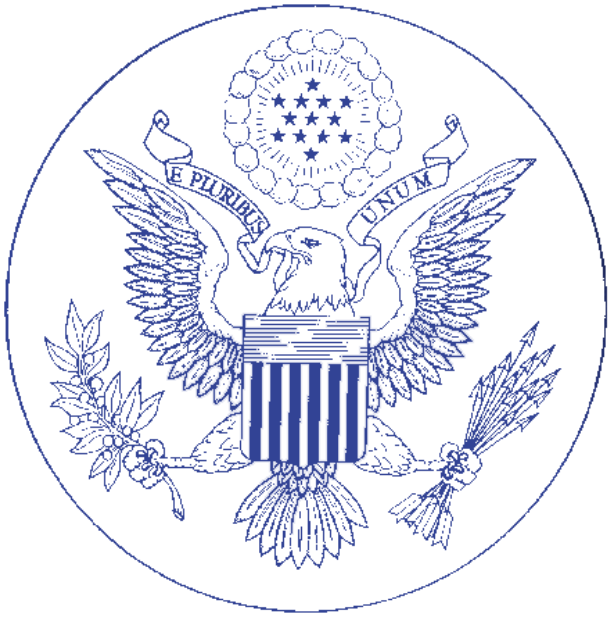
United States Department of State
And the Broadcasting Board of Governors

Office of Inspector General



Executive Summary

Government Information Security Reform Act
Broadcasting Board of Governors
FY 2002 Submission

September 16, 2002

EXECUTIVE SUMMARY

PURPOSE

In response to the Government Information Security Reform Act (GISRA), Public Law 106-398, the Office of Inspector General (OIG) performed an independent evaluation of the information security program and practices of the Broadcasting Board of Governors (BBG). This executive summary provides the results of OIG's evaluation in two parts. Part I summarizes the results of OIG's review of BBG's information security program. Part II contains OIG's assessment of BBG's information security program using performance measures provided by the Office of Management and Budget (OMB).

PART I

Results of OIG's Information Security Program Evaluation (Report IT-A-02-07)

OIG's evaluation of the effectiveness of the BBG's information security program concluded that BBG has made progress, but more must be done to comply with GISRA. BBG has developed an agency-wide information security program, and it has performed program-level self-assessments and documented the results of its self-assessments in its quarterly reporting of the agency's plans of action and milestones to the Office of Management and Budget (OMB). Included in this reporting was the identification of 37 information security weaknesses, of which 20 have been corrected. Also, BBG is in the process of hiring a contractor to develop and revise required information security-related policies and procedures to satisfy its needs.

OIG also found several key areas of security that still require management attention. Specifically, it found that BBG needs to develop an incident response process and reporting procedures to share information effectively on common vulnerabilities and threats. Also, OIG concluded that BBG lacks security and contingency plans at the systems and major application level and needs to develop these plans to meet its information security requirements and comply with GISRA. Lastly, OIG found that BBG lacks an information security training program and must develop and implement a program that addresses the needs of the agency and its employees.

Part II

OIG Assessment of the Broadcasting Board of Governor's Information Security Program Based on OMB Performance Measures

A. General Overview

1. N/A

2. Identify and describe as necessary the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials, CIOs, or OIGs in both last year's report (FY 01) and this year's report (FY 02) according to the format provided below. Agencies should specify whether they used the NIST self-assessment guide or an agency developed methodology. If the latter was used, confirm that all elements of the NIST guide were addressed.

TABLE A.1: PROGRAM AND SYSTEM REVIEWS

		FY 2001	FY 2002
2a	Total number of agency programs.	6	6
2b	Total number of agency systems.	49	31
2c	Total number of programs reviewed by OIG.	4	6
2d	Total number of systems reviewed by OIG.	2	0

Note 1: In 2a, agency programs include: International Broadcasting Bureau, Office of Computing Services, Office of Cuba Broadcasting, Office of Internet Development, Office of Engineering and Technical Services, and Voice of America Broadcast Operations.
Note 2: In 2b, agency totals show all systems as represented in BBG's functional area security plans for FY 2002.

