



Office of Inspector General

UNCLASSIFIED

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

Office of Audits

Evaluation of the Broadcasting Board of
Governors Information Security Program

Report Number AUD/IT/IB-12-15, November 2011

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.~~

UNCLASSIFIED



UNCLASSIFIED

United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

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 a review of the Broadcasting Board of Governors (BBG) Information Security Program for FY 2011. To perform this review, OIG contracted with the independent public accountant Williams, Adley & Company, LLP. The contract required that the independent public accountant perform its evaluation in accordance with guidance contained in the *Government Auditing Standards*, issued by the Comptroller General of the United States. The public accountant's report is included. The report is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

The independent public accountant identified areas in which improvements could be made, including system inventory, security configuration management, security awareness training, plans of action and milestones, remote access, user account management controls, vulnerability assessments, enterprise-wide and system-specific contingency plans, and incident response.

OIG evaluated the nature, extent, and timing of Williams, Adley & Company's work; monitored progress throughout the evaluation; reviewed Williams, Adley & Company's supporting documentation; evaluated key judgments; and performed other procedures as appropriate. OIG concurs with Williams, Adley & Company's findings, and the recommendations contained in the report were developed on the basis of the best knowledge available and were 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.

A handwritten signature in black ink, appearing to read "Harold W. Geisel".

Harold W. Geisel
Deputy Inspector General

UNCLASSIFIED



Evaluation of Broadcasting Board of Governors Information Security Program

November 7, 2011

Office of Inspector General
U.S. Department of State
2201 C St., NW
Washington, D.C. 20520

Williams, Adley & Company, LLP (referred to as “we” in this letter), is pleased to provide the Office of Inspector General (OIG) the results of the evaluation of the Broadcasting Board of Governors (BBG) Information Security Program for FY 2011. We evaluated BBG’s Information Security Program performance in compliance with the Federal Information Security Management Act, Office of Management and Budget (OMB), and National Institute of Standards and Technology regulations, standards, and requirements. Additionally, the evaluation was performed to provide sufficient support for OIG in providing responses to OMB in accordance with OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated September 14, 2011.

This evaluation, performed under Contract No. SAQMMA10F2159, was designed to meet the objectives identified in Appendix A, “Objectives, Scope, and Methodology,” of the report. We communicated the results of our review and the related findings and recommendations to BBG’s management.

We appreciate the cooperation provided by BBG personnel during the evaluation. Should you have any questions, or if we can be of further assistance, please contact either

(b) (6)

Williams Adley & Company, LLP

Acronyms

AD	Windows Active Directory
BBG	Broadcasting Board of Governors
CIO	Chief Information Officer
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
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
POA&M	Plan of Action and Milestones
PII	personally identifiable information
SP	Special Publication
US-CERT	United States Computer Emergency Response Team

Table of Contents

EXECUTIVE SUMMARY1

BACKGROUND4

RESULTS OF REVIEW5

**A. BBG HAS NOT IMPLEMENTED A SYSTEM INVENTORY MANAGEMENT
PROCESS5**

**B. SECURITY STANDARDS AND PROCEDURES HAVE NOT BEEN
IMPLEMENTED AND ENFORCED6**

**C. COMPLIANCE WITH BBG’S SECURITY AWARENESS TRAINING
PROGRAM WAS NOT STRICTLY ENFORCED8**

D. PLANS OF ACTION AND MILESTONES HAVE NOT BEEN COMPLETED9

**E. REMOTE ACCESS TO THE BBG NETWORK WAS NOT PROPERLY
MANAGED AND CONTROLLED10**

F. USER ACCOUNT MANAGEMENT CONTROLS NEED IMPROVEMENT11

G. VULNERABILITY ASSESSMENTS WERE NOT PERFORMED.....13

**H. ENTERPRISE-WIDE AND SYSTEM-SPECIFIC CONTINGENCY PLANS DO
NOT EXIST14**

**I. BBG’S INCIDENT RESPONSE POLICY DOES NOT ADHERE TO UNITED
STATES COMPUTER EMERGENCY READINESS TEAM’S REPORTING
REQUIREMENTS.....15**

LIST OF CURRENT YEAR RECOMMENDATIONS18

APPENDIX A. OBJECTIVES, SCOPE, AND METHODOLOGY20

**APPENDIX B. FOLLOWUP OF RECOMMENDATIONS FROM THE FY 2010 FISMA
REPORT.....23**

APPENDIX C. BROADCASTING BOARD OF GOVERNORS RESPONSE26

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 evaluation 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 OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated September 14, 2011.

We reviewed BBG’s remedial actions taken to address the FY 2010 reported Information Security Program control weaknesses identified in OIG’s FY 2010 report *Review of the Broadcasting Board of Governors Information Security Program* (AUD/IT/IB-11-08, November 2010). The statuses of the FY 2010 review recommendations are in Appendix B. Since FY 2010, BBG has taken the following steps to improve management controls:

- Completed security tests and evaluations and developed risk assessments and system security plans for its major systems.
- Implemented a more robust security incident response tracking process.
- Developed password management policies and procedures to reduce to the risk of unauthorized access.

