



UNITED STATES DEPARTMENT OF STATE
AND THE BROADCASTING BOARD OF GOVERNORS
OFFICE OF INSPECTOR GENERAL

AUD-IT-IB-14-02

Office of Audits

October 2013

Audit of the Broadcasting Board of Governors Information Security Program

~~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.~~



~~SENSITIVE BUT UNCLASSIFIED~~

United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

(U) PREFACE

(U) 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.

(U) 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 2013. To perform this audit, OIG contracted with the independent public accountant Williams, Adley & Company, LLP. The audit report is based on interviews with employees and officials of the Broadcasting Board of Governors, direct observation, and a review of applicable documents.

(U) The independent public accountant identified areas in which improvements could be made, including the risk management program, continuous monitoring, contingency planning, incident response and reporting, plans of actions and milestones, remote access management, configuration management, identity and access management, and security training and awareness.

(U) 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 audit report 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.

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

A handwritten signature in blue ink, appearing to read "S. Linick".

Steve A. Linick
Inspector General

~~SENSITIVE BUT UNCLASSIFIED~~



Audit of the Broadcasting Board of Governors Information Security Program

October 15, 2013

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's 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 and the Broadcasting Board of Governors Office of Inspector General.

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

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

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

(U) Acronyms

(U) BBG	Broadcasting Board of Governors
(U) CIO	Chief Information Officer
(U) CTO	Chief Technology Officer
(U) DHS	Department of Homeland Security
(U) FIPS	Federal Information Processing Standards
(U) FISMA	Federal Information Security Management Act
(U) GAGAS	Generally Accepted Government Auditing Standards
(U) IT	Information Technology
(U) NIST	National Institute of Standards and Technology
(U) OIG	Office of Inspector General
(U) OMB	Office of Management and Budget
(U) PIV	Personal Identity Verification
(U) POA&M	Plans of Action and Milestones
(U) SP	Special Publication
(U) VPN	Virtual Private Network

(U) Table of Contents

(U) <u>Section</u>	(U) <u>Page</u>
(U) Executive Summary	1
(U) Background	2
(U) Objective	3
(U) Results of Audit.....	3
(U) Finding A. Risk Management	3
(U) Finding B. Continuous Monitoring Management	6
(U) Finding C. Contingency Planning	8
(U) Finding D. Incident Response and Reporting	9
(U) Finding E. Plans of Action and Milestones	10
(U) Finding F. Remote Access Management.....	11
(U) Finding G. Configuration Management	13
(U) Finding H. Identity and Access Management	15
(U) Finding I. Security Training and Awareness.....	17
(U) Finding J. