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

Office of Audits

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

Report Number AUD/IT-08-37, October 2008

IMPORTANT NOTICE

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

United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

PREFACE

This report was prepared by the Office of Inspector General (OIG) pursuant to the Inspector General Act of 1978, as amended, Section 209 of the Foreign Service Act of 1980, the Arms Control and Disarmament Amendments Act of 1987, and the Department of State and Related Agencies Appropriations Act, FY 1996. It is one of a series of audit, inspection, investigative, and special reports prepared by OIG periodically as part of its oversight responsibility with respect to the Department of State and the Broadcasting Board of Governors to identify and prevent fraud, waste, abuse, and mismanagement.

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

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

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

Mark W. Duda
Assistant Inspector General for Audits

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In response to the Federal Information Security Management Act of 2002 (FISMA),[1] the Office of Inspector General (OIG) performed an independent evaluation of the information security program at the Broadcasting Board of Governors (BBG). OIG reviewed BBG's progress in addressing information management and information security program requirements per FISMA and other statutory requirements, including Office of Management and Budget (OMB) guidance. The OIG team assessed performance in various areas, including inventory, plan of action and milestones (POA&M), certification and accreditation (C&A), security planning, contingency planning, risk management, incident response, security awareness and training, configuration management, and privacy requirements.

OIG could not perform an assessment of the adequacy of BBG's oversight and evaluation for 13 of its 14 identified systems because BBG had not conducted all aspects of a formal security program during FY 2008. Therefore, BBG could not provide the supporting documentation that would have been available for this FISMA review. As a result, BBG's overall assessment is poor, with improvements needed in several areas. OIG has, however, noted instances where improvements have been made since the FY 2007 review.

Since last year, BBG has completed one POA&M and C&A for its largest system: Central Infrastructure Domain. OIG's review of the supporting documentation demonstrated a thorough performance and compliance with security controls for this system. BBG has appointed a Privacy Officer to address the agency's privacy responsibilities. Further, BBG has developed an online training program for its employees using a customized application. The training content for the online course is developed by the Chief Information Security Officer (CISO) per statutory requirements and is revised as needed to address current hot topics.

While improvements have been made, OIG identified controls needing further enhancements. Specifically, the Broadcasting Board of Governors should ensure that

- a formal procedure for inventory identification and management is developed, documented, and implemented; and should include the process for identifying all changes to the inventory, including additions, retirements, and realignments of information systems;
- all required POA&Ms are completed for all major information systems;
- milestone completion dates and changes to milestone data are accurate in each POA&M;
- C&A is performed and completed for all FISMA reportable information systems;
- the security incident response plan is updated to include policy on safeguarding and responding to breaches related to personally identifiable information;

[1] 44 U.S.C. § 3545 et seq.

- a configuration management policy is developed that incorporates controls found in National Institute of Standards and Technology Special Pulication 800-53, including configuration management controls 1 through 8;
- complete and cirrent systems security plans for each of its systems are developed and maintained; and
- written policies to staff are established and disseminated, consistent with the four phases of an incident response program described in NIST SP 800-61, on handling and reporting security incidents to include, at a minimum, common types of security incidents, breaches of personally identifiable information, incident reporting timeframes, guidance for prioritizing incidents, and required post-incident activity.

BACKGROUND

Section 3545 of FISMA directs each agency to conduct an annual independent evaluation of its information security program and practices. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of operational, technical, and management controls over information technology (IT) that supports federal operations and assets. FISMA also provides a mechanism for improved oversight of federal agency information security programs. OMB Memorandum M-08-21,[2] issued July 14, 2008, contained guidance to assist OIGs with reporting FISMA performance metrics.