Overall, we found that BBG had continued its efforts to further develop its information security program. However, to improve the information security program and to bring the program into compliance with FISMA, OMB, and NIST requirements, BBG needs to address the following control weaknesses:

A. System Inventory

BBG did not complete a system inventory of information technology (IT) assets and had not implemented a process to routinely update and manage its IT assets. Without a process to properly 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, the related system interfaces, and underlying support systems.

B. Security Configuration Management

BBG did not complete the development and implementation of its security configuration management standards and procedures for its IT environment. Furthermore, BBG’s standard operating procedures and information security practices were not enforced at the Office of Cuba Broadcasting (OCB). As a result,

¹ Public Law No. 107-347, Title III.

UNCLASSIFIED

BBG did not maintain control over OCB systems connected to its network. Additionally, OCB did not complete a security authorization process.

Without detailed procedures and guidance that 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. Additionally, BBG cannot be assured that security controls are properly managed and maintained for all systems that access the BBG network.

C. Security Awareness Training

BBG did not sanction employees and contractors who did not complete the annual security awareness training course. Although users were informed of the possibility of enforcement actions for not completing the course, no such actions were implemented. Additionally, contract personnel were not consistently required to complete BBG's security awareness training prior to, or shortly after, being granted access to BBG's network.

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.

D. Plans of Action and Milestones

BBG's Plans of Action and Milestones (POA&M) have not been implemented fully to track all identified weaknesses pertaining to BBG's major applications and general support systems. Furthermore, the POA&Ms did not provide sufficient details of the security weaknesses, planned actions, prioritizations of security weaknesses, resources required to address security weaknesses, and changes to milestones for actions completed.

Without periodic updates and reviews of the POA&Ms, BBG IT management may be unaware of the status of corrective actions. As a result, delays in the implementation of corrective actions may prevent security issues from being resolved in a timely manner. Additionally, IT management may be unable to properly assess and prioritize the resources that are required to implement corrective actions.

E. Remote Access

BBG's remote access policy allowed users to access the BBG network from personal computers using software provided by BBG. However, BBG did not have procedures in place to ensure that proper safeguards were implemented on non-BBG computers that were authorized to access the BBG network remotely.

UNCLASSIFIED

Without proper policies and procedures that require the use of properly secured devices, BBG may be unable to ensure the security of its data and network when allowing access to authorized third-party devices. As a result, the risks of introducing viruses, worms, and other malicious code increase significantly.

F. User Account Management Controls

Although BBG has implemented new user account management controls in FY 2011, such as user verification controls for password resets that required users to present photo identification in person prior to obtaining new passwords, the following account management control deficiencies continued in FY 2011:

- Guest, test, and shared user accounts that, when used, do not allow for individual accountability.
- Five of 94 employees who separated from BBG in FY 2011 between October 1, 2010, and June 8, 2011, retained “active” Windows Active Directory² (AD) user accounts as of June 14, 2011.
- One hundred nineteen active user accounts in AD have never been used, and 27 of the 119 user accounts were created before 2009.
- Seventy-six active user accounts in AD have not been used for over 90 days, and 24 of the 76 active user accounts have not been used since 2009 or before that year.
- An individual requested and was provided a new password via a telephone call.

Without more stringent user account management controls, the risk of unauthorized use of user accounts and thus unauthorized access to systems increase 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.

G. Vulnerability Assessments

BBG did not perform routine vulnerability assessments of its major systems and network environment using the framework outlined in NIST Special Publication (SP) 800-53A,³ *Guide for Assessing the Security Controls in Federal Information Systems*. Although BBG performed ad hoc scans of its systems and the general support system, BBG has not expanded the process to include the periodic re-performance of vulnerability assessments for all major systems or the routine performance of such scans on its enterprise network. Without periodic reviews or the performance of risk-based vulnerability assessments, new threats and vulnerabilities may not be identified and mitigated in a timely manner.

² 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.

³ NIST SP 800-53A, *Guide for Assessing Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*, July 2008.

H. Enterprise-Wide and System-Specific Contingency Plans

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, Revision 1,⁴ *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, which includes periodic testing of the plan's reliability, 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 a disaster.

I. Incident Response

BBG's Computer Security Incident Management Policy does not comply fully with the requirements established by the United States Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security (DHS). BBG's policy requires category one (CAT 1) incidents to be reported to US-CERT within 2 hours of detection, but US-CERT stipulates that CAT 1 incidents be reported within 1 hour of discovery/detection. Further, BBG's policy does not include reporting requirements for incidents of compromised personally identifiable information (PII). The US-CERT reporting timeframe for incidents that involve compromised PII is within 1 hour of detection regardless of the incident's category reporting timeframe. Without an effective incident response capability, BBG may not detect security incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore computing services in a timely manner.

Although this report contains 12 recommendations, we believe the most significant security deficiencies relate to security configuration management (Finding B), POA&M (Finding D), vulnerability assessments (Finding G), contingency plans (Finding H), and incident response (Finding I).

We provided the draft report to BBG officials on October 27, 2011. In BBG's November 2, 2011, response (see Appendix C) to this report, BBG concurred with the 12 recommendations. Based on the response, OIG considers all 12 recommendations resolved, pending further action.

