UNITED STATES DEPARTMENT OF STATE
AND THE BROADCASTING BOARD OF GOVERNORS

OFFICE OF INSPECTOR GENERAL

AUD-IT-IB-13-04	Office of Audits	November 2012

Audit of the Broadcasting Board of Governors Information Security Program

PREFACE

This report is being transmitted pursuant to the Inspector General Act of 1978, as amended, and Section 209 of the Foreign Service Act of 1980, as amended. It is one of a series of audit, inspection, investigative, and special reports prepared as part of the Office of Inspector General's (OIG) responsibility to promote effective management, accountability, and positive change in the Department of State and the Broadcasting Board of Governors.

In accordance with the Federal Information Security Management Act of 2002 (FISMA), OIG performed an audit of the Broadcasting Board of Governors Information Security Program for FY 2012. To perform this review, OIG contracted with the independent public accountant Williams, Adley & Company-DC, LLP. The management letter is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents. The management letter contains identified weaknesses in information security that did not meet the criteria for inclusion in the annual FISMA report but require management action.

The independent public accountant identified weaknesses in security training and the contingency planning process.

OIG evaluated the nature, extent, and timing of the independent public accountant's work; monitored progress throughout the audit; reviewed supporting documentation; evaluated key judgments; and performed other procedures as appropriate. OIG concurs with the findings, and the recommendations contained in the management letter were developed based on the best knowledge available and discussed in draft form with those individuals responsible for implementation. OIG's analysis of management's response to the recommendations has been incorporated into the report. OIG trusts that this report will result in more effective, efficient, and/or economical operations.

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

Harold W. Geisel
Deputy Inspector General

WILLIAMS ADLEY

Audit of the Broadcasting Board of Governors Information Security Program

November 7, 2012

Office of Inspector General
U.S. Department of State
Washington, DC

Williams, Adley & Company-DC, LLP has performed an audit of the Broadcasting Board of Governors' (BBG) Information Security Program. We audited the BBG compliance with the Federal Information Security Management Act, Office of Management and Budget requirements and National Institute of Standards and Technology standards. We performed this audit under Contract No. SAQMMA10F2159. The audit was designed to meet the objectives described in the report.

We conducted this performance audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. We communicated the results of our audit and the related findings and recommendations to the U.S. Department of State Office of Inspector General.

We appreciate the cooperation provided by BBG personnel during the audit.

Williams, Adley & Company-DC, LLP
Washington, DC

WILLIAMS, ADLEY & COMPANY-DC, LLP
Certified Public Accountants / Management Consultants
1030 15th Street, NW, Suite 350 West • Washington, DC 20005 • (202) 371-1397 • Fax: (202) 371-9161
www.williamsadley.com

Acronyms

AC	Access Control
AD	Windows Active Directory
AT	Awareness and Training
BBG	Broadcasting Board of Governors
CIO	Chief Information Officer
CM	Configuration Management
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
IT	information technology
NIST	National Institute of Standards and Technology
OCB	Office of Cuba Broadcasting
OIG	Office of Inspector General
OMB	Office of Management and Budget
PM	Program Management
POA&M	Plans of Action and Milestones
PS	Personnel Security
SP	Special Publication
US-CERT	United States Computer Emergency Response Team

TABLE OF CONTENTS

Executive Summary

In accordance with the Federal Information Security Management Act of 2002 (FISMA),[1] the Office of Inspector General (OIG) contracted with Williams, Adley & Company, LLP (referred to as "we" in this report), to perform an independent audit of the Broadcasting Board of Governors (BBG) Information Security Program's compliance with Federal laws, regulations, and standards established by FISMA, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). Additionally, the results are designed to assist OIG in providing responses to the Department of Homeland Security (DHS) FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics, dated March 6, 2012.

We reviewed BBG's remedial actions taken to address the FY 2011 reported information security program control weaknesses identified in OIG's FY 2011 report *Evaluation of the Broadcasting Board of Governors Information Security Program* (AUD/IT/IB-12-15, November 2011). The statuses of the FY 2011 evaluation recommendations are in Appendix B. Since FY 2011, BBG has taken the following steps to improve management controls:

- Implemented security tools and procedures to perform routine vulnerability assessments across the BBG network.
- Developed policies and procedures to limit and manage the use of shared, test, and guest user accounts.

Overall, we found that BBG had continued its efforts to further develop its information security program. However, we identified control weaknesses that, if exploited, could adversely affect the confidentiality, integrity, and availability of information and information systems. Further, we found that BBG had not taken corrective action to remediate all of the control weaknesses identified in the FY 2011 FISMA report. To improve the information security program and to bring the program into compliance with FISMA, OMB, and NIST requirements, BBG should address the control weaknesses discussed.

BBG did not fully develop security procedures and guidance to govern configuration management processes, the absence of which may lead to ineffectual systems security and inconsistent performance. We are recommending that the Chief Information Officer (CIO) ensure that security configuration standards and procedures are completed, as required by NIST Special Publication (SP) 800-53, Revision 3.[2]

Although BBG's Information Technology Department provided services and guidelines to the Office of Cuba Broadcasting (OCB), BBG's CIO did not possess the authority to enact consequences for noncompliance with BBG security requirements, potentially exposing BBG's network and systems to risks and vulnerabilities. We are recommending that BBG develop and

[1] Pub. L. No. 107-347, tit. III, 116 Stat. 2946 (2002).

[2] NIST SP 800-53, Rev. 3, "Recommended Security Controls for Information Systems and Organizations," Aug. 2009 (updated through May 2010).

implement policies to require all agencies with systems that connect to the BBG network to follow established BBG security policies. Further, we are recommending that BBG grant the CIO the necessary authority to enforce consequences for noncompliance.

BBG's user account management controls did not ensure that system access was provided to only authorized personnel. We observed the following management control deficiencies for "active" user accounts in the Windows Active Directory[3] (AD): 93 accounts were not used for more than 90 days, 31 accounts did not require the use of a password, and passwords for 411 accounts were not changed for over 90 days. We are recommending that the CIO ensure that user accounts are properly configured and maintained in accordance with existing BBG policies.

One of two security incidents that BBG identified and reported to the United States Computer Emergency Readiness Team (US-CERT) at DHS was reported three business days after observation rather than within one business day after observation, as required by US-CERT. Without timely reporting of security incidents to US-CERT, BBG may adversely impact US-CERT's ability to improve the nation's cybersecurity. We are recommending that the CIO ensure that BBG Computer Security Incident Management Policy procedures are followed and security incidents are reported in a timely manner, as required by US-CERT.

Less than 25 percent of BBG's personnel completed security awareness training in FY 2011, yet BBG did not sanction employees and contractors who did not complete the annual security awareness training course. Without the completion of initial and annual security awareness training, personnel may be unaware of new risks that may compromise the confidentiality, integrity, and availability of information. We are recommending that the CIO develop and implement a formal sanction process for personnel who do not successfully complete required security awareness training.

Although BBG had implemented revisions to its Plans of Action and Milestones (POA&M) program, the completed POA&Ms did not consistently provide sufficient detailed information. Without a robust POA&M program that includes sufficient details for managing and tracking corrective actions, BBG's information technology (IT) management may be unable to properly assess and implement corrective activities and may be unable to prevent security issues from being resolved in a timely manner. We are recommending that the CIO ensure that the BBG POA&M program is fully developed to include data elements required by OMB Memorandum M-02-01.[4]

BBG's remote access policy allowed users to access the BBG network from personally owned computers using software provided by BBG. However, BBG had not implemented procedures to ensure that remote access was granted only to computers that had proper security safeguards. Without proper policies and procedures that require the use of properly secured third-party devices, BBG network and systems may be susceptible to the introduction of viruses,

[3] Windows Active Directory (AD), a technology created by Microsoft, provides a variety of network services, such as identification and authentication, directory access, and other network services.

[4] OMB Memorandum M-02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones," Oct. 17, 2001.

worms, or other malicious code. We are recommending that the CIO implement procedures to assess the security configurations of third-party devices requesting access to the BBG network and grant access only to properly configured devices, as required by NIST SP 800-53, Revision 3.[5]

BBG did not implement a process or procedure to fully manage and routinely update its inventory of IT assets at least annually or when changes were made to its systems. Without a process to identify, document, and maintain an inventory of major and minor applications, as well as general support systems, BBG may not have an accurate accounting of its IT assets and the related system interfaces and underlying support systems. We are recommending that the CIO create and implement a standardized process to collect information, update the BBG system inventory and update the general support system's security plan control, as required by NIST SP 800-53, Revision 3.[6]

BBG did not develop and implement contingency planning and testing policies and procedures compliant with OMB requirements and requirements contained in NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems." Specifically, BBG did not complete its enterprise-wide and system-specific contingency plans or conduct contingency tests. Without an effective contingency plan, BBG may be unable to access critical information and resources and perform mission-critical business functions in the event of an extended outage and/or disaster. We are recommending that the CIO ensure that contingency planning policies and procedures be developed and implemented and that personnel responsible for network and systems recovery complete training and perform periodic testing.

Although this report contains nine recommendations, we believe the most significant security deficiencies relate to security standards and procedures (Finding A), compliance enforcement authority (Finding B), Plans of Action and Milestones (Finding F), and enterprise-wide and system-specific contingency plans (Finding I).

In BBG's November 6, 2012, response (see Appendix C) to this report, BBG concurred with all of the report's recommendations. Based on this information, the Office of Inspector General (OIG) considers each recommendation resolved. BBG's responses and OIG's analyses are presented after each recommendation.

[5] NIST SP 800-53, Rev. 3, AC-17, "Remote Access."
[6] NIST SP 800-53, Rev. 3, CM-8, "Information System Component Inventory."

Background

With the passage of FISMA, Congress recognized the importance of information security to the economic and national security interests of the United States and required each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or source. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of management, operational, and technical controls over IT that supports Federal operations and assets, and it provides a mechanism for improved oversight of Federal agency information security programs.

To strengthen information system security, FISMA assigns specific responsibilities to DHS, NIST, OMB, and other Federal agencies. In particular, FISMA requires the head of each agency to implement policies and procedures to cost effectively reduce IT security risks to an acceptable level. To ensure the adequacy and effectiveness of information system controls, FISMA requires agency program officials, chief information officers, senior agency officials for privacy, and inspectors general to conduct annual reviews of the agency's information security program and report the results to DHS.

On an annual basis, OMB provides guidance with reporting categories and questions to meet the current year's reporting requirements.[7] OMB uses responses to its questions to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with FISMA.

Objective

The objective of this audit was to perform an independent evaluation of BBG's information security program and practices for FY 2012, which included testing the effectiveness of security controls for a subset of systems, as required.

Results of Audit

Overall, we found that BBG made progress in FY 2012 toward developing its information security program, but significant challenges remain. BBG needs to address several control weaknesses as described to bring the information security program into compliance with FISMA, OMB, and NIST requirements.

Finding A. Security Standards and Procedures Need To Be Implemented and Enforced

As first identified during the FY 2010 *Review of the Information Security Program at the Broadcasting Board of Governors* (AUD/IT-10-09, November 2009), BBG did not complete the development of procedures and guidance to govern routine and critical configuration

[7] DHS FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics.

management processes during Fiscal Year 2012, although BBG was in the process of gathering system information for the development of its standard baseline configurations.

According to NIST SP 800-53, Revision 3, CM-1, "Configuration Management [CM] Policy and Procedures," the organization develops, disseminates, and periodically reviews and updates:

> a. A formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
>
> b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

BBG's IT management stated that a lack of human resources hindered their ability to complete the implementation of the security standards and procedures. BBG's IT management further stated that systems were being retired in an effort to improve standardization.

Without detailed procedures and guidance to govern the performance of routine and critical configuration management processes, BBG may not be able to effectively secure its systems, which may lead to the introduction of security weaknesses and inconsistent performance.

> **Recommendation 1.** We recommend that the Chief Information Officer ensure that security configuration standards and procedures are completed, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.
>
> **Management Comments:** BBG concurred with the recommendation, stating that it had "created and filled a Change Manager Position within TSI's IT Directorate to address configuration standards and procedures." BBG further stated that through the Change Manager's efforts, "TSI is adopting change management policy and processes consistent with Information Technology Information Library standards" and that TSI has acquired Microsoft's System Center Configuration Manager (MS SCCM) for configuration management of agency servers and workstations." According to BBG, configuration planning for the MS SCCM implementation is underway; "full production system utilization" is expected by March 31, 2013; and the CIO will oversee testing of MS SCCM and the development of associated processes."
>
> **OIG Analysis:** OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and approved documentation showing security configuration standards and procedures have been developed and implemented.