Section 3544(b) of FISMA requires that agencies develop, document, and implement an agency-wide information security program. As part of that program, section 3544(b)(6) requires that the CIO develop a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. OMB Memorandum M-04-25,[3] dated August 23, 2004, discusses the POA&M requirements for federal agencies, which include identifying tasks that need to be accomplished, the resources that are required to accomplish the elements of the POA&M, the milestones to meet the task, and scheduled milestone completion dates. The memorandum includes a spreadsheet to be used as a model to develop POA&Ms, including details such as the specific identified weakness, point of contact, resources required, scheduled completion date, milestones with attendant completion dates, changes in milestones, identification of weakness, and status. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53[4] lists the security controls that system owners should implement for their systems, depending on applicability to the system. The annual C&A process

[2] OMB Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 14, 2008.
[3] OMB Memorandum M-04-25, *Memorandum for Heads of Executive Department and Agencies*, August 23, 2004.
[4] NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, December 2006.

required by NIST SP 800-37[5] identifies security control weaknesses requiring remediation.

SCOPE AND METHODOLOGY

The OIG team consisted of staff with the OIG Office of Audits and the audit services firm of Regis & Associates, PC. References to the work conducted for this evaluation by OIG refer to this team. To perform the FISMA evaluation, OIG researched federal laws, regulations, and guidance to identify relevant criteria for implementing and managing information security programs. To identify prior issues and to follow up on past recommendations, OIG also reviewed previous reports that evaluated BBG's information security and privacy programs. OIG reviewed documents provided by BBG officials regarding systems inventory, C&A, POA&Ms, standard operating procedures, process guides, and training. OIG's analysis was based on information and documentation for the period ending the third quarter of FY 2008 to allow sufficient time for analysis and verification by the team. OIG included all 14 systems that BBG had categorized as moderate and low-impact level systems as its subset sample for this year's FISMA review. BBG does not have any systems categorized as high-impact level. BBG, however, has only completed the lifecycle process for one system. Therefore, OIG performed its review of BBG's inventory, contingency plans and annual testing, C&A, POA&M, privacy, and configuration management processes using documentation for this one system: the Central Infrastructure Domain system.

OIG met with BBG officials to discuss roles and responsibilities for implementing and managing information security programs for its networks. OIG met with the CISO to gather updates on C&A, configuration management, the POA&M process, and security awareness training. OIG held discussions with system owners to gather additional information on BBG's incident response procedures and BBG's configuration management process. In addition, OIG met with the Privacy Officer to gather information on efforts to protect personally identifiable information (PII). OIG held discussions with officials from OMB about expectations for government-wide compliance with Federal Desktop Core Configuration (FDCC) requirements.

The results of OIG's review are discussed below. OIG's Office of Audits conducted its fieldwork for this review from June 20 to August 29, 2008. A draft of this report was provided to BBG officials for their management review and comment, and all applicable comments were considered and incorporated into this final report.

In its October 10, 2008, formal response, BBG officials concurred with all of the recommendations made by OIG in this report (see Appendix A). OIG will follow-up on corrective actions taken, planned, or underway by BBG during its compliance analysis reviews to determine resolution of each recommendation. Comments or questions about the report may be directed to Karen Bell, Deputy Assistant Inspector General for Audits, at bellk@state.gov or by telephone at 703-284-2604.

[5] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

RESULTS

OIG could not perform an assessment of the adequacy of BBG's oversight and evaluation for 13 of its 14 identified systems because BBG had not conducted all aspects of a formal security program during FY 2008. Therefore, BBG could not provide the supporting documentation that would have been available for this FISMA review. As a result, BBG's overall assessment is poor, with improvements needed in several areas. OIG has, however, noted instances where improvements have been made since the FY 2007 review.

Inventory Management

The management and identification of the information systems inventory items is handled by staff within BBG's International Bureau of Broadcasting (IBB), including those systems that are defined as major information systems in accordance with Federal Information Processing Standards (FIPS) Publication 199.[6] BBG captures and tracks its inventory in one central repository, called the "Multi-user Information Security Forms Inspection Tool." This is a web-based inventory system, which also tracks implementation of NIST 800-53[7] controls and details the C&A processes.