BBG's responses to the recommendations and OIG's analyses are presented after each recommendation.

Background

FISMA recognizes the importance of information security to the economic and national security interests of the United States and requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information

⁴ NIST SP 800-34, rev.1, *Contingency Planning Guide for Federal Information Systems*, May 2010.

UNCLASSIFIED

systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor or another 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.⁵ 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.

Results of Review

Overall, we found that BBG made progress in FY 2011 toward developing its information security program, but 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.

A. BBG Has Not Implemented a System Inventory Management Process

The FY 2010 *Review of the Information Security Program at the Broadcasting Board of Governors* concluded that BBG did not complete its system inventory of IT assets.

BBG has not implemented a process or procedures to routinely update and manage its IT assets. During the fourth quarter of FY 2010, an IT director was hired to develop the system inventory management process. A system inventory management tool was selected and the required purchase order was submitted. However, the procurement has not been finalized.

FISMA requires the head 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. Each agency must identify information systems in an inventory, including the interfaces between each system and all other systems or networks, to include those not operated by or under the control of the agency. FISMA further requires that the inventory be updated at least annually and be used to support information resources management. Additionally, NIST

⁵ OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Sept.14, 2011.

UNCLASSIFIED

SP 800-53, Revision 3,⁶ *Recommended Security Controls for Information Systems and Organizations*, requires the organization to develop, document, and maintain an inventory of information system components that accurately reflects the current information system, is consistent with the authorization boundary of the information system, is at the level of granularity deemed necessary for tracking and reporting, includes organization-defined information deemed necessary to achieve effective property accountability, and is available for review and audit by designated organization officials.

Without a system inventory management process, BBG may not have an accurate accounting of its IT assets and the related system interfaces and underlying support systems and will not be able to properly identify and mitigate security risks. As a result, critical management processes such as strategic planning, budgeting, system administration, and resource management may be adversely affected.

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 National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Management Comments: BBG concurred with the recommendation, stating that it “has acquired the inventory management software tool and is currently installing and configuring the tool. The CIO will oversee testing of this tool and the development of a process to update BBG’s system inventory periodically.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that BBG has implemented a system inventory process.

B. Security Standards and Procedures Have Not Been Implemented and Enforced

The FY 2010 *Review of the Information Security Program at the Broadcasting Board of Governors* concluded that BBG did not complete the development and implementation of its security configuration and performance measurement standards and procedures for the IT environment. Further, BBG’s standard operating procedures and information security policies were not enforced at OCB. Therefore, BBG did not maintain control over OCB systems connected to its network, and OCB managed its own servers that were connected to BBG’s network. Additionally, OCB did not complete the security authorization process.

BBG drafted several IT policies and procedures during FY 2011; however, BBG’s IT management stated that the additional IT policies and procedures had not been implemented

⁶ NIST SP 800-53, rev.3, *Recommended Security Controls for Information Systems and Organizations*, Aug.2009 (updated through Sept. 14, 2009).

UNCLASSIFIED

because of resource limitations. Additionally, although BBG's IT department provides guidance to OCB regarding development and implementation of IT policies and procedures, it does not have the authority to enforce compliance because OCB reports directly to the Broadcasting Board of Governors.

In regard to security standards and procedures, NIST SP 800-53, Revision 3,⁷ states:

The organization develops, disseminates, and periodically reviews/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.

Without detailed procedures and guidance that govern the performance of routine and critical processes, BBG may not be able to effectively manage its IT program, which could introduce security weaknesses and result in inconsistent performance. Additionally, BBG cannot be assured that security controls are properly managed and maintained for all systems that access the BBG network. As a result, systems may operate in the production environment without appropriate controls or management oversight.

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 National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Management Comments: BBG concurred with the recommendation, stating that the CIO "will oversee the collection and organization of any existing security configuration procedures, will assess progress to complete the development and implementation of additional procedures by March 31, 2012, and will periodically assess compliance with these implemented procedures."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing standard operating procedures for security configuration.

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 National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Management Comments: BBG concurred with the recommendation, stating that the CIO "will oversee the development of procedures to provide oversight such that security

⁷ Configuration Management Policy and Procedures (CM-1).

controls are properly managed and maintained for all systems that directly access the BBG network by March 31, 2012.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing procedures for overseeing the management and maintenance of security controls for all systems that access the BBG network.

C. Compliance With BBG’s Security Awareness Training Program Was Not Strictly Enforced

The FY 2010 *Review of the Information Security Program at the Broadcasting Board of Governors* concluded that BBG did not sanction employees and contractors who did not complete the annual security awareness training course. Although users were informed of the possibility of enforcement actions for not completing the course, no such actions were implemented. BBG IT management stated that compliance with the security awareness training policy was not strictly enforced because of concerns about possible disruption of BBG’s mission and employees’ job responsibilities if user access was restricted. Additionally, contractor personnel were not consistently required to complete BBG’s security awareness training prior to or shortly after being granted access to BBG’s network.

In regard to security awareness, NIST SP 800-53, Revision 3,⁸ states:

The organization ensures all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and thereafter (that is, at least annually).⁹

The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.¹⁰

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 data. As a result, personnel may be unable to recognize and respond appropriately to real and potential security concerns.