BBG has taken steps to consolidate its information systems under five functional areas. These steps include:

- Designating existing program offices as functional areas and designating all systems within each functional area as one system;
- Performing internal risk assessments at the functional area level and incorporating the risk assessments as a major part of the functional area security plans;
- Completing self-assessments of the International Broadcasting Bureau (IBB) and five functional areas, without using National Institute of Standards and Technology (NIST) standard methodology; and
- Incorporating self-assessment results into the plans of action and milestones (POA&M) for the BBG submission to OMB.

In FY 2001, OIG performed two systems reviews and four program reviews. In FY 2002, using NIST guidance tailored for OIG's evaluation, OIG reviewed the IBB agency-wide information security program and the five functional area programs. At the time of this review, BBG had not completed its FY 2002 self-assessment reviews. However, BBG's chief information officer (CIO) told OIG that these assessments would be completed using NIST guidance by the end of FY 2002.

3. Identify all material weaknesses in policies, procedures, or practices as identified and required to be reported under existing law. (Section 3534(1)-(2) of the Security Act.) Identify the number of reported material weaknesses for FY 01 and FY 02, and the number of repeat weaknesses in FY 02.

TABLE A.2: MATERIAL WEAKNESSES			
		FY 2001	**FY 2002**
3a	Number of material weaknesses reported.	0	0
3b	Number of material weaknesses repeated in FY02.	0	0

BBG reported no material weaknesses in either FY 2001 or FY 2002.

B. Responsibilities of Agency Head

1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth the Security Act's responsibilities and authorities for the agency CIO and program officials. Specifically, how are such steps implemented and enforced? Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?

For FYs 2001 and 2002, BBG took a number of actions to develop and implement its security program. Specifically, in FY 2001, the Director, International Broadcasting Bureau, appointed the associate director for management as the CIO. In addition, BBG developed an agency-wide information security program plan and five functional area level security plans. Finally, responsible program officials and the CIO performed functional-level internal risk assessments. In FY 2002, responsible program officials and the CIO performed functional-level self-assessments. Also, BBG obtained a contractor to develop information security policies and procedures.

Under the BBG's information security program, the CIO is also responsible for IT planning and budgeting activities, with assistance from the Broadcast Technology Steering Committee. The Broadcast Technology Steering Committee reviews and recommends funding for all IT projects. OIG did not perform work to determine the role of the CIO in the IT acquisition process.

2. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system? (Sections 3533(a) (1) (A)-(B), (b)(3) (C)-(D), (b) (6) and 3534 (a) (C) of the Security Act.) During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the life cycle of each system?

The agency head, through the Director of the International Broadcasting Bureau, delegated all information security authority and responsibility to BBG's CIO. OIG found no other actions taken by the head of the agency to oversee the performance of agency program officials and the CIO to verify that functional area managers are ensuring that security plans are up-to-date and practiced throughout the life cycle of each system.

Under the CIO's direction, during FY 2001, BBG completed security plans for each of its five functional areas and for FY 2002, identified each of its five functional areas as a general support

system or major application. It designated all systems within each functional area as one system. OIG found that BBG's approach to developing system security plans was flawed because it focused solely on functional areas and not individual systems.

3. How has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)? (Sections 3534 (a) (1) (B) and (b) (1) of the Security Act.) Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complementary across the various programs and disciplines?

BBG is a relatively small federal agency with only minor information technology (IT) connectivity outside its operational environment. According to BBG's CIO, it integrates its information technology security program with its internal critical infrastructure protection responsibilities through its security program and the International Broadcasting Technical Discussion Group.

The Director, Office of Security, is assigned responsibility for physical security, while information security is assigned to the CIO and delegated to the Director, Office of Computing Services. In BBG's organizational structure, the Director, Office of Security, and Director, Office of Computing Services, report to the CIO. No specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent.