OIG met with BBG officials to obtain an understanding of their methodology and approach for defining BBG's FISMA-reportable inventory. According to BBG management the guidelines defined in NIST SP 800-37[8] are the processes it uses for identifying and managing FISMA reportable major information systems and thus BBG therefore did not develop its own written process. BBG management further explained that the system owners and the four members of the CIO staff are in continuous (often daily) communication with each other. For these reasons, BBG officials determined that no additional written internal policy or procedures were necessary.

Some of BBG's major information systems ride on the general support systems (GSS)[9] for internal communications. The BBG Central Infrastructure Domain, Central Services Domain, Central Extranet Domain, Central BBG Domain, and Cuba Broadcasting Headquarters Network (Cuba HQ) are all GSS. The Central Infrastructure Domain provides the link and routing layers, as well as what BBG refers to as the network "glue services" (e.g., Domain Naming System) for the entire agency internet (BBG's network of interconnected IP networks, not to be confused with the public

[6] FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
[7] NIST SP 800-53, revision 1, *Recommended Security Controls for Federal Information Systems*, December 2006.
[8] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.
[9] A general support system is an interconnected set of information resources under the same direct management control that share common functionality. It normally includes hardware, software, information, data, applications, communications, and people. Sources: NIST SP 800-53 and OMB Circular A-130, Appendix III.

Internet). The four other general support systems use the services of the Central Infrastructure Domain but are enumerated separately for the purposes of FISMA and OMB Circular A-130[10] criteria for setting accreditation boundaries described in NIST SP 800-37.

Currently, BBG has identified 14 major FISMA-reportable systems that comprise ten agency and four contractor-owned and/or operated major information systems. These ten BBG-owned major information systems include the following: the five GSS systems previously listed, the Integrated Digital Audio Production System (IDAPS), the Video Production System, the Master Control Automation System, the Cuba Broadcasting Public Internet Website, and Security Credentialing System. The four contractor-owned and/or operated major information systems include the following: the Public Internet Website, the Public Internet Media Streaming Site, the BBG Public Internet Mail Distribution Lists, and the VOA Public Internet Mail Distribution Lists.

Based on information from BBG management, OIG determined that BBG's methodology of identifying major information systems in accordance with NIST SP 800-37 is a reasonable starting point; however, its process is not documented to formalize and describe roles and responsibilities. A documented inventory process will enable BBG to ensure a continuous process is in place with adequate management oversight.

Recommendation 1: The Broadcasting Board of Governors should develop, document, and implement a formal procedure for inventory identification and management. This procedure should include the process for identifying all changes to the inventory, including additions, retirements, and realignments of information systems.

Plan of Action and Milestones Process

As reported last year and again for FY 2008, BBG has not developed or implemented formal written processes, policies, or procedures to sufficiently address risk management as part of its POA&M program. BBG officials stated that doing so would not necessarily contribute to protecting their information systems, and that the existence of such policies is not required by statute. OIG reviewed applicable statutes and regulations and agreed that BBG was not technically required to develop and implement written processes, policies, and procedures. However, OIG's interpretation of the applicable statutes and regulations places the onus on BBG to document and formalize its POA&M process in order to meet the intent of relevant OMB and NIST guidance.[11] This guidance states that agencies should use the POA&M process as a management tool for identifying and tracking remedial actions. According to OMB Memorandum M-04-25, the POA&M process is designed to resolve IT security control weaknesses with prioritization to ensure vulnerabilities are addressed in a timely and cost-effective manner. Without an effective POA&M process, security control weaknesses may result

[10] OMB Circular A-130, *Management of Federal Information Resources*, November 28, 2000.
[11] NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006, and NIST SP 800-37.

in the unauthorized access, use, disruption, disclosure, modification, or destruction of information.

BBG's POA&M process was not fully implemented for FY 2008. Specifically, BBG had completed a POA&M for only one of its reported 14 systems, the Central Infrastructure Domain system. The POA&M reflected action items needed to address 41 security control categories mandated by OMB and NIST guidance.[12] Agencies categorize their systems according to FIPS 199 standards to determine which NIST SP 800-53 controls are required.