Finding B. Chief Information Officer Lacks Compliance Enforcement Authority

Although BBG's IT Department provided services and guidelines to the Office of Cuba Broadcasting (OCB), BBG's CIO did not have the authority to enforce security requirements at OCB or enact consequences for noncompliance. Instead, OCB maintained responsibility for the configuration of its systems and the assignment of access to its systems. As a result, BBG had no assurance that OCB's systems that connected to the BBG network were configured with adequate preventative and detective safeguards.

According to NIST SP 800-53, Revision 3, PM-1, "Information Security Program Plan," the organization:

> Develops and disseminates an organization-wide information security program plan that provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.

NIST SP 800-53, Revision 3, PM-2, "Senior Information Security Officer," further states that "the organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program."

OCB, which directs the operations of Radio and TV Martí, reports directly to the BBG Board of Governors and not to BBG's CIO. Although BBG's IT Department provided services to OCB, as mandated by the Board of Governors, BBG's CIO cannot enforce its security requirements because of this reporting structure.

Without the authority to enforce BBG's security policies and procedures for all systems that access the BBG network, BBG's CIO cannot ensure that security controls are properly managed and maintained. As a result, systems may operate in the production environment without appropriate controls or management oversight, exposing BBG's network and systems to additional risks and vulnerabilities.

> **Recommendation 2.** We recommend that the Broadcasting Board of Governors develop and implement policies to require all agency entities with systems that connect to the Broadcasting Board of Governors network to abide by the security policies and requirements established by the Broadcasting Board of Governors Information Technology Department and grant the Chief Information Officer the necessary authority to enforce consequences for noncompliance.
>
> **Management Comments:** BBG concurred with the recommendation, stating that the CIO "will attempt to strengthen the IT security controls over all Federal BBG elements," which include the International Broadcasting Bureau, OCB, and the Voice of America,

which connect to the BBG's Wide Area Network (WAN). BBG further stated that "compensating controls will be put in place to ensure an acceptable risk level" for BBG "[i]f full compliance cannot be met" and that the CIO "will continue to assess progress."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed pending OIG's review and approval of documentation showing that BBG's policies and procedures require all agency entities with systems that connect to the Broadcasting Board of Governors network to abide by the security policies and requirements.

Finding C. User Account Management Controls Need Improvement

As first identified during the FY 2010 review,[8] BBG's user account management controls did not ensure that access was provided to authorized personnel only. Although BBG had implemented new user account management controls in FY 2012, including policies and procedures restricting the use of guest, test, and shared user accounts, we observed the following account management control deficiencies: Of 3,551 "active" user accounts in AD, 93 accounts were not accessed for more than 90 days, 31 accounts did not require the use of a password, and passwords for 411 accounts were not changed for over 90 days.

BBG policy[9] requires system owners to implement the policy and procedures for managing access to IT systems, including creating, deleting, and monitoring user accounts and establishing processes to disable user accounts that have been inactive for 45 days or more. In respect to password management, BBG policy[10] for all information systems and information system components requires passwords to be constructed according to set length and complexity requirements and requires passwords to be changed every 90 days.

BBG management stated that its previous use of older technology had prevented BBG from segmenting its users, effectively requiring manual intervention to process exceptions to its stated policies. Exceptions to the stated policies were granted for user accounts that did not routinely log in to the network. BBG management also stated that some user accounts were improperly configured during the migration to Microsoft Office 365.[11]

Without more stringent user account management controls, the risk of unauthorized use of user accounts and thus unauthorized access to systems, increases significantly. Unauthorized access to systems may result in the submission of false transactions, improper access to and dissemination of confidential data, and other malicious activities.

[8] AUD/IT-10-09, Nov. 2009.

[9] Identification and Authentication Policy, Apr. 1, 2011, revised Mar. 27, 2012.

[10] BBG/IBB/VOA Password Policy, Feb. 1, 2011.

[11] Microsoft Office 365, a hosted service provided by Microsoft, offers virtual access to Microsoft solutions, such as email, calendars, Web-based applications, instant messaging, conferencing, and file sharing.

Recommendation 3. We recommend that the Chief Information Officer ensure that user accounts are properly configured and maintained in accordance with the Broadcasting Board of Governors policies. If the Broadcasting Board of Governors determines that exceptions to the implemented policies may be necessary, the Broadcasting Board of Governors should identify, assess, and document the associated risks. If the Broadcasting Board of Governors further determines that the identified risks are acceptable, the exceptions should be documented and approved by information technology management.

Management Comments: BBG concurred with the recommendation, stating that the CIO "will review and strengthen IT processes that manage user accounts" and that it "strongly believes that the "account irregularities" OIG observed during the audit "resulted from temporary transition issues caused by migration of agency mail accounts and VPN [virtual private network] token vendors." BBG stated that it expected the recommendation to be complied with by January 31, 2013."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed with OIG reviews and approved documentation showing that a process has been implemented to properly configure and maintain user accounts, including the disabling of user accounts that are no longer needed.

Finding D. Security Incidents Are Not Timely Reported to the United States Computer Emergency Readiness Team

One of two security incidents that BBG identified and reported to US-CERT at DHS was not reported in accordance with US-CERT's reporting requirements. The incident, which pertained to the identification of malicious code, was not reported within one business day, as required by US-CERT. Rather, BBG reported the incident three business days after it was identified.

The US-CERT Federal Incident Reporting Guidelines and NIST SP 800-61, Revision 1,[12] require the following information:

Category	Name	Description	Reporting Time Frame
CAT 3	Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.

[12] NIST SP 800-61, Rev. 1, "Computer Security Incident Handling Guide," Mar. 2008.

Further, BBG policy[13] requires BBG's Computer Security Incident Response Team to categorize and report security incidents in accordance with US-CERT and NIST SP 800-61.[14]

Although the security incident had been properly recorded in BBG's incident tracking system, reporting to US-CERT was delayed as BBG conducted its assessment. BBG's IT management stated that they were focused on identifying the cause of the problem and subsequently remediating the identified weakness, which delayed reporting.

Without timely reporting of security incidents to US-CERT, BBG may adversely impact US-CERT's ability to improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks.

Recommendation 4. We recommend that the Chief Information Officer ensure that procedures as stated within the Broadcasting Board of Governors Computer Security Incident Management Policy are followed to ensure that security incidents are properly reported, as required by the United States Computer Emergency Readiness Team's Federal Incident Reporting Guidelines.

Management Comments: BBG concurred with the recommendation, stating that the CIO "has taken steps to implement this policy immediately."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed pending OIG review and approval of documentation showing that security incidents are properly reported as required.