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 National Institute of Standards and Technology Special Publication 800-53, Revision 3, and the Broadcasting Board of Governors information security policies.

⁸ Ibid.

⁹ Security Awareness Control (AT-2).

¹⁰ Personnel Sanctions Control (PS-8).

UNCLASSIFIED

Management Comments: BBG concurred with the recommendation, stating that the CIO “has initiated discussions” with BBG’s Office of Human Resources “to require all new personnel to attend initial or refresher security awareness training.” BBG further stated that the CIO “will update the security awareness training policy by December 31, 2011,” and “will work with” the Office of Human Resources “to develop and implement consequences for personnel who are non-compliant with the policy, while minimizing the impact on Agency operations and the BBG mission.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts the revised security awareness training policy showing the requirements of training for new personnel and the enforcement actions to be taken for noncompliant personnel.

D. Plans of Action and Milestones Have Not Been Completed

The FY 2010 *Review of the Information Security Program at the Broadcasting Board of Governors* concluded that BBG’s POA&Ms have not been completed fully to track all identified weaknesses in BBG’s major applications and general support systems. Further, POA&Ms did not include sufficient details of security weaknesses such as planned actions, prioritization of weaknesses, required resources, or changes to milestones for actions that had not been completed according to the plan.

Although BBG contracted with a vendor during the third quarter of FY 2010 to assist it with the security authorization of its systems, including the development of POA&Ms for each system, the POA&M process has not been formalized to establish the information requirements or a requirement to review and update the POA&Ms periodically.

OMB Memorandum M-11-33 states:¹¹ “POA&Ms must include all security weaknesses found during any other review done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments. These plans should be the authoritative agency-wide management tool, inclusive of all evaluations.”

Without periodic updates and reviews of POA&M activities, BBG IT management may be unaware of the statuses of corrective actions. As a result, delays in the implementation of corrective actions may prevent 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 5: We recommend that 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 Office of Management and Budget Memorandum M-11-33, *FY 2011 Reporting Instructions for the*

¹¹ OMB M-11-33, sec. 36, POA&M (citing previous guidance contained in OMB M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*).

UNCLASSIFIED

Federal Information Security Management Act and Agency Privacy Management, September 14, 2011.

Management Comments: BBG concurred with the recommendation, stating that the CIO “will edit” the current POA&M policy by December 31, 2011, “to require responsible managers to review and update their respective POA&Ms periodically.” BBG further stated that the CIO or his designee will also “review these POA&M reports periodically to determine whether or not additional resources need to be allocated.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that POA&Ms are reviewed and updated periodically and that resources have been allocated as necessary to prevent delays in taking corrective actions.

E. Remote Access to the BBG Network Was Not Properly Managed and Controlled

The FY 2010 *Review of the Information Security Program at the Broadcasting Board of Governors* concluded that BBG’s remote access policy allowed users to access the BBG network from personal computers using software provided by BBG. However, BBG did not have procedures in place to ensure that proper safeguards were implemented on non-BBG computers that were authorized to access the BBG network remotely.

BBG allows its users to remotely access the BBG network using their personal computers. BBG’s IT management stated that a process has been drafted and a software tool has been identified that will detect and scan the security settings of requesting computers but that the project has not been funded.

According to NIST SP 800-53, Revision 3,¹² the organization documents, monitors, and controls all methods of remote access (for example, dial-up and the Internet) to the information system, including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.

Without proper policies and procedures that require the use of properly secured devices, BBG may be unable to ensure the security of its data and network when allowing access to authorized third-party devices. As a result, the risks of introducing viruses, worms, or other malicious code increase significantly.

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 National Institute of Standards and Technology Special Publication 800-53, Revision 3.

¹² Remote Access Control (AC-17).

UNCLASSIFIED

Management Comments: BBG concurred with the recommendation, stating that the CIO “will develop the process and initiate planning and testing of the software tool intended 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 it “will grant access only to those [third-party devices] whose configurations are deemed sufficient, by March 31, 2012, pending allocation of sufficient funds for this purpose.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that BBG has implemented a process to assess the adequacy of the security configurations of third-party devices that request access to the BBG network and grant access only to properly configured devices.

F. User Account Management Controls Need Improvement

The FY 2010 *Review of the Information Security Program at the Broadcasting Board of Governors* concluded that BBG’s user account management controls do not ensure that access is provided to authorized personnel only. Although BBG implemented new user account management controls in FY 2011, including user verification controls that require users to obtain new passwords in person after presenting photo identification, we observed the following account management control deficiencies:

- Guest, test, and shared user accounts that, when used, do not allow for individual accountability.
- Five of 94 employees who separated from BBG in FY 2011 between October 1, 2010, and June 8, 2011, retained “active” AD user accounts as of June 14, 2011.
- One hundred nineteen active user accounts in AD have never been used, and 27 of the 119 user accounts were created before 2009.
- Seventy-six active user accounts in AD have not been used for over 90 days, and 24 of the 76 active user accounts have not been used since 2009 or before that year.
- An individual requested and was provided a new password via a telephone call.

