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

Memorandum Report

Information Security Program Evaluation: Broadcasting Board of Governors

Report Number IT/A-02-07, September 2002 (UNCLASSIFIED VERSION)

MEMORANDUM REPORT IT-A-02-07

Information Security Program Evaluation:

Broadcasting Board Of Governors

September 2002

In response to the Government Information Security Reform Act (GISRA),[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). GISRA provides: (1) a comprehensive framework for establishing and ensuring the effectiveness of controls over information technology resources; and (2) a mechanism for improved oversight of federal agency information security programs. The specific objective of OIG's review was to determine whether BBG is effectively implementing the requirements of GISRA. The purpose, scope, and methodology for OIG's review are discussed in appendix A.

RESULTS IN BRIEF

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

[1] Public Law No. 106-398, Div. A, Title X, Subtitle G., 114 Stat. 1654A (2000), 44 U.S.C. 3531 et seq.

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.

BACKGROUND

The U.S. International Broadcasting Act of 1994[2] created BBG as a self-governing element within the former United States Information Agency, which provided some administrative, technical, and management support to BBG. The Foreign Affairs Reform and Restructuring Act of 1998[3] granted BBG independence from the United States Information Agency on October 1, 1999. BBG is responsible for overseeing all U.S. government-funded, civilian broadcasting, including the operations of the International Broadcasting Bureau (IBB), which includes the broadcasting entities of Voice of America (VOA), WorldNet Television and Film Service, and Office of Cuba Broadcasting. BBG also oversees two grantee organizations: Radio Free Europe/Radio Liberty and Radio Free Asia.

Information security is an important consideration for any organization that depends on information systems and information networks to carry out its mission or business. Information-supported government operations, including those at BBG are at increased risk. The dramatic expansion and rapid increase in the use of the Internet has changed the way the U.S. government communicates and conducts business. However, without proper safeguards, this widespread interconnectivity poses significant risks to the infrastructure it supports and makes it easier for individuals and groups to eavesdrop on or interfere with government operations, obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other information networks and systems.

Faced with growing concerns about information security risks to the federal government, the Congress passed and President signed GISRA into law in late 2000. GISRA provides: (1) a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support federal operations and assets; and (2) a mechanism for improving oversight of federal agency information security programs. Specifically, GISRA requires each agency to:

[2] Public Law 103-236, Title III, Sec. 314.

[3] Public Law 105-277, Division G.

- identify, use, and share best security practices;
- develop an agency-wide information security plan;
- incorporate information security principles and practices throughout the life cycles of the agency's information systems; and
- ensure that the information security plan is practiced throughout all life cycles of the agency's information systems.

In addition, GISRA assigns the agency's Chief Information Officer (CIO) the authority to administer key functions under the statute, including:

- designating a senior information security official who reports to the CIO;
- developing and maintaining an agency-wide information security program;
- ensuring that the agency effectively implements and maintains information security policies, procedures, and control techniques; and
- training and overseeing personnel with significant responsibilities for information security.

Finally, in addition to a number of other provisions, GISRA requires that each agency have an annual independent evaluation performed of its information security program and practices. OIG or the independent evaluator performing a review may use any audit, evaluation, or report relating to the effectiveness of the agency's information security program. The agency is required to submit the independent evaluation, along with its own assessment, to OMB as part of its annual budget request.

Overview of Broadcasting Board of Governors Information Security Program

Beginning early in 2001, BBG initiated a formal agency information security program to include the assignment of responsibilities, development of system security plans, and establishment of policies and procedures. BBG's information security program plan, issued in September 2001, identifies the CIO as the overall accountable official responsible for establishing agency information management policy and the agency information security program. In addition, the plan recognizes five functional areas[4] within BBG's overall structure and designates the directors of these areas as program officials with responsibilities for developing and

[4]The five functional areas consist of Office of Computing Services, Office of Cuba Broadcasting, Office of Internet Development, Office of Engineering and Technical Services, and VOA Broadcast Operations.

implementing a risk management-based security program to protect the information and information systems under their control. Lastly, the plan establishes a broadcast technology steering committee responsible for providing integrated technology to the agency for all operational and administrative activities.