Finding E. Compliance With Security Awareness Training Program Is Not Strictly Enforced

As first reported in the FY 2010 review,[15] BBG did not sanction employees and contractors who had not completed the annual security awareness training course. Specifically, less than 25 percent of BBG personnel completed security awareness training in FY 2011. At the completion of our onsite verification in July 2012, BBG had just started its annual security awareness training program to include both online and in-person training. Although 3 months remained in the fiscal year during which BBG personnel could complete the training, consequences for noncompliance had not been implemented.

OMB Memorandum M-12-20, "FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," Oct. 2, 2012, requires "all employees to receive annual security and privacy awareness training, and they must be included as part of [an] agency's training totals."

[13] Computer Security Incident Management Policy, May 16, 2011, revised Jan. 11, 2012.
[14] NIST SP 800-61, Rev. 1, "Computer Security Incident Handling Guide," Mar. 2008.
[15] AUD/IT-10-09, Nov. 2009.

Regarding compliance with policies and procedures, NIST SP 800-53, Revision 3, Personnel Sanctions (PS-8), states, "The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures."

BBG's IT management stated that compliance with the security awareness training policy had not been implemented because of concerns about possible disruption of BBG's mission and employees' job responsibilities if user access was restricted. BBG's IT management further stated that in-person training presentations had been developed to increase compliance.

Without the completion of initial and annual security awareness training, personnel may be unaware of new risks that may compromise the confidentiality, integrity, and availability of information. As a result, personnel may be unable to recognize and respond appropriately to real and potential security threats.

Recommendation 5. We recommend that the Chief Information Officer develop and implement a formal sanction process for personnel who do not successfully complete the security awareness training, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Management Comments: BBG concurred with the recommendation, stating that the CIO and BBG's leadership team "have taken steps to implement strict discipline measures effective this year with the current cycle of the IT security awareness training." BBG further stated that on the security awareness training deadline (October 31, 2012), TSI's IT Directorate notified BBG users and their direct supervisors that IT was "prepared to disable their computer accounts" if the employees did not complete the required training by November 2, 2012. BBG stated that the extension was provided because of "potential hardships" caused by Hurricane Sandy. BBG stated its compliance rate of 92 percent versus its 2011 rate of 25 percent and stated that "senior management has been apprised of the email message sent to impacted employees."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed pending OIG review and approval of the revised security awareness training policy showing the enforcement actions to be taken for noncompliant personnel.

Finding F. Plans of Action and Milestones Are Not Properly Completed

Although BBG implemented revisions to its POA&M program, the completed POA&Ms did not consistently provide sufficient detail, such as the resources required to address the security weaknesses, milestones used to measure progress toward completion, and changes to the milestones when corrective actions were not completed or were past due.

OMB Memorandum M-12-20[16] states, "While agencies are no longer required to follow the exact format prescribed in the POA&M examples in OMB Memorandum 04-25, they must still include all of the associated data elements in their POA&Ms."

Regarding the data elements required in the POA&M, OMB Memorandum M-04-25[17] states that the following information must be included:

- Severity and brief description of the weakness.
- Identity of the office or organization responsible for resolving the weakness.
- Estimated funding and personnel required to resolve the weakness.
- Scheduled completion date for resolving the weakness.
- Key milestones with completion dates.
- Changes to milestones, including new completion dates for the changed milestone.
- The source of the weakness (for example, program review, OIG audit, or GAO audit).
- Status (for example, ongoing or completed).

Further, BBG policy[18] requires BBG's PO&AMs to include the data elements stated in OMB Memorandum M-02-01.[19]

BBG's IT management stated that the development of its POA&M program was a "work in progress" and that the POA&M program had not included "such granular project management" because of the relatively small number of personnel involved in the remediation efforts, as well as the frequent meetings held among the responsible personnel.

Without a robust POA&M program that includes sufficient details for managing and tracking corrective actions, BBG's IT management may be unable to properly assess the statuses of corrective activities. As a result, BBG may encounter delays in the implementation of corrective actions, preventing security issues from being resolved in a timely manner. Additionally, IT management may be unable to properly assess and prioritize the resources required to implement corrective actions.

Recommendation 6. We recommend the Chief Information Officer ensure that the Broadcasting Board of Governors Plans of Action and Milestones program is developed in accordance with its policy, which requires the Broadcasting Board of Governors Plans of Action and Milestones to include the data elements found in Office of Management and Budget Memorandum M-02-01.

Management Comments: BBG concurred with the recommendation, stating, "The CIO will expand on the data elements contained in the POA&M tracking sheet as efforts

[16] OMB Memorandum M-12-20, Oct. 2, 2012.
[17] OMB Memorandum M-04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," Aug. 23, 2004.
[18] Information Security Plan of Action and Milestones (POA&M) Policy, May 12, 2010, revised Feb. 9, 2012.
[19] OMB Memorandum M-02-01, Oct. 17, 2001.

continue to mature internal IT project governance." BBG further stated that this improvement will be reflected on "the March 2013 quarterly cycle of POA&M tracking sheets."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed pending OIG review and approval of documentation showing that POA&Ms are being reviewed and updated periodically and that they include the data elements required by BBG policy.

Finding G. Remote Access to the Network Is Not Properly Managed and Controlled

As first identified during the FY 2010 review,[20] BBG's remote access policy allowed users to access the BBG network from personally owned computers using software provided by BBG. However, BBG had not implemented procedures to ensure that remote access was granted only to computers that had proper security safeguards.

NIST SP 800-53, Revision 3, AC-17, "Remote Access," states the following:

Control: The organization:

a. Documents allowed methods of remote access to the information system;
b. Establishes usage restrictions and implementation guidance for each allowed remote access method;
c. Monitors for unauthorized remote access to the information system;
d. Authorizes remote access to the information system prior to connection; and
e. Enforces requirements for remote connections to the information system.

BBG's IT management stated that a process had been drafted and a software tool had been identified that will detect and scan the security settings of computers attempting to access the BBG network remotely and deny requests from computers with improper safeguards. However, BBG IT management stated that the tool had not been implemented because of ongoing changes to the remote access process, as well as the need to direct available resources to other IT projects.

Without proper policies and procedures that require the use of properly secured third-party devices, BBG network and systems may be susceptible to the introduction of viruses, worms, or other malicious code by such third-party devices.