OIG included all 14 reported systems as part of its subset sample for performing an analysis of BBG's POA&M process. Although OIG cannot draw conclusions about the universe of BBG systems based on the sole POA&M BBG completed in FY 2008, it can summarize its review results for the available POA&M: the Central Infrastructure Domain, a GSS which is connected to the other reported systems. The POA&M addressed all known security weaknesses for the Central Infrastructure Domain system through testing the security-control categories. The POA&M included OIG findings where applicable, which were prioritized for timely and appropriate measures. However, BBG has not addressed known weaknesses for the remaining 13 systems. During the FY 2007 FISMA review, BBG provided OIG with 13 POA&Ms, which OIG reviewed at that time. For the current year's review, BBG did not provide POA&Ms for 13 systems because officials stated that they were outdated and would change based upon the newly mandated FDCC requirements. OIG found that BBG's CIO centrally tracks the POA&M that BBG developed for the one system and reviewed it on a regular basis.

OIG discussed the Central Infrastructure Domain POA&M with the BBG CISO and other BBG officials. OIG compared it with the POA&M for the same system reviewed during the prior year and found that the current POA&M was more complete and contained detailed information for more action items.[13] The POA&M from the prior year, while listing many more action items, did not include detailed information for each action item, such as scheduled completion dates, milestones and completion dates, milestone changes, and resources required. Both POA&Ms listed the status of action items as ongoing and identified whether the items had been identified during a Chief Financial Officer audit or other external review. The current POA&M was well written and closely followed the guidance issued in OMB Memorandum M-08-21.[14] The POA&M addressed weaknesses in 41 security control categories from NIST SP 800-53. In addition, for the most part, the POA&M included information for points of contact, monetary resources required to complete POA&M action items, scheduled completion dates, milestones and completion dates, milestone changes, how the weakness was identified, and its status. The plan was only remiss in that some of the milestone

[12] FISMA directed NIST to develop standards to categorize all information and systems, which NIST published in Federal Information Processing Standards 199. OMB reiterated this in its guidance, Memorandum M-08-21, dated July 14, 2008.
[13] The current POA&M included 41 NIST SP-800-53 security controls, whereas the POA&M from the prior year assessed only 32, but included much more detailed information.
[14] OMB Memorandum M-08-21.

completion dates and milestone changes data were incomplete. OIG advised BBG officials of these omissions and encouraged them to consistently include such information so as to better manage the POA&M process in the future.

Recommendation 2: The Broadcasting Board of Governors should ensure that all required plans of action and milestones are completed for all major information systems.

Recommendation 3: The Broadcasting Board of Governors should ensure that milestone completion dates and changes to milestone data are accurate in each plan of action and milestones.

Certification and Accreditation

Significant improvements are needed for the C&A process, in which OIG concludes BBG is currently failing. Each of the 14 reported systems were due for C&A during FY 2008; however, BBG had completed C&A for only one system: Central Infrastructure Domain. According to the CISO, the other 13 systems did not undergo the required C&A because of limited resources. As such, BBG management focused their time and attention to their largest major information system, the Central Infrastructure Domain.

Standards and guidance for performing C&A is contained within NIST SP 800-37 and NIST SP 800-53, revision 1. As stated within the guidance, security certification and accreditation are closely related and, at the same time distinct, activities. Officials must be able to determine the risk to operations, assets, or individuals and the acceptability of such risk given the mission or business needs of their agencies. Officials must weigh the appropriate factors and decide to either accept or reject the risk to their respective agencies. Security certification supports security accreditation by providing authorizing officials with information necessary to make credible, risk-based decisions about whether to place new information systems into operation or to continue using the current systems. Security accreditation includes the acceptance and management of risk—the risk to agency operations, agency assets, or individuals that results from the operation of an information system.