To address the GISRA requirements for developing system-level security plans and performing program and system-level self-assessment reviews of general support systems[5] and major applications,[6] BBG formed five functional areas. In each functional area, the program manager grouped all systems and applications together under one system security plan and performed an annual program-level review of the functional area. The results of the self-assessments were then compiled and reported in the agency's plans of action and milestones (POA&M). Under GISRA, the POA&M must reflect all known security weaknesses within an agency, and be used as the authoritative management mechanism to prioritize, track, and manage all agency efforts to close security performance gaps.

REVIEW FINDINGS

Self-Assessments Need To Be Documented

BBG performed security self-assessments on its information systems in FY 2001, but the methodology and scope for the assessments were not documented. At the time of this review, BBG had not completed its FY 2002 self-assessment reviews. However, the CIO told OIG that these assessments will be completed using National Institute of Standards and Technology (NIST) guidance by the end of FY 2002. GISRA requires annual reviews of each agency-wide security program and system by senior management officials to ensure the protection of agency systems and data contained within the systems. The depth and breadth of the annual reviews depends on the risk to the system, completeness of prior reviews, and adequacy of the agency POA&M.

In FY 2001, BBG's five functional area managers completed self-assessment reviews and documented 36 information security weaknesses in BBG's POA&M. During FY 2002, one additional weakness was identified and corrected, while 19 of the original weaknesses were also corrected. Table 1 shows by control category,

[5] OMB Circular No. A-130, Appendix III defines a general support system as a set of interconnected information resources under the same direct management control and to share common functionality.

[6] OMB Circular No. A-130, Appendix III defines a major application as an application that requires special security attention because of the potential risk or harm from its loss, misuse, or unauthorized access.

the 17 remaining weaknesses defined in BBG's POA&M. For a detailed exhibit of BBG's information security weaknesses by functional area, see appendix B.

TABLE 1: BROADCASTING BOARD OF GOVERNORS INFORMATION SECURITY CONTROL WEAKNESSES

Control Objectives	Total Weaknesses
Management Controls	
Risk Management	4
Operational Controls	
Physical and Environmental Protection	1
Contingency Planning	2
Data Integrity	2
Documentation	1
Security Awareness, Training, and Education	1
Technical Controls	
Identification and Authentication	2
Logical Access Controls	3
Audit Trails	1
Total Control Weaknesses	**17**

BBG Lacks Adequate Information Security Policies and Procedures

OIG found that BBG's information security policies and procedures were outdated and incomplete. 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. BBG's information security program includes issue-specific policies, such as issuing e-mail reminders to information users about viruses, electronic mail attachments, installation of user software, participation in chat rooms, and security threats. Still, OIG found that employees lacked an awareness of the policies that do exist on the rules of behavior, incident reporting, and specific issues policies. In one functional area, employees were found to be using government equipment for their own personal use and visiting prohibited websites.

At the time of this review, BBG's management was in the process of hiring a contractor to develop and update its information system security policies and procedures. Effective implementation of security policies will help BBG management in addressing information security issues and ultimately result in the development and implementation of an improved information security program and protection of systems and information. It is not clear when BBG's new or updated policies and procedures will be finalized.

BBG Incident Response and Reporting Inadequate

OIG found that BBG lacked an information security incident response process and had 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 need 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 FY 2001 and FY 2002, none of which was 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 and major applications.

Recommendation 1: OIG recommends that the Broadcasting Board of Governors direct its Chief Information Officer to develop an agency-wide incident response capability and formal security incident reporting procedures for its information systems.

BBG Response

In commenting on a draft of this report (see appendix C), BBG concurred with this recommendation. BBG noted that procedures exist for reporting within the agency; however, they need to be more detailed and uniformly applied.

OIG Comments

OIG accepts this response and considers this recommendation resolved. OIG notes that GISRA requires that procedures include the notification of law enforcement officials and other offices and authorities, and consultation with the Federal Computer Incident Response Center. The center assists agencies with incident prevention and response. A lack of agency reporting procedures to the Federal Computer Incident Response Center hampers its ability to determine the scope of the threat to the Federal government and may affect other agencies and Departments. As noted in its response, BBG's procedures should support an agency-wide incident response capability and include required reporting outside the agency. BBG should provide OIG with its formal security incident reporting procedures for consideration in closing this recommendation.

System Security Plans Not Developed

OIG found that BBG had not developed security plans at the systems or major application level. Further, OIG found that BBG's approach to developing system security plans was flawed because it focused solely on functional areas and not individual 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 information technology 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. As shown in table 2, not one plan addresses each of 14 key elements of a security plan. In addition, five of the 14 elements are not addressed by BBG's five functional area system security plans.