4. Has the agency undergone a Project Matrix review? If so, describe the steps the agency has taken as a result of the review. If no, describe how the agency identifies its critical operations and assets, their interdependencies and interrelationships, and how they secure those operations and assets. (Sections 3535(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a) (C) of the Security Act.)

BBG has not undergone a Project Matrix review. According to BBG's CIO, it is not necessary because the agency does not have any national security systems or connections between itself and other agencies, except for limited financial and payroll system connections with the Department of State. According to BBG, the Department is responsible for the security of those system connections.

5. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities? Identify and describe the procedures for external reporting to law enforcement authorities and to the General Services Administration's Federal Information Incident Response Center (FedCIRC). Identify actual performance according to the measures and the number of incidents reported in the format provided below. (Section 3534(b)(2)(F)(i)-(iii) of the Security Act.)

The agency head has not ensured that the agency has documented procedures for reporting incidents and sharing information regarding common vulnerabilities. As OIG reported in its FY 2002 GISRA evaluation report, BBG lacks an information security incident response process and has no external security incident reporting procedures. GISRA requires that agencies have procedures in place for detecting, reporting, and responding to security incidents. Toward that end, BBG's agency-wide information security program plan calls for each of its five functional

area program officials to develop incident response and reporting procedures. However, four of the five program officials reported that the procedures had not been developed. The BBG information security program plan states that incidents should be reported to the CIO and the Office of Computing Services so that they can determine whether law enforcement agencies and the General Services Administration's (GSA) Federal Computer Incident Response Center needs to be notified. However, only one of the five BBG functional areas overseeing information technology (IT) security has documented procedures in place to react to information security incidents.

BBG officials informed OIG of only four information security incidents that occurred during FYs 2001 and 2002, none of which were reported outside the agency. Two of the incidents were not reported outside the functional area where they occurred. In two of the four instances, several thousand dollars were spent bringing in outside consultants to evaluate the damage caused by the incidents and to perform a risk assessment of the functional area information systems.

Table B.1: Incident Response Capability

		FY 2002
5a	Total number of agency components including bureaus, field activities (functional areas and worldwide transmitting sites).	29
5b	Number of agency components with incident handling and response capability.	0
5c	Number of agency components that report to FedCIRC.	1
5d	Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?	No
5e	What is the required average time to report to the agency and FedCIRC following an incident?	N/A
5f	How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?	see note below

		FY 2001	FY 2002
5g	By agency and individual component, number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported by each component.	2	2
5h	By agency and individual component, number of incidents reported externally to FedCIRC or law enforcement.	0	0

Note: In 5f, according to the BBG CIO, manufacturer's documentation regarding patches is reviewed and then applied manually to all servers that require it. The patches are then pushed out to the workstations.

C. Responsibilities of Agency Program Officials

1. Have agency program officials: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? (Section 3534(a)(2) of the Security Act.)

TABLE C.1: TOTAL SYSTEMS

	Component or Bureau Name	Total Number of Systems
C1.1	Office of Computing Services	5
C1.2	Office of Cuba Broadcasting	4
C1.3	Office of Internet Development	1
C1.4	Office of Engineering and Technical Services	20
C1.5	Voice of America Broadcasting Operations	1
	Total Number of Agency Systems	**31**

Note: System totals come from functional area security plans and may not represent all BBG systems. BBG also reported on 23 systems in FY 2001 that were not reported under any of the functional area security plans in FY 2002. BBG did not provide OIG with information on these 23 systems.

1) BBG's five functional areas performed internal risk assessments as part of their development of functional area security plans. All of the five functional areas performed their initial risk assessments internally, based on work experience.

2) BBG's risk assessments assign a level of security protection required for its IT assets and operations based on its internal risk assessment. However, BBG has not documented these assessments.

3) BBG has not developed security plans at the systems or major application level. Further, BBG's approach to developing system security plans is flawed because it focuses solely on functional areas and not individualized systems. System security plans, which are required by GISRA, provide an overview of system security requirements, describe established system controls, and provide a means for improving the protection of IT resources. During the latter part of FY 2001, BBG completed security plans for each of its five functional areas. However, it did not develop separate plans for each of the systems within these functional areas. For example, OIG found that one functional area grouped 20 of BBG's 31 reported systems for FY 2002 under one security plan.