OIG reviewed the one completed C&A package for the Central Infrastructure Domain to identify, certify, and accredit security controls. With two apparent exceptions, OIG found the C&A package to be thorough and complete in accordance with standards. The package, however, seemed to be missing the privacy impact assessment (PIA) and the certification test plan. In follow-up meetings with BBG officials, however, the OIG learned that the PIA was not required because the system did not collect, maintain, or share PII, while the requirement for the certification test plan had been fully satisfied with an annual test performed in FY 2008.

Annual testing for the Central Infrastructure Domain system security controls was completed during FY 2008 and resulted in satisfactory results except for five sampled controls. The NIST SP 800-53 security controls that failed are as follows: Access Controls AC-04 and AC–07 that relate to Information Flow Enforcement and

Unsuccessful Login Attempts, respectively; System and Communication Protection controls SC–04 and SC-07 as they relate to sharing of Information Remnants and Boundary Protection, respectively; and control IA-2 – Identification and Authentication as it relates to User Identification and Authentication. In OIG's estimation, these exceptions are minimal and do not affect the overall results of the annual test, given that other access, identification, authorization, system, and communication-protection controls were tested successfully. The Contingency Plan for this system was also successfully tested and updated during FY 2008.

Recommendation 4: The Broadcasting Board of Governors should conduct certification and accreditation testing on the remaining 13 major information systems and bring these systems into compliance with statutory requirements.

Privacy

BBG has made progress since last year in addressing its privacy responsibilities by assigning a Privacy Officer, issuing some of the required privacy policies, and performing PIAs for one of its information systems. BBG also improved posting Privacy Act information on its website.

Federal privacy guidance is described in Section 208 of the E-Government Act of 2002, OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* and OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.* Per the E-Government Act of 2002, agencies are required to conduct PIAs for electronic information systems and information collection and make the assessments publicly available. Further, the agency must post privacy policies on agency websites and translate privacy policies into a standardized machine-readable format. OMB Memorandum M-03-22 provides additional guidance to the agencies and directs them to conduct reviews of how information about individuals is handled within agencies when they use electronic means to collect new information or when agencies develop or buy new systems to handle collections of PII. OMB Memorandum M-07-16 reemphasizes the responsibilities under existing law, executive orders, regulations, and policies to assist agencies to appropriately safeguard PII and to train employees about their responsibilities in this area. Threshold analyses are used as a good management tool for each agency's privacy initiatives.

BBG updated its website to include internet privacy policy and reports to address OMB Memorandum M-03-22 requirements. The BBG Internet Privacy Policy webpage states that the agency collects no personal information when the public visits the website unless the public chooses to provide that information voluntarily. BBG also added a *Privacy Reports* webpage, which includes links to its System of Records Notice and to the PIA for the Momentum Financials System, which was prepared by BBG because this is its outsourced financial management system and it contained contractor privacy information.

BBG also made progress in implementing the provisions of OMB Memorandum M-07-16 by issuing four policies and two implementation plans. The four policies are as follows: (1) privacy awareness training, (2) privacy breach notification, (3) BBG rules of behavior for safeguarding PII, and (4) PIA. The implementation plans address (1) eliminating unnecessary use of social security numbers and (2) reviewing and reducing the volume of PII. BBG officials did not indicate when the implementation plans will be disseminated to staff.

OMB Memorandum M-07-16 also requires each agency to develop and implement a breach notification policy within 120 days of its issue date of May 22, 2007. BBG did not issue its *Privacy Breach Notification Policy* until July 14, 2008, and it still has not updated its *Information Security Incident Response Plan* to reference the new policy.

BBG completed privacy threshold analyses for five of its 14 information systems: the Central Infrastructure Domain; the Central BBG Domain, the Central Extranet Domain, the IDAPS Audio Production System, and the Video Production System. The analyses concluded that PIAs were not required for the five systems. According to BBG's Senior Agency Official for Privacy, BBG did not perform threshold analyses or PIAs on the remaining systems because the systems were not newly acquired or modified during the year, as provided for by OMB Memorandum M-03-22.