TABLE 2: GENERAL SUPPORT SYSTEMS AND MAJOR APPLICATIONS

General Support Systems		Major Applications	
OMB Circular No. A-130 Requirement	Controls Contained in Security Plan	OMB Circular No. A-130 Requirement	Controls Contained in Security Plan
Rules of the System	No	Application Rules	No
Training	Partially	Specialized Training	Partially *
Personnel Controls	No	Personnel Security	Partially **
Incident Response Capability	Partially	Contingency Planning	Partially *
Continuity of Support	Partially	Technical Controls	Partially
Technical Security	Partially	Information Sharing	No
System Interconnections	No	Public Access Controls	Partially

* Two of three functional area security plans mentioned specialized training and contingency planning.
** One of three functional area security plans mentioned personnel security

BBG also reported on 23 systems in FY 2001 that were not reported under any of the functional areas in FY 2002. BBG could not provide OIG with information on these systems, including whether it had developed security plans for them.

Recommendation 2: OIG recommends that the Broadcasting Board of Governors direct its Chief Information Officer to develop security plans to address the information security requirements of each system.

BBG Response

In its written comments, BBG states that it initially designated five systems within the BBG for GISRA purposes and a security plan has been developed for each. Therefore, according to BBG, the objective of this recommendation would seem to have been met. BBG also states that OIG's recommendation appears to be based upon the assertion that the BBG had 31 reported systems for FY 2002. Further, BBG states that it had designated five systems and reported 31 different applications in use within these systems. BBG also states that an agency contractor recently concluded an analysis of one of the agency systems and recommended that consideration be given to dividing it into four separate domains.

OIG Comment

BBG is not correct in its statement that the objective of this recommendation appears to have been met. OIG's analysis of the functional area security plans found that a total of 31 systems or applications were distributed across the five functional areas designated by the BBG. BBG management informed OIG of its intent to group all systems within a functional area under one security plan regardless of the systems' functions. This approach, OIG believes, does not meet GISRA's requirements for system security plans. Further, as OIG notes in its report, BBG has 23 other systems that are not reported under any of the functional areas in FY 2002. These systems as well may need security plans in accordance with GISRA.

Information System Contingency Plans Needed

OIG found that BBG lacks system or major application contingency plans to support all of its information technology operations. As required by OMB Circular A-130, contingency plans ensure an agency's ability to recover from a disruption and provide service sufficient to meet the minimal needs of users. They are essential in the event of a power outage, hardware failure, fire, storm, or malicious intrusion.

OIG found that BBG functional areas were in different stages of IT contingency plan development. Specifically, the stages were:

- one functional area was revising its contingency plan;
- two functional areas were developing their contingency plans;
- one functional area was relying upon a contract provider to have a contingency plan in place; and
- one functional area was doing nothing to develop a contingency plan.

Contingency planning at the functional level was identified as a weakness by BBG's self-assessment in FY 2001, and it remains a weakness identified in its POA&M.

Recommendation 3: OIG recommends that the Broadcasting Board of Governors direct the Chief Information Officer to ensure that all functional areas and key systems and major applications have information technology contingency plans.

BBG Response

The BBG concurs with this recommendation.

OIG Comment

OIG accepts this response and considers this recommendation resolved. BBG should provide OIG with copies of its information technology contingency plans for functional areas, key systems and major applications for consideration in closing this recommendation.

Need for an Information Security Training Program

OIG found that BBG does not have an information security training program. BBG 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. Although the BBG Information Security Program Plan acknowledges the need for information security training and assigns the Office of Computing Services responsibility for developing and implementing an information security education program, BBG officials reported that no specific information security training was taking place. These officials stated that orientation training for new employees included an information awareness component; however, no employees OIG spoke with could recall such a component when they completed orientation. Also, neither the BBG training office nor the Office of Security was aware of having implemented initial or refresher information security training for employees.

Recommendation 4: OIG recommends that the Broadcasting Board of Governors, through its Chief Information Officer and training office director, develop and implement an information security training program that addresses the needs of all system users.

BBG Response

The BBG concurs with this recommendation.

OIG Comment

OIG accepts this response and considers this recommendation resolved. BBG should provide OIG with a copy of its information security training program for consideration in closing this recommendation.