Recommendation 7. We recommend that the Chief Information Officer implement procedures to assess the adequacy of the security configurations of third-party devices that request access to the Broadcasting Board of Governors network and grant access

[20] AUD/IT-10-09, Nov. 2009.

only to properly configured devices, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Management Comments: BBG concurred with the recommendation, stating that the CIO would "develop the process and initiate planning and testing of the tool procured to assess the adequacy of the security configurations of third-party devices that request access (generally through a Virtual Private Network [VPN]) to the BBG network." BBG further stated that access will be granted only to those devices whose configurations are deemed sufficient by March 31, 2013."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed pending OIG review and approval of documentation showing that BBG has implemented the process to assess the adequacy of the security configurations of third-party devices as described.

Finding H. System Inventory Management Process Needs To Be Implemented

As first identified during the FY 2010 review,[21] BBG did not implement a process or procedures to manage and routinely update its inventory of IT assets at least annually or when changes were made to its systems. Although BBG had implemented a tool to record its system inventory, the corresponding process and procedures for developing and maintaining the system inventory had not been implemented.

FISMA requires the heads of each agency to develop and maintain an inventory of major information systems, including major national security systems, operated by or under the agency's control and to identify information systems in an inventory, including identifying the interfaces between each system and all other systems or networks and those not operated by or under the control of the agency. FISMA further requires the inventory to be updated at least annually, to be made available to the Comptroller General, and to be used to support information resources management. Additionally, NIST SP 800-53, Revision 3, CM-8, "Information System Component Inventory," requires the following:

> Control: The organization develops, documents, and maintains an inventory of information system components that:
>
> a. Accurately reflects the current information system;
> b. Is consistent with the authorization boundary of the information system;
> c. Is at the level of granularity deemed necessary for tracking and reporting;
> d. Includes [*Assignment: organization-defined information deemed necessary to achieve effective property accountability*]; and
> e. Is available for review and audit by designated organizational officials.

[21] AUD/IT-10-09, Nov. 2009.

BBG's IT management stated that the process and procedures for developing and maintaining the system inventory had not been completed because of a lack of standards for the system inventory's information requirements. The lack of standards resulted in a great deal of variety with the information that had been collected and supplied by system owners, for example, licensing information and planned retirement dates.

Without a process to identify, document, and maintain an inventory of major and minor applications, as well as general support systems, BBG may not have an accurate accounting of its IT assets and the related system interfaces and underlying support systems. An inaccurate or incomplete asset inventory may also prohibit BBG from effectively implementing its continuous monitoring program and practices, including performing vulnerability scans of its assets. Additionally, critical management processes such as strategic planning, budgeting, system administration, and resource management may be adversely affected.

Recommendation 8. We recommend that the Chief Information Officer ensure that the Information Technology Director create and implement a standardized process to collect information used to develop and subsequently update the Broadcasting Board of Governors system inventory and update the general support system's security plan control for CM-8, "Information System Component Inventory," specifically, the organizationally defined frequency of inventory assessments, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Management Comments: BBG concurred with the recommendation, stating that it had acquired an inventory management software tool and was establishing internal tracking processes. BBG further stated that although "significant progress has been made," full implementation was not expected until March 31, 2013, and that the CIO would "continue to oversee this effort."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed pending OIG review and approval of documentation showing that BBG has implemented a system inventory process, including standards for collecting information used to develop and subsequently update BBG's system inventory.

Finding I. Enterprise-Wide and System-Specific Contingency Plans Do Not Exist

As first identified during the FY 2010 review,[22] BBG did not develop and implement contingency planning and testing policies and procedures compliant with OMB and NIST requirements contained in NIST SP 800 34.[23] Specifically, BBG did not complete its enterprise-wide and system-specific contingency plans or conduct contingency tests.

[22] AUD/IT-10-09, Nov. 2009.

[23] NIST SP 800-34, Rev. 1, "Contingency Planning Guide for Federal Information Systems," May 2010 (last updated Nov. 11, 2010).

NIST SP 800-34, Revision 1,[24] states that information systems are "vital elements" in most business functions and that "it is critical" that the services provided by these systems be able to operate effectively without excessive interruption. The NIST guidance[25] further states, "Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption."

BBG's IT management stated that although a strategic plan had been developed to address BBG's contingency and business resumption needs, resources had not been appropriated for the development of such policies, procedures, and the related contingency plans because of ongoing changes to the system architecture and other competing priorities.

Without an effective contingency plan, which includes periodic testing of the plan's reliability, BBG may be unable to access critical information and resources and to perform mission-critical business functions in the event of an extended outage and/or disaster. As a result, BBG may be unable to resume operations in an efficient and effective manner should such an incident occur.

Recommendation 9. We recommend that the Chief Information Officer ensure that the Director of Disaster Recovery and Business Continuity develop and implement contingency planning policies and procedures, develop contingency plans for the Broadcasting Board of Governors infrastructure (network) and its major systems, provide contingency planning training to personnel who are responsible for the recovery of the network and systems, perform periodic testing of the Broadcasting Board of Governors contingency plans, and update the plan based on lessons learned as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.

Management Comments: BBG concurred with the recommendation, stating that it "agrees to further develop contingency plans and increase investments in offsite systems to be used for business continuity". BBG further stated that "[t]o support and lead this effort, the CIO is attempting to fill a Disaster Recovery and Business Continuity Manager position. "If full compliance cannot be met," according to BBG, "compensating controls will be put in place to ensure an acceptable risk level for BBG" and the CIO "will continue to assess progress."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed pending OIG review and approval of documentation showing the development of contingency planning policies and procedures that include training requirements for personnel responsible for the recovery of the network and systems and contingency plans for the BBG infrastructure and its major systems.

[24] Ibid., p. 1.
[25] Ibid., p. 1.

List of Current Year Recommendations

Recommendation 1. We recommend that the Chief Information Officer ensure that security configuration standards and procedures are completed, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Recommendation 2. We recommend that the Broadcasting Board of Governors develop and implement policies to require all agency entities with systems that connect to the Broadcasting Board of Governors network to abide by the security policies and requirements established by the Broadcasting Board of Governors Information Technology Department and grant the Chief Information Officer the necessary authority to enforce consequences for noncompliance.

Recommendation 3. We recommend that the Chief Information Officer ensure that user accounts are properly configured and maintained in accordance with the Broadcasting Board of Governors policies. If the Broadcasting Board of Governors determines that exceptions to the implemented policies may be necessary, the Broadcasting Board of Governors should identify, assess, and document the associated risks. If the Broadcasting Board of Governors further determines that the identified risks are acceptable, the exceptions should be documented and approved by information technology management.