Recommendation 5: The Broadcasting Board of Governors should update its Information Security Incident Response Plan to reflect the Privacy Breach Notification Policy with regard to safeguarding against and responding to personally identifiable information breaches per Office of Management and Budget Memorandum M-07-16.

Configuration Management

BBG has not issued an adequate configuration management (CM) policy. CM controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended. This includes the following: policies, plans, and procedures; current configuration identification information; proper authorization, testing, approval, and tracking of all configuration changes; routine monitoring of the configuration; and software updates on a timely basis to protect against known vulnerabilities.

In FY 2008, all 14 of BBG's systems were required to have a C&A, but only one was completed: the Central Infrastructure Domain. OIG selected this system for review and applied NIST 800-53, revision 1, standards to determine whether BBG's documentation was in compliance. BBG provided OIG with its IT Change Management Policy as evidence of an agency-wide security configuration management policy. While the Change Management Policy incorporates several key components of CM standards, it lacks others such as common security configuration procedures for all types of systems and workstations and detailed change control procedures.

Recommendation 6: The Broadcasting Board of Governors should develop a configuration management policy that incorporates controls found in National Institute of Standards and Technology Special Publication 800-53, including configuration management controls 1 through 8.

Federal Desktop Core Configuration (FDCC):

OMB Memorandum M-07-11[15] requires agencies to adopt FDCC standards. Specifically, these standards require agencies to adopt standardized security configurations for desktops when using Microsoft Windows XP and Vista operating systems. BBG's workstations currently use the Windows 2000 operating system; therefore, this requirement currently is not applicable. BBG management has indicated it will be transitioning to Windows XP within the next year and, at that time, it will be implementing FDCC compliance requirements.

Incident Reporting

BBG's security incident reporting program requires further improvement. Specifically, BBG has not updated its information security incident response plan to identify common types of security events that require reporting. It also does not include information on potential PII breaches, guidance on prioritizing security events, and dissemination of incident reporting procedures.

FISMA requires agencies to establish procedures for detecting, reporting, and responding to security incidents. NIST SP 800-61 provides guidance to agencies on establishing an effective incident response program. The guidance focuses on four phases: (1) preparation, (2) detection and analysis, (3) containment/eradication/recovery, and (4) post-incident activity. Because events can occur in numerous ways, it is important for officials to develop comprehensive procedures with step-by-step instructions for handing every event, especially common types of events. OMB requires agencies to develop system security plans (SSP).[16] The SSP is an overview of the security requirements of the system and describes the controls in place—or planned—to meet those requirements. The plan also delineates the responsibilities and expected behavior for all individuals who access the system. The system security is organized into three general classes of security controls: management, operational, and technical. Incident reporting is part of the operational security controls.

OIG identified several areas that require improvement by BBG. For example, BBG stated in its current information security incident response plan, dated June 7, 2004, that system owners or designated individuals responsible for information security are to be identified in the SSP and that system users should report any security incident through reporting channels established by the system owners or designated individuals. However, based on its review, OIG found that only one of the 14 systems has an SSP. The

[15] OMB Memorandum M-07-11, *Implementation of Commonly Accepted Security Configuration for Windows Operating Systems*, March 2007.
[16] OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

information security incident response plan has not been updated and still states that the identity of system owners is found in the SSP. The identity of system owners is located on BBG's Intranet website, yet the Intranet address has not been included in the incident response plan. Further, BBG's information security incident response plan states that system owners or designated individuals should exercise good judgment and common sense when evaluating and reporting security incidents, but it does not provide examples to assist in making these determinations.