Appendix A

PURPOSE, SCOPE, AND METHODOLOGY

Section 3535 of GISRA directs each agency to conduct an annual independent evaluation of its information security program and practices beginning in FY 2001. In response to GISRA, OIG conducted a review with the specific objectives to: (1) identify the BBG policies and procedures for securing information on its information systems; and (2) determine whether BBG is complying with GISRA with regard to establishing and ensuring the effectiveness of controls over information resources. For its 2002 report on GISRA, the OIG evaluated BBG's progress in implementing the requirements of the law.

To fulfill the review objectives, OIG met with BBG officials from IBB, VOA, Office of Cuba Broadcasting and system owners and information system security officers from the Department of State whose systems connect to BBG systems. OIG did not conduct a detailed review of BBG's grantee organizations, Radio Free Europe/Radio Liberty, and Radio Free Asia. They are private, nonprofit organizations that own and operate their own information technology systems.

In addition to interviews with appropriate BBG management and staff, OIG performed a detailed analysis of BBG's system security plans and information security program. OIG collected other relevant supporting information technology documentation as appropriate. OIG obtained written comments on a draft of this report and revised the report where appropriate. The BBG's comments are included in appendix C. Staff from OIG's Information Technology Evaluation Area performed this evaluation from February 2002 through July 2002. Contributors to this report were Frank Deffer, James Davies, Anthony Carbone, Matthew Worner, and Heather Rogers. Comments or questions about the report may be directed to Mr. Deffer at defferf@state.gov or at (703) 284-2715 or to Mr. Davies at daviesj@state.gov or at (703) 284-2673.

Appendix B

Agency Comments

BROADCASTING BOARD OF GOVERNORS
UNITED STATES OF AMERICA

September 5, 2002

Mr. Clark Kent Ervin
Inspector General
Office of Inspector General
U.S. Department of State
Washington, D.C. 20520-6817

Dear Mr. Ervin:

The Broadcasting Board of Governors (BBG) and the International Broadcasting Bureau (IBB) have reviewed the OIG's draft report titled *Information Security Program Evaluation: Broadcasting Board of Governors,* Report Number IT-A-O2-07. As a result of the review, the following comments are provided:

Recommendation 1: OIG recommends that the Broadcasting Board of Governors direct its Chief Information Officer to develop an agency-wide incident response capability and formal security incident reporting procedures for its information systems.

BBG Comment. The BBG concurs with the recommendation. Procedures exist for reporting within the agency, however, they need to be more detailed and uniformly applied. It is worth noting that the existing procedures were followed in the case of the four incidents cited in the draft report. Deliberate decisions were made not to report to FEDCIRC because the nature of the incidents did not warrant such a report. However, one incident was referred to the FBI for potential criminal prosecution.

Recommendation 2. OIG recommends that the Broadcasting Board of Governors direct its Chief Information Officer to develop security plans to address the information security requirements of each system.

BBG Comment. The BBG initially designated five systems within the BBG for GISRA purposes and a security plan has been developed for each. Therefore, the object of this recommendation would seem to have been met. These program plans are under continuing development as the agency makes every effort to protect its systems and its ability to accomplish our mission. This DIG recommendation appears to be based upon the assertion that the BBG had 31 reported systems for FY2002. In fact the agency had only designated five systems but reported 31 different applications in use within these systems. This reported number should have been 54, but in any case, there is no direct correlation between applications in use and the agency

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

systems that require a separate security plan. An agency contractor recently concluded an analysis of one of the agency 'systems' and recommended that consideration be given to dividing it into four separate security domains. The agency intends to do so and a security plan that implements this distinction will be developed. This plan will be a prototype for each of the other systems. Recommend the draft report be changed to suggest the BBG continue its efforts to analyze its programs to ensure that systems are designated consistent with the logical functional security boundaries and that security plans be developed for each. Further recommend that the references to reported systems be changed to "reported applications".

Recommendation 3. OIG recommends that the Broadcasting Board of Governors direct its Chief Information Officer to ensure that all functional areas and key systems and major applications have information contingency plans.

BBG Comment. The BBG concurs with this recommendation.

Recommendation 4. OIG recommends that the Broadcasting Board of Governors through its Chief Information Officer and training office director, develop and implement an information security training program that addresses the needs of all system users.

BBG Comment. The BBG concurs with this recommendation.

Thank you for the opportunity to provide our comments. Should you require additional information, please do not hesitate to contact me at (202) 619-1088, or contact Monica Smith, Acting Director, Office of Administration at (202) 610-3988.

Sincerely,

Kenneth Y. Tomlinson
Chairman