Recommendation 4. We recommend that the Chief Information Officer ensure that procedures as stated within the Broadcasting Board of Governors Computer Security Incident Management Policy are followed to ensure that security incidents are properly reported, as required by the United States Computer Emergency Readiness Team's Federal Incident Reporting Guidelines.

Recommendation 5. We recommend that the Chief Information Officer develop and implement a formal sanction process for personnel who do not successfully complete the security awareness training, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Recommendation 6. We recommend the Chief Information Officer ensure that the Broadcasting Board of Governors Plans of Action and Milestones program is developed in accordance with its policy, which requires the Broadcasting Board of Governors Plans of Action and Milestones to include the data elements found in Office of Management and Budget Memorandum M-02-01.

Recommendation 7. We recommend that the Chief Information Officer implement procedures to assess the adequacy of the security configurations of third-party devices that request access to the Broadcasting Board of Governors network and grant access only to properly configured devices, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Recommendation 8. We recommend that the Chief Information Officer ensure that the Information Technology Director create and implement a standardized process to collect information used to develop and subsequently update the Broadcasting Board of Governors system inventory and update the general support system's security plan control for CM-8,

"Information System Component Inventory," specifically, the organizationally defined frequency of inventory assessments, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Recommendation 9. We recommend that the Chief Information Officer ensure that the Director of Disaster Recovery and Business Continuity develop and implement contingency planning policies and procedures, develop contingency plans for the Broadcasting Board of Governors infrastructure (network) and its major systems, provide contingency planning training to personnel who are responsible for the recovery of the network and systems, perform periodic testing of the Broadcasting Board of Governors contingency plans, and update the plan based on lessons learned as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.

Appendix A

Scope and Methodology

In order to fulfill its responsibilities related to the Federal Information Security Management Act of 2002 (FISMA),[1] the Office of Inspector General (OIG), Office of Audits, contracted with Williams, Adley & Company, LLP (referred to as "we" in this appendix), an independent public accountant, to evaluate the Broadcasting Board of Governors (BBG) information security program and practices to determine the effectiveness of such programs and practices for FY 2012. The OIG and Williams, Adley & Company-DC, LLP, held an exit conference with BBG management on November 7, 2012.

FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor or another source. To ensure the adequacy and effectiveness of these controls, FISMA requires the agency inspector general or an independent external auditor to perform annual reviews of the information security program and to report those results to the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). DHS uses this data to assist in oversight responsibilities and to prepare its annual report to Congress regarding agency compliance with FISMA.

We conducted the audit from April through September 2012. In addition, we performed the audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), FISMA, OMB, and National Institute of Standards and Technology Special Publication (NIST SP) guidance. GAGAS requires that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We used the following laws, regulations, and policies to evaluate the adequacy of the controls in place at BBG:

- DHS Inspector General FISMA Reporting Metrics.[2]
- OMB Memoranda M-02-01, M-04-04, M-06-19, and M-12-20.[3]

[1] Pub. L. No. 107-347, tit. III, 116 Stat. 2946, (2002).

[2] DHS FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics, dated Mar. 6, 2012.

[3] OMB Memorandum M-02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones, Oct. 17, 2001; OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," Dec. 16, 2003; OMB Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," July 12, 2006; and OMB Memorandum M-12-20, "FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," Oct. 2, 2012.

- BBG policies and procedures, such as the BBG Computer Security Incident Management Policy.
- Federal laws, regulations, and standards, such as FISMA and those contained in OMB Circular No. A-130, Revised,[4] and OMB Circular No. A-11.[5]
- NIST SPs, Federal Information Systems Processing Publications (FIPS), other applicable NIST publications, and industry best practices.

During our audit, we assessed BBG's information security program policies, procedures, and processes in the following areas:

- Continuous monitoring management
- Configuration management
- Identity and access management
- Incident response and reporting
- Risk management
- Security training
- Plans of action and milestones
- Remote access management
- Contingency planning
- Contractor systems
- Security capital planning

The audit covered the period October 1, 2011, to September 30, 2012. During the fieldwork, we took the following actions:

- Determined the extent to which the BBG's information security plans, programs, and practices complied with FISMA requirements; applicable Federal laws, regulations, and standards; relevant OMB Circular No. A-130, revised; processes and reporting requirements included in Appendix III; and NIST and FIPS requirements.
- Reviewed relevant security programs and practices to report on the effectiveness of BBG's agency-wide information security program in accordance with OMB's annual FISMA reporting instructions. The audit approach addressed the DHS FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics, dated March 6, 2012.
- Assessed programs for monitoring of security policy and program compliance and responding to security events, for example, unauthorized changes detected by intrusion detection systems.
- Performed testing of major systems at the discretion of OIG.

[4] OMB Circular No. A-130, rev., "Management of Federal Information Resources," app. III, "Security of Federal Automated Information Resources," Nov. 30, 2000.

[5] OMB Circular No. A-11, "Preparation, Submission, and Execution of the Budget," Aug. 2011.

- Assessed the adequacy of internal controls related to the areas reviewed. Control deficiencies identified during the review are included in this report.
- Evaluated BBG's remedial actions taken to address the previously reported information security program control weaknesses identified in OIG's *Evaluation of the Information Security Program at the Broadcasting Board of Governors* (AUD/IT/IB-12-15, November 2011).

Review of Internal Controls

We reviewed BBG's internal controls to determine whether

- The organization has established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- The agency has established and is maintaining a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- The agency has established and is maintaining an account and identity management program that is generally consistent with NIST and OMB FISMA requirements and identifies users and network devices.
- The agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- The organization has established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- The agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- The agency has established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and that tracks and monitors known information security weaknesses.
- The agency has established and is maintaining a remote access program that is generally consistent with NIST and OMB FISMA requirements.
- The agency established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST and OMB FISMA requirements.
- The organization has established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization.
- The agency has established and maintains a capital planning and investment program for information security.

Use of Computer-Processed Data

During the audit, we utilized computer-processed data to obtain samples and information regarding the existence of information security controls. Specifically, we obtained data extracted from Microsoft's Windows Active Directory and BBG's human resources system to test user account management controls. We assessed the reliability of computer-generated data primarily by comparing selected data with source documents. We determined that the information was reliable for assessing the adequacy of related information security controls.