To ensure proper handling and reporting of security events throughout the agency, OIG believes that BBG should provide more information to its system owners and designated individuals, including common types of security events, potential PII breaches, reporting timeframes, and guidance for prioritizing events. In addition, the contact information pertaining to internal and external groups, such as human resources, legal, other incident response teams, and law enforcement entities, should be included in the security incident response plan to facilitate communication. For example, the information security incident response plan states that if an incident involves deliberate activity by a user, one or more additional reports should be filed with the Offices of Personnel, Contracts, or Security. However, specific contact information is not provided in the information security incident reporting plan. By having information readily available, the amount of time spent by staff locating pertinent information may be reduced, thereby ensuring sufficient time for analyzing and properly reporting relevant security events.

Additionally, BBG's information security incident response plan does not address post-incident procedures, which involves identifying lessons learned, assessing the effectiveness of the incident reporting process, and identifying improvements in security controls and practices. For example, BBG had a security incident on July 22, 2008, that involved malicious code injected in its server database. The incident was discovered by employees and reported to a member of the Office of Engineering (E/II) technical staff. The incident was escalated through the reporting channels in E/II to the technical services team leader and then to the head E/II, who reported the incident via email to the CISO. The CISO determined that the incident should have been referred to the United States Computer Emergency Readiness Team (US-CERT)[17] because it met the US-CERT federal agency reporting guidelines for a category 3 incident involving malicious code. The incident[18] was forwarded by the CISO to US-CERT on July 22, 2008, and the code on the affected server was corrected by the appropriate officials.

Further, actions taken by BBG officials for this security incident contained the first three phases of the incident response process; however, the fourth phase of the process—post incident procedures—was not fully performed. The fourth phase requires

[17] The US-CERT is a partnership between the Department of Homeland Security and the public and private sectors to protect the nation's Internet infrastructure. US-CERT coordinates defense against and responses to cyber attacks across the nation. US-CERT is responsible for 1) analyzing and reducing cyber threats and vulnerabilities, 2) disseminating cyber threat warning information, and 3) coordinating incident response activities.

[18] Report No. 2008-US-CERTv33F1P7D.

that BBG develop lessons learned, assess the incident reporting process, and improve security controls as needed. Lessons learned and other data gathered from each incident can be used to identify systemic security weaknesses and deficiencies in policies and procedures. Although the malicious code was eliminated from the server and officials are currently rewriting code for other vulnerable coding scripts, BBG officials did not develop information regarding improving the security controls that would prevent either intentional or accidental changes to code. Lessons learned and other data gathered from each incident can be used to identify systemic security weaknesses and deficiencies in policies and procedures.

During its review, OIG received mixed responses from system owners about their understanding of the incident reporting process, as well as their grasp of their individual responsibility to report information security incidents. For example, several system owners indicated that all incident reporting procedures had been consolidated and published on the BBG Intranet website. However, another system owner informed OIG that there are no written procedures regarding incident reporting for the system but that users inform the system owner of any known problems. A third system owner stated that incident reporting requirements are separated within two procedures that differ for unprivileged and privileged users. Unprivileged users report incidents to the help desk, while privileged users report incidents to their system managers. OIG believes that inconsistencies in reporting and handling security incidents throughout the agency could hamper BBG's ability to effectively manage its information systems.

Recommendation 7: The Broadcasting Board of Governors should develop and maintain complete and current systems security plans for each of its systems.

Recommendation 8: The Broadcasting Board of Governors should establish and disseminate written policies—consistent with the four phases of an incident response program described in NIST SP 800-61—to staff that explain the proper handling and reporting of security incidents. This should include, at a minimum, common types of security incidents, breaches of personally identifiable information, incident reporting timeframes, guidance for prioritizing incidents, and required post-incident procedures.