4) BBG did not provide OIG with any documentation supporting testing and evaluation of security controls. From its discussions with BBG officials, OIG is not clear that methodical testing and evaluation is taking place. OIG intends to review testing and evaluation in more depth during its FY 2003 independent evaluation.

By each major agency component and aggregated into an agency total, from last year's report (FY 01) and this reporting period (FY 02) identify actual performance according to the measures and in the format provided below for the number and percentage of total systems.

BBG did not provide sufficient information for OIG to complete this section.

2. For operations and assets under their control, have agency program officials used appropriate methods (e.g., audits or inspections) to ensure that contractor-provided services (e.g., network or website operations) or services provided by another agency for their program and systems are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy? Identify actual performance according to the measures and in the format provided below. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act.)

TABLE C.2: OFFICE OF INTERNET DEVELOPMENT

		FY 2001	FY 2002
2a	Number of contractor operations or facilities.	1	1
2b	Number of contractor operations or facilities reviewed.	0	0

BBG's functional area/program officials have not used appropriate methods to ensure that contractor-provided services are adequately secure and meet statutory and regulatory guidance. BBG contracts with Genuity for its Voice of America Internet operations. However, as shown in the table above, it has not performed any security reviews on the operation for the services provided to the Voice of America. Also, on the island of Tinian in the South Pacifc, BBG maintains a transmitting station that is government owned and contractor operated. As shown in the table below, the site has not been reviewed to determine if it meets the requirements of GISRA, OMB policy and NIST guidance.

TABLE C.3: OFFICE OF ENGINEERING AND TECHNICAL SERVICES

		FY 2001	FY 2002
2a	Number of contractor operations or facilities.	1	1
2b	Number of contractor operations or facilities reviewed.	0	0

D. Responsibilities of Agency Chief Information Officers

1. Has the agency CIO: 1) adequately maintained an agency-wide security program; 2) ensured the effective implementation of the program and evaluated the performance of major agency components; and 3) ensured the training of agency employees with significant security responsibilities? Identify actual performance according to the measures and in the format provided below. (Section 3534(a)(3)-(5) and (Section 3534(a)(3)(D), (a)(4), (b)(2)(C)(i)-(ii) of the Security Act.)

TABLE D.1: AGENCY-WIDE SECURITY PROGRAM

		FY 2001	FY 2002
1a	Other than GAO or IG audits and reviews, how many agency components and field activities received security reviews?	6	6
1b	What percentage of components and field activities have had such reviews? (One bureau, five functional areas, 23 transmitting stations)	21%	21%
1c	Number of agency employees including contractors.	3,237	3,191
1d	Number and percentage of agency employees including contractors that received security training.	13 0.4%	14 0.4%
1e	Number of employees with significant security responsibilities	21	22
1f	Number of employees with significant security responsibilities that received specialized training.	13	14
1g	Briefly describe what types of security training were available.	see D. 1. 3	see D. 1. 3
1i	Do agency POA&Ms account for all known agency security weaknesses, including all components and field activities? If no, why not?	Yes	Yes
1j	Has the CIO appointed a senior agency information security official?	No	No

Note 1: In 1a, the number includes self-assessments.
Note 2: In 1c, employees and contractors are approximate numbers as of Oct. 2000 and Oct. 2001.

1) Adequately maintained an agency-wide security program.

BBG's CIO has not maintained adequately an agency-wide security program. As shown in OIG's FY 2002 GISRA independent evaluation report, the BBG has developed an agency-wide information security program plan that assigns responsibility for information security and identifies the agency information management policy and security program manager as the CIO. The program also assigns five program officials with the responsibility for implementing a risk management-based security program. Although BBG's program plan appropriately covers the program level for addressing information security issues, BBG has decided not to develop information security plans at the systems level. System security plans, which are required by GISRA, provide an overview of system security requirements, describe established system controls, and provide a means for improving the protection of information technology resources. BBG has completed security plans for each of its five functional areas; however there are no separate plans for each of the systems within these functional areas. For example, OIG found that one functional area grouped 20 of BBG's 31 reported systems for FY 2002 under one security plan.