Appendix B

Followup of Recommendations From the FY 2011 Evaluation of the Broadcasting Board of Governors Information Security Program

The audit team reviewed actions implemented by management to mitigate the findings identified in the FY 2011 evaluation of BBG's Information Security Program. The current status of each of the recommendations follows:

Recommendation 1. We recommend that the Chief Information Officer ensure that the selected system inventory management software tool is acquired and implemented and a process is developed to update, not less than annually, the Broadcasting Board of Governors' (BBG) system inventory when changes are made to those information systems operated by or under the control of BBG or by third-party contractors or agencies on behalf of BBG, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Status: Closed from FY 2011 report; this repeat recommendation has become Recommendation 8 (Finding H) in the FY 2012 report.

Recommendation 2. We recommend that the Chief Information Officer complete the development and implementation of security configuration procedures and periodically assess compliance with the implemented procedures, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Status: Closed from FY 2011 report; this repeat recommendation has become Recommendation 1 (Finding A) in the FY 2012 report.

Recommendation 3. We recommend that the Chief Information Officer develop procedures to ensure that security controls are properly managed and maintained for all systems that access the Broadcasting Board of Governors network as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Status: Closed from FY 2011 report; this repeat recommendation has become Recommendation 2 (Finding B) in the FY 2012 report.

Recommendation 4. We recommend that the Chief Information Officer update the security awareness training policy requiring all new personnel to attend initial and refresher security awareness training and enforce consequences of noncompliance for personnel who do not successfully complete the security awareness training, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3, and the Broadcasting Board of Governors information security policies.

Status: Closed from FY 2011 report; this repeat recommendation has become Recommendation 5 (Finding E) in the FY 2012 report.

Recommendation 5. We recommend the Chief Information Officer develop a policy requiring responsible managers to review and update Plans of Action and Milestones and assess the timeliness of corrective actions to determine whether additional resources may need to be allocated to prevent delays, as required by the Office of Management and Budget Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, September 14, 2011.

Status: Closed. The Plans of Action and Milestones (POA&M) policy was revised in February 2012 to require system owners to review progress toward remediating security weaknesses identified in their systems and updating the POA&M accordingly. We observed minutes from meetings reviewing the statuses of correction actions, the status reports provided by system owners, and the corresponding POA&Ms.

Recommendation 6. We recommend that the Chief Information Officer implement the process and software tool to assess the adequacy of the security configurations of third-party devices that request access to the Broadcasting Board of Governors network and grant access only to properly configured devices, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Status: Closed from FY 2011 report; this repeat recommendation has become Recommendation 7 (Finding G) in the FY 2012 report.

Recommendation 7. We recommend that the Chief Information Officer establish policies and procedures to restrict the use of guest, test, and shared user accounts to ensure user accountability in accordance with the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Status: Closed. We observed that policies and procedures had been updated in March 2012 to limit and manage the use of guest, test, and shared user accounts. We also reviewed a sample of the quarterly reports detailing the required existence of guest, test, and shared user accounts.

Recommendation 8. We recommend that the Chief Information Officer establish policies and procedures requiring system owners to notify account managers when information system users are terminated, transferred, or information system usage or need-to know/need-to-share changes are made, in accordance with the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Status: Closed from FY 2011 report; this repeat recommendation has become Recommendation 3 (Finding C) in the FY 2012 report.

Recommendation 9. We recommend that the Chief Information Officer implement procedures to monitor and review compliance with the password reset procedures to ensure that Help Desk personnel enforce the password reset policy, which requires the requesting user to be physically present to allow Help Desk personnel to verify the user's identity.

Status: Closed. The password reset procedures were refined to include user identification measures, and training was provided to Help Desk personnel in May 2012. During our testing of the procedures, we requested a password reset. No exceptions were noted.

Recommendation 10. We recommend that the Chief Information Officer develop and implement policies and procedures to perform routine vulnerability assessments for all major systems and general support systems, as required by the National Institute of Standards and Technology Special Publication 800-53A.

Status: Closed. We observed that policies and procedures had been implemented in February 2012 to perform monthly vulnerability assessments for all major systems and general support systems. Additionally, we requested and inspected a sample of the monthly vulnerability assessment reports.

Recommendation 11. We recommend that the Chief Information Officer ensure that the Director of Disaster Recovery and Business Continuity develop and implement contingency planning policies and procedures; develop contingency plans for the Broadcasting Board of Governors (BBG) infrastructure (network) and its major systems; provide contingency planning training to personnel who are responsible for the recovery of the network and systems; perform periodic testing of BBG's contingency plans; and update the plan based on lessons learned, as required by the National Institute of Standards and Technology Special Publication 800-34, Revision 1.

Status: Closed from FY 2011 report; this repeat recommendation has become Recommendation 9 (Finding I) in the FY 2012 report.

Recommendation 12. We recommend that the Chief Information Officer develop and implement a complete and comprehensive process that meets United States-Computer Emergency Readiness Team's (US-CERT) requirements for identifying, reporting, and resolving computer security incidents in a timely manner, as required by the National Institute of Standards and Technology Special Publication 800-61, Revision 1, and Office of Management and Budget Memorandum M-07-16. Also, BBG's Computer Security Incident Management Policy should be revised to include clear and comprehensive guidance for the identification, prioritization, and notification of security incidents, both internally and to US-CERT. The security incident identification and notification procedures should also specifically address the procedures for responding to security incidents involving the breach of personally identifiable information whether in electronic or paper format.

Status: Closed. We observed that the incident response policy had been revised in January 2012 to include the US-CERT requirements for identifying, reporting, and resolving computer security incidents, inclusive of security incidents involving the breach of personally identifiable information.

Appendix C

Broadcasting Board of Governors Response

Broadcasting Board of Governors
INTERNATIONAL BROADCASTING BUREAU

NOV - 6 2012

Mr. Harold W. Geisel
Deputy Inspector General
Department of State

Dear Mr. Geisel:

This is in response to the e-mail from Ms. Amy Conigliaro, dated October 22, 2012, regarding the Office of Inspector General (OIG) draft report titled, "Audit of the Broadcasting Board of Governors Information Security Program," Report Number AUD-IT-XX-XX, issued October 2012.

The Broadcasting Board of Governors (BBG) has reviewed the report and provides its comments to address Recommendations 1 through 9 as noted on the enclosure.

We thank you for the opportunity to respond to the report. If you have any questions, please feel free to contact Ms. Barbara Tripp at (202) 203-4609 or Ms. Kelu Chao, Director, IBB Office of Performance Review at (202) 203-4800.