Security Awareness Training, Peer-to-Peer File Sharing

BBG has made some progress in administering security awareness training to its employees. This includes developing an online training program for its employees using a customized application named "Moodle." The training content for the online computer security course is developed by the CISO per statutory requirements, and it is revised as needed to address hot topics. The current training content includes discussions on computer risks and vulnerabilities, disclosure of personal information, malicious software, and the protection of sensitive information. However, policies regarding the use of collaborative web technologies and peer-to-peer file sharing were not part of the awareness training provided to employees as required by OMB Memorandum M-08-21. Privacy matters are covered separately within another training course developed by BBG's Privacy Officer. The privacy training material covers system users'

responsibilities, general privacy principles, and regulatory guidance. As of August 2008, 1,757 (approximately 51 percent) of 3,460 BBG employees had received certificates for the online awareness courses—computer security and privacy.

Security awareness training is being administered to BBG employees with system access; however, BBG is not focusing on providing awareness, in any form, to those without system access. Per OMB Memorandum M-08-21, each agency should be providing security awareness to all users—those with and without system access—as part of the agency's training efforts. BBG is not complying with this requirement, and it did not have any plans to train non-system employees during the course of the FISMA review. Further, BBG officials are not reviewing training records for duplication of entries. In documentation received, OIG noticed in several cases where the same employee was reported more than once on the training records for the online security awareness training course. OIG brought this recordkeeping issue to the attention of BBG officials, who indicated that steps will be put in place to address this matter.

RECOMMENDATIONS

Recommendation 1: The Broadcasting Board of Governors should develop, document, and implement a formal procedure for inventory identification and management. This procedure should include the process for identifying all changes to the inventory, including additions, retirements, and realignments of information systems.

Recommendation 2: The Broadcasting Board of Governors should ensure that all required plans of action and milestones are completed for all major information systems.

Recommendation 3: The Broadcasting Board of Governors should ensure that milestone completion dates and changes to milestone data are accurate in each plan of action and milestones.

Recommendation 4: The Broadcasting Board of Governors should conduct certification and accreditation testing on the remaining 13 major information systems and bring these systems into compliance with statutory requirements.

Recommendation 5: The Broadcasting Board of Governors should update its Information Security Incident Response Plan to reflect the Privacy Breach Notification Policy with regard to safeguarding against and responding to personally identifiable information breaches per Office of Management and Budget Memorandum M-07-16.

Recommendation 6: The Broadcasting Board of Governors should develop a configuration management policy that incorporates controls found in National Institute of Standards and Technology Special Publication 800-53, including configuration management controls 1 through 8.

Recommendation 7: The Broadcasting Board of Governors should develop and maintain complete and current systems security plans for each of its systems.

Recommendation 8: The Broadcasting Board of Governors should establish and disseminate written policies—consistent with the four phases of an incident response program described in NIST SP 800-61—to staff that explain the proper handling and reporting of security incidents. This should include, at a minimum, common types of security incidents, breaches of personally identifiable information, incident reporting timeframes, guidance for prioritizing incidents, and required post-incident procedures.

APPENDIX A – MANAGEMENT RESPONSE

BROADCASTING BOARD OF GOVERNORS
UNITED STATES OF AMERICA

October 10, 2008

Mr. Mark Duda
Assistant Inspector General for Audits
Office of Inspector General
U.S. Department of State

Dear Mr. Duda:

This is in response to your memorandum dated September 29, 2008, regarding the Office of Inspector General Fiscal Year 2008 Federal Information Security Management Act (FISMA) Reporting Template for the Broadcasting Board of Governors (BBG).

We appreciate the opportunity to respond to the Office of Inspector General's FISMA evaluation of the Broadcasting Board of Governors' (BBG) information security program and practices.

We concur with the eight recommendations in the report. If you have any questions, please feel free to contact Ms. Renee Tyrance-Gauff, International Broadcasting Bureau (IBB) Chief of Analysis and Administration Division, at (202) 203-4664, or Mr. Vince Nowicki, IBB Director for Engineering & Technical Services, at (202) 382-7300.

Sincerely,

Jeffrey N. Trimble
Executive Director

330 INDEPENDENCE AVENUE, SW ROOM 3360 COHEN BUILDING WASHINGTON, DC 20237 (202) 203-4545 FAX (202) 203-4568

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

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

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

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