2) Ensured the effective implementation of the program and evaluated the performance of major agency components.

The CIO has not ensured effective implementation of BBG's security program. OIG reported in its FY 2002 independent evaluation that BBG's information security policies and procedures were outdated and incomplete.[1] Agencies are required by GISRA to develop and implement security policies, procedures, and controls, which provide each system with security protections equal to the risk of system operations. In a recent risk assessment, an independent contractor reported that IBB lacked defined security policies to address configuration management and installation of non-mission related software. Also, GISRA requires that agencies have procedures in place for detecting, reporting, and responding to security incidents, and BBG's agency-wide information security program plan reiterates this requirement. However, BBG lacks an information security incident response process and has no external security incident reporting procedures. Lastly, OIG reported in its FY 2002 GISRA evaluation that BBG lacks system or major application contingency plans to support all of its information technology operations. BBG's information security program recognizes that contingency plans ensure an agency's ability to recover from a disruption and provide service sufficient to meet the minimal needs of users and calls for the plans to be developed. However, OIG found that no systems contingency plans had been developed and that only one of the five functional areas had a contingency plan.

3) Ensured the training of agency employees with significant security responsibilities.

The CIO has not ensured that employees with significant security responsibilities are trained adequately. Few employees at BBG receive any information security training, and those who do are technical employees. Although the BBG Information Security Program Plan acknowledges the need for information security training and assigns the Office of Computing Services with responsibility for developing and implementing an information security education program, BBG officials reported that no specific information security training was taking place. Further, BBG lacked a formal mechanism for tracking individual training, and officials were not able to provide OIG with any statistical data on information security training that showed the classes taken, which employees took the classes, or the associated cost.

2. For operations and assets under their control (e.g., network operations), has the agency CIO used appropriate methods (e.g., audits or inspections) to ensure that contractor-provided services (e.g., network or website operations) or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy? Identify actual performance according to the measures and in the format provided below. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act.)

TABLE D.2: CONTRACTOR OPERATIONS AND FACILITIES

		FY 2001	FY 2002
2a	Number of contractor operations or facilities.	2	2
2b	Number of contractor operations or facilities reviewed.	0	0

Note: 2a includes Tinian transmission station and Office of Internet Development contracting operations.

[1] *Information Security Program Evaluation: Broadcasting Board of Govenors* (Report Number IT-A-02-07, September 2002)

The CIO has not used appropriate methods to ensure that contractor-provided services are adequately secure and meet statutory and regulatory guidance. BBG maintains a transmitting station on the island of Tinian, which is contractor operated. The site was not reviewed to determine whether it meets the requirements of GISRA, OMB policy and NIST guidance. However, BBG did review information systems related to this transmitting station as part of its risk assessment. BBG also contracts with Genuity for its Voice of America Internet operations, but there were no security reviews performed on this operation.

3. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were security requirements and costs reported on every FY 03 capital asset plan (as well as in the exhibit 53) submitted by the agency to OMB? If no, why not? Identify actual performance according to the measures and in the format provided below. (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.)

TABLE D.3: CAPITAL PLANNING AND INVESTMENT CONTROL PROCESS

		FY 2003 Budget Materials	FY 2004 Budget Materials
3a	Number of capital asset plans and justifications submitted to OMB	0	0
3b	Number of capital asset plans and justifications submitted to OMB without requisite security information and costs?	0	0
3c	Were security costs reported for all agency systems on the agency's exhibit 53?	N/A	N/A
3d	Have all discrepancies been corrected?	N/A	N/A
3e	How many have the CIO/other appropriate official independently validated prior to submittal to OMB?	N/A	N/A

According to the BBG CIO, BBG is not required to prepare an exhibit 53, and its capital asset plan is under development.