BBG has taken actions to remove unnecessary user accounts; however, the process has not been completed and procedures have not been established to perform the review routinely. Additionally, BBG’s help desk personnel did not consistently adhere to the established user verification controls for the issuance of new passwords.

OMB Circular No. A-130, Revised, Appendix III,¹³ states:

¹³ OMB Circular No. A-130 Revised, *Management of Federal Information Resources*, app. III, “Security of Federal Automated Information Resources,” Nov. 28, 2000.

UNCLASSIFIED

Agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. “Adequate security” means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

Additionally, NIST SP 800-53, Revision 3,¹⁴ states that the organization manages information system accounts, including authorizing and monitoring the use of guest and anonymous and temporary accounts, and reviewing accounts.

Without more stringent user account management controls, unauthorized use of user accounts and thus, the risk of 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.

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 National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Management Comments: BBG concurred with the recommendation, stating that the CIO “has made significant progress in reviewing the history and rationale of guest, test, and shared user accounts.” BBG further stated that the CIO “will develop policies and procedures to restrict the use of guest, test, and shared user accounts to ensure user accountability for access to BBG computing resources by December 31, 2011.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts BBG’s policies and procedures that restrict the use 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 or transferred or when information system usage or need-to know/need-to-share changes are made, in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Management Comments: BBG concurred with the recommendation, stating that the CIO “will develop policies and procedures requiring system owners to notify account managers when user employment status or system access needs change by March 31, 2012.”

¹⁴ Account Management Access Control 2 (AC-2).

UNCLASSIFIED

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts BBG's policies and procedures that require system owners to notify account managers when there is a change in a user's employment status or system access needs.

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.

Management Comments: BBG concurred with the recommendation, stating that the CIO "will develop and implement procedures for monitoring and reviewing compliance with the password reset procedures by March 31, 2012." BBG further stated that the CIO "will review the password reset policy and consider alternative methods for implementing the user identification requirements."

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that compliance with the password reset procedures is monitored and reviewed.

G. Vulnerability Assessments Were Not Performed

The FY 2010 *Review of the Information Security Program at the Broadcasting Board of Governors* concluded that BBG did not perform routine vulnerability assessments of its major systems and network environment using the framework outlined in NIST SP 800-53A.¹⁵ Although BBG performed ad hoc scans of its systems and the general support system, BBG did not expand the process to include the periodic re-performance of vulnerability assessments for all major systems or the routine performance of such scans on its enterprise network.

BBG IT management stated that a vulnerability assessment tool was implemented during FY 2011 to perform scans of its network. However, the policy and related procedures for routine vulnerability assessments have not been developed and implemented.

According to NIST SP 800-53A,¹⁶ the organization scans for vulnerabilities in the information system under an organization-defined frequency schedule or when significant new vulnerabilities potentially affecting the system are identified and reported.

Without periodic reviews or the performance of risk-based vulnerability assessments using NIST SP 800-53A,¹⁷ new threats and vulnerabilities may not be identified and mitigated in a timely manner. Such threats and vulnerabilities may limit the effectiveness of security controls, thereby resulting in the loss, damage, or theft of valuable information and/or resources.

¹⁵ NIST SP 800-53A, *Guide for Assessing Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*, July 2008.

¹⁶ Risk Assessment Control RA-5.

¹⁷ *Ibid.*

UNCLASSIFIED

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 National Institute of Standards and Technology Special Publication 800-53A.

Management Comments: BBG concurred with the recommendation, stating that it “has acquired a software tool and is currently installing and configuring the tool.” BBG further stated that the CIO “will develop policies and procedures to perform routine vulnerability assessments with the tool for all major systems and general support systems by December 31, 2011.”

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation showing that routine vulnerability assessments are performed for all major systems and general support systems.

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

The FY 2010 *Review of the Information Security Program at the Broadcasting Board of Governors* concluded that BBG did not develop and implement contingency planning and testing policies and procedures compliant with NIST SP 800-34, Revision 1.¹⁸ Specifically, BBG did not complete its enterprise-wide and system-specific contingency plans or conduct contingency tests.

BBG does not have formal policies and procedures for developing contingency plans. BBG’s IT management stated that although a strategic plan was developed to address BBG’s contingency and business resumption needs, resources were not appropriated to develop policies and procedures for contingency plans because of substantial budget uncertainties at BBG during FY 2011.

NIST SP 800-34, Revision 1,¹⁹ states that information systems are “vital elements” in most business functions and that “it is critical” that the services provided by these systems are able to operate effectively without excessive interruption. Further, NIST SP 800-53, Revision 3,²⁰ states, “Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered quickly and effectively following a service disruption.”

Without an effective contingency plan, which includes periodic testing of the plan's reliability, BBG may be unable to access critical information and resources or perform mission-

¹⁸ NIST SP 800-34, rev. 1, *Contingency Planning Guide for Federal Information Systems* May 2010 (last updated November 11, 2010).

¹⁹ Ibid.

²⁰ NIST SP 800-53, rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, Aug 2009.

critical business functions in the event of an extended outage and/or a disaster. As a result, BBG may be unable to resume operations in an efficient and effective manner.