Sincerely,

for Richard M. Lobo
Director

Enclosure: As Stated

330 Independence Avenue, SW Washington, DC 20237

Enclosure

BBG's Response to ●IG's Draft Report
"Audit of the Broadcasting Board of Governors Information Security Program,"
Report Number AUD-IT-XX-XX, Issued October 2012

BBG Comments:

The Broadcasting Board of Governors (BBG) believes significant progress has been made over the past year in complying with FISMA requirements. In light of that progress, the BBG requests that the ●IG consider adding the following bullet points to the management control improvements listed on page one of the Executive Summary as follows:

- Installed and configured an inventory management tool.
- Developed and implemented policies and procedures for Plans of Action and Milestones (P●A&M).
- Ensured adherence to password reset policies and procedures.
- Revised the BBG Incident Response Policy to align with guidance from the National Institute of Standards and Technology (NIST).

Recommendation 1: We recommend that the Chief Information ●fficer ensure that security configuration standards and procedures are completed, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

BBG Response (October 31, 2012): BBG concurs. The BBG has created and filled a Change Manager Position within TSI's IT Directorate to address configuration standards and procedures. Through his efforts, TSI is adopting change management policy and processes consistent with Information Technology Information Library standards. Additionally, TSI has acquired Microsoft's System Center Configuration Manager (MS SCCM) for configuration management of agency servers and workstations. Configuration planning for the MS SCCM implementation is currently underway with full production system utilization expected by March 31, 2013. The CI● will oversee testing of this tool and the development of associated processes.

Recommendation 2: We recommend that the Broadcasting Board of Governors develop and implement policies to require all agency entities with systems that connect to the Broadcasting Board of Governors network to abide by the security policies and requirements established by the Broadcasting Board of Governors Information Technology Department and grant the Chief Information Officer the necessary authority to enforce consequences for noncompliance.

BBG Response (October 31, 2012): BBG concurs. The CI● will attempt to strengthen the IT security controls over all Federal BBG elements that connect to the BBG's Wide Area Network (WAN). These BBG Federal elements include the International Broadcasting Bureau, the Office of Cuba Broadcasting, and the Voice of America. If full compliance

cannot be met, compensating controls will be put in place to ensure an acceptable risk level for the BBG. The CIO will continue to assess progress.

Recommendation 3: We recommend that the Chief Information Officer ensure that user accounts are properly configured and maintained in accordance with the Broadcasting Board of Governors policies. If the Broadcasting Board of Governors determines that exceptions to the implemented policies may be necessary, the Broadcasting Board of Governors should identify, assess, and document the associated risks. If the Broadcasting Board of Governors further determines that the identified risks are acceptable, the exceptions should be documented and approved by information technology management.

BBG Response (October 31, 2012): BBG concurs. The CIO will review and strengthen IT processes that manage user accounts. The BBG strongly believes that the account irregularities the OIG observed resulted from temporary transition issues caused by migration of agency mail accounts and VPN token vendors. The BBG expects to be in full compliance of this recommendation by January 31, 2013.

Recommendation 4: We recommend that the Chief Information Officer ensure that procedures, as stated within the Broadcasting Board of Governors Computer Security Incident Management Policy, are followed to ensure that security incidents are properly reported, as required by the United States Computer Emergency Readiness Team's Federal Incident Reporting Guidelines.

BBG Response (October 31, 2012): BBG concurs. The CIO has taken steps to implement this policy immediately.

Recommendation 5: We recommend that the Chief Information Officer develop and implement a formal sanction process for personnel who do not successfully complete the security awareness training, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

BBG Response (October 31, 2012): BBG concurs. The CIO and BBG's leadership team have taken steps to implement strict discipline measures effective this year with the current cycle of the IT security awareness training. On October 31, 2012, the security awareness training deadline, TSI's IT Directorate notified all BBG users and their direct supervisors that IT is prepared to disable their computer accounts if employees fail to complete the required training by November 2, 2012. The BBG provided the extension in light of potential hardships created by Hurricane Sandy. BBG's current compliance rate is 92% versus 25% in 2011.

Please also note that senior management has been apprised of the email message sent to impacted employees.

Recommendation 6: We recommend the Chief Information Officer ensure that the Broadcasting Board of Governors Plans of Actions and Milestones program is developed in accordance with its policy, which requires the Broadcasting Board of Governors Plans of Action

and Milestones to include the data elements found in Office of Management and Budget Memorandum M-02-01.

BBG Response (October 31, 2012): BBG concurs. The CIO will expand on the data elements contained in the POA&M tracking sheet as efforts continue to mature internal IT project governance. The March 2013 quarterly cycle of POA&M tracking sheets will reflect this improvement.

Recommendation 7: We recommend that the Chief Information Officer implement procedures to assess the adequacy of the security configurations of third-party devices that request access to the Broadcasting Board of Governors network and grant access only to properly configured devices, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

BBG Response (October 31, 2012): BBG concurs. The CIO will develop the process and initiate planning and testing of the tool procured to assess the adequacy of the security configurations of third-party devices that request access (generally through a Virtual Private Network [VPN]) to the BBG network. The CIO will grant access only to those whose configurations are deemed sufficient by March 31, 2013.

Recommendation 8: We recommend that the Chief Information Officer ensure that the Information Technology Director create and implement a standardized process to collect information used to develop and subsequently update the Broadcasting Board of Governors system inventory, and update the general support system's security plan control for Information System Component Inventory (CM-8), specifically the organizationally defined frequency of inventory assessments, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

BBG Response (October 31, 2012): BBG concurs. The BBG has acquired an inventory management software tool and is currently establishing internal tracking processes. Significant progress has been made, but full implementation is not expected until March 31, 2013. The CIO will continue to oversee this effort.

Recommendation 9: We recommend that the Chief Information Officer ensure that the Director of Disaster Recovery and Business Continuity develop and implement contingency planning policies and procedures, develop contingency plans for the Broadcasting Board of Governors infrastructure (network) and its major systems, provide contingency planning training to personnel who are responsible for the recovery of the network and systems, perform periodic testing of the Broadcasting Board of Governors contingency plans, and update the plan based on lessons learned, as required by the National Institute of Standards and Technology Special Publication 800-34, Revision 1.

BBG Response (October 31, 2012): BBG concurs. The BBG agrees to further develop contingency plans and increase investments in offsite systems to be used for business continuity. To support and lead this effort, the CIO is attempting to fill a Disaster Recovery and Business Continuity Manager position. If full compliance cannot be met,

compensating controls will be put in place to ensure an acceptable risk level for BBG. The CIO will continue to assess progress.

4