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 National Institute of Standards and Technology Special Publication 800-34, Revision 1.

Management Comments: BBG concurred with the recommendation, stating that although its IT Directorate in the Office of Technology, Services, and Innovation does have data backup, restoration plans, and deep investments in internal redundant architecture, BBG “agrees to further develop contingency plans and increase investments in offsite systems to be used for business continuity.” BBG further stated: “To support and lead this effort, the CIO is planning to add a Disaster Recovery and Business Continuity Manager position by March 31, 2012, to focus specifically on this subject. All positions and equipment required to meet this recommendation are subject to available funding.”

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

I. BBG’s Incident Response Policy Does Not Adhere to United States Computer Emergency Readiness Team’s Reporting Requirements

BBG’s Computer Security Incident Management Policy does not comply with the requirements established by US-CERT. BBG’s policy requires category 1 (CAT 1) incidents to be reported to US-CERT within 2 hours of detection, but US-CERT stipulates that CAT 1 incidents be reported within 1 hour of discovery/detection.

The US-CERT Federal Incident Reporting Guidelines and NIST SP 800-61, Revision 1,²¹ require the following:

Category	Name	Description	Reporting Timeframe
CAT 1	Unauthorized Access	In this category, an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.	Within one (1) hour of discovery/detection.

²¹ NIST SP 800-61, rev.1, *Computer Security Incident Handling Guide*, March 2008.

UNCLASSIFIED

Further, BBG's policy does not include reporting requirements for incidents of compromised PII. The US-CERT reporting timeframe for incidents that involve compromised PII is within 1 hour of detection regardless of the incident's category reporting timeframe. OMB Memorandum M-07-16²² states:

Agencies must report all incidents involving personally identifiable information to US-CERT. This reporting requirement does not distinguish between potential and confirmed breaches. The US-CERT concept of operations for reporting Category 1 incidents is modified as follows:

Category 1: Unauthorized Access or Any Incident Involving Personally Identifiable Information. In this category agencies must report when: 1) an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource; or 2) there is a suspected or confirmed breach of personally identifiable information regardless of the manner in which it might have occurred. Reporting to US-CERT is required within one hour of discovery/detection.

Lastly, BBG's Computer Security Incident Management Policy²³ states that incidents will be escalated to external entities (for example, US-CERT and law enforcement) only during normal business hours.²⁴

BBG's IT management stated that some US-CERT requirements were mistakenly excluded during the development of its new incident response policy. IT management further stated that the reporting timelines were extended because of BBG's resource limitations.

Without an effective incident response capability, BBG may not be able respond to security incidents in a timely manner and restore computing services.

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 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 the breach occurred in electronic or paper format.

²² OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007.

²³ Computer Security Incident Management Policy May 16, 2011

²⁴ *Ibid.*

UNCLASSIFIED

Management Comments: BBG concurred with the recommendation, stating that it “will modify the policy” by December 31, 2011.

OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts the revised incident response policy showing a complete and comprehensive process that meets US-CERT’s requirements for identifying, reporting, and resolving computer security incidents.

List of Current Year Recommendations

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 National Institute of Standards and Technology Special Publication 800-53, Revision 3.

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.

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 National Institute of Standards and Technology Special Publication 800-53, Revision 3.

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.

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 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.

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 National Institute of Standards and Technology Special Publication 800-53, Revision 3.

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 National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Recommendation 8: We recommend that the Chief Information Officer establish policies and procedures requiring system owners to notify account managers when information system users

UNCLASSIFIED

are terminated or transferred or when 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.

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.

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 National Institute of Standards and Technology Special Publication 800-53A.

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 National Institute of Standards and Technology Special Publication 800-34, Revision 1.

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 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 the breach occurred in electronic or paper format.

Appendix A. Objectives, Scope, and Methodology

In order to fulfill its responsibilities related to the Federal Information Security Management Act (FISMA), the Office of Inspector General (OIG) 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 2011.

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 evaluation from April through September 2011. In addition, we performed the review 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 and OIG believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We performed fieldwork from April through July 31, 2011. Our fieldwork was completed before OMB Memorandum M-11-33, dated September 14, 2011, was issued. This memorandum provided instructions for FY 2011 reporting requirements. We reviewed the memorandum and determined that no additional testing was required to fulfill the FISMA reporting requirements.

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

UNCLASSIFIED

- OMB Memoranda M-02-01, M-07-16, M-08-21, and M-11-33.¹
- 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,² and OMB Circular No. A-11.³
- NIST SPs, Federal Information Systems Processing Publications (FIPS), other applicable NIST publications, and industry best practices.

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

- Risk management framework (formerly Certification & Accreditation)
- Security configuration management
- Incident response and reporting
- Security training
- Plans of action and milestones
- Remote access
- Account and identity management
- Continuous monitoring
- Contingency planning
- Oversight of contractor systems
- Security architecture and capital planning

The evaluation covered the period October 1, 2010, to September 30, 2011. During the fieldwork, we took the following actions:

- Determined the extent to which 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 evaluation approach addressed OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated September 14, 2011.

¹ OMB Memoranda M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, Oct. 17, 2001; M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007; M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 14, 2008; and M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Sept. 14, 2011.

² OMB Circular No. A-130 Revised, *Management of Federal Information Resources*, app.III, "Security of Federal Automated Information Resources," Nov. 30, 2000.

³ OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, Aug. 2011.

UNCLASSIFIED

- Assessed programs for monitoring of security policy and program compliance and responding to security events (that is, unauthorized changes detected by intrusion detection systems).
- Performed testing of major systems at the discretion of OIG.
- 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 *Review of the Information Security Program at the Broadcasting Board of Governors* (AUD/IT/IB-11-08, November 2010).

Appendix B. Followup of Recommendations From the FY 2010 FISMA Report

The evaluation team reviewed actions implemented by management to mitigate the findings identified in the FY 2010 FISMA report. The current status of each of the recommendations follows:

Recommendation 1: We recommend that the Chief Information Officer ensure that the Information Technology Director develop and implement a process to update, not less than annually, the Broadcasting Board of Governors (BBG) system inventory when changes occur or are made to those information systems operated by or under the control of BBG or by those third-party contractors or agencies on behalf of BBG.

2011 Status – Open; this repeat recommendation has become Recommendation 1 (Finding A) in the FY 2011 report.

Recommendation 2: We recommend that the Chief Information Officer continue efforts to complete the certification and accreditation of the Broadcasting Board of Governors major systems to include the development and maintenance of documentation used in the certification process and the security accreditation decision, inclusive of the Federal Information Processing Standards Publication 199 system categorization, risk assessment, system security plan, plan of action and milestones, and contingency plan.

2011 Status – Closed.

Recommendation 3: We recommend that the Chief Information Officer ensure that the appropriate information technology personnel are assigned to develop and implement standard operating procedures for security configuration and performance measurement and ensure that management of the Broadcasting Board of Governors periodically assess compliance with the implemented procedures.

2011 Status – Closed.

Recommendation 4: We recommend that the Chief Information Officer develop standard operating procedures, including the performance of periodic security assessments and continuous monitoring for security threats, for the oversight of all systems and hardware that are connected to the Broadcasting Board of Governors network.

2011 Status – Open; this repeat recommendation has become Recommendation 2 (Finding B) in the FY 2011 report.

Recommendation 5: We recommend that the Chief Information Officer update the security awareness training policy requiring all new employees and contractors to attend initial security awareness training, require all employees and contractors to receive refresher training annually,

UNCLASSIFIED

develop disciplinary actions for those who do not take annual refresher training, and develop training for personnel who have significant security responsibilities.

2011 Status – Open; this repeat recommendation has become Recommendation 4 (Finding C) in the FY 2011 report.

Recommendation 6: We recommend the Chief Information Officer develop a policy requiring responsible managers to review and update Plans of Action and Milestones (POA&M) at a minimum, on a quarterly basis; review the quarterly POA&M reports; and assess the timeliness of corrective actions to allocate resources needed to prevent delays.

2011 Status – Open; this repeat recommendation has become Recommendation 5 (Finding D) in the FY 2011 report.

Recommendation 7: We recommend that the Chief Information Officer implement security mechanisms that assess the adequacy of the security configurations of third-party devices that request access to the Broadcasting Board of Governors (BBG) network prior to granting the requested access. Improperly configured devices should not be allowed to access the BBG network.

2011 Status – Open; this repeat recommendation has become Recommendation 6 (Finding E) in the FY 2011 report.

Recommendation 8: We recommend that the Chief Information Officer limit remote access privileges to employees who have been properly authorized by user management in accordance with the Broadcasting Board of Governors remote access policies and procedures.

2011 Status – Closed.

Recommendation 9: We recommend that the Chief Information Officer implement password management policy and procedures that require system users to select, at a minimum, three of the following four categories when establishing a system's passwords: English uppercase characters (A through Z); English lowercase characters (a through z); base 10 digits (0 through 9); or non-alphabetic characters, such as !, \$, #, or %.

2011 Status – Closed.

Recommendation 10: We recommend that the Chief Information Officer develop procedures that require individual users to establish password reset information that only the individual users can verify when they request password reset by telephone.

2011 Status – Closed.

Recommendation 11: We recommend that the Chief Information Officer restrict the use of guest, test, and shared user accounts to ensure user accountability.

2011 Status – Open; this repeat recommendation has become Recommendation 7 (Finding F) in the FY 2011 report.

UNCLASSIFIED

Recommendation 12: We recommend that the Chief Information Officer allocate existing resources or acquire additional resources, if needed, to develop and implement policies and procedures for the routine performance of security assessments for all major systems and general support systems. The results of such security assessments should be reviewed, and Plans of Action and Milestones should be developed for the improvement of the security controls of major systems and general support systems.

2011 Status – Open; this repeat recommendation has become Recommendation 10 (Finding G) in the FY 2011 report.

Recommendation 13: We recommend that the Chief Information Officer record all security incidents in the ticketing systems for centralized reporting, analysis, monitoring, and resolution.

2011 Status – Closed.

Recommendation 14: 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; perform periodic testing of BBG's contingency plans; and make updates to the plan based on lessons learned.

2011 Status – Open; this repeat recommendation has become Recommendation 11 (Finding H) in the FY 2011 report.

UNCLASSIFIED

Appendix C. Broadcasting Board of Governors Response

Broadcasting Board of Governors

INTERNATIONAL BROADCASTING BUREAU



November 2, 2011

Mr. Harold W. Geisel
Deputy Inspector General
Office of Inspector General
U.S. Department of State

Dear Mr. Geisel:

This is in response to the e-mail from Ms. Amy Conigliaro, dated October 27, 2011, regarding the Office of Inspector General's (OIG) Draft Report titled, "Evaluation of the Broadcasting Board of Governors Information Security Program," Report Number AUD/IT-XX-XX-XXX, dated October 2011.

The Broadcasting Board of Governors is grateful for the opportunity to review the OIG's draft report. Our IT staff made a concerted effort to cooperate with the team and provide an open forum of discussion and a willingness to comply with the team's requests for documentation. We appreciate the team's recognition of this effort during the FISMA review process and believe the report will be helpful to us in strengthening BBG's information security program. Our detailed comments on the draft report recommendations are annotated on the enclosure.

If you have any questions, please feel free to contact me,

(b) (6)

Sincerely,

A handwritten signature in black ink, appearing to read "Richard M. Lobo".

Richard M. Lobo
Director

Enclosure: As stated

330 Independence Avenue, SW

Washington, DC 20237

UNCLASSIFIED

Enclosure

**Broadcasting Board of Governors (BBG) Response to
the Office of Inspector General's (OIG) Office of Audits Draft Report titled,
"Evaluation of the Broadcasting Board of Governors Information Security Program,"
Report Number AUD/IT-XX-XX-XXX, dated October 2011**

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.

Response: The BBG concurs. The BBG has acquired the inventory management software tool and is currently installing and configuring the tool. The CIO will oversee testing of this tool and the development of a process to update BBG's system inventory periodically.

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.

Response: The BBG concurs. The CIO will oversee the collection and organization of any existing security configuration procedures, will assess progress to complete the development and implementation of additional procedures by March 31, 2012 and will periodically assess compliance with these implemented procedures.

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 National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Response: The BBG concurs. The CIO will oversee the development of procedures to provide oversight such that security controls are properly managed and maintained for all systems that directly access the BBG network by March 31, 2012.

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 non-compliance 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 Governor's information security policies.

1

UNCLASSIFIED

Response: The BBG concurs. The CIO has initiated discussions with the BBG's Office of Human Resources (HR) to require all new personnel to attend initial or refresher security awareness training. In addition, the CIO will update the security awareness training policy by December 31, 2011. The CIO also will work with HR to develop and implement consequences for personnel who are non-compliant with the policy, while minimizing the impact on Agency operations and the BBG mission.

Recommendation 5: We recommend the Chief Information Officer develop a policy requiring responsible managers to review and update Plans of Action and Milestones (POA&M) 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.

Response: The BBG concurs. The CIO will edit the current POA&M policy by December 31, 2011, to require responsible managers to review and update their respective POA&Ms periodically. The CIO or his designee also will review these POA&M reports periodically to determine whether or not additional resources need to be allocated.

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.

Response: The BBG concurs. The CIO will develop the process and initiate planning and testing of the software tool intended 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 and will grant access only to those whose configurations are deemed sufficient, by March 31, 2012, pending allocation of sufficient funds for this purpose.

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.

Response: The BBG concurs. The CIO has made significant progress in reviewing the history and rationale of guest, test, and shared user accounts. The CIO will develop policies and procedures to restrict the use of guest, test, and shared user accounts to ensure user accountability for access to BBG computing resources by December 31, 2011.

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, in accordance with the National Institute of Standards and Technology Special Publication 800-53, Revision 3.

UNCLASSIFIED

Response: The BBG concurs. The CIO will develop policies and procedures requiring system owners to notify account managers when user employment status or system access needs change by March 31, 2012.

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.

Response: The BBG concurs. The CIO will develop and implement procedures for monitoring and reviewing compliance with the password reset procedures by March 31, 2012. The CIO also will review the password reset policy and consider alternative methods for implementing the user identification requirements.

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.

Response: The BBG concurs. The BBG has acquired a software tool and is currently installing and configuring the tool. The CIO will develop policies and procedures to perform routine vulnerability assessments with the tool for all major systems and general support systems by December 31, 2011.

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.

Response: The BBG concurs. Although the BBG's IT Directorate in the Office of Technology, Services, and Innovation (TSI) does have data backup, restoration plans, and deep investments in internal redundant architecture, 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 planning to add a Disaster Recovery and Business Continuity Manager position by March 31, 2012, to focus specifically on this subject. All positions and equipment required to meet this recommendation are subject to available funding.

Recommendation 12: We recommend that the Chief Information Officer develop and implement a complete and comprehensive process that meets the US-CERT's 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. BBG's Computer Security

UNCLASSIFIED

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 the 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.

Response: The BBG concurs. The BBG will modify the policy, as requested, by December 31, 2011.

UNCLASSIFIED

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
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 oig.state.gov

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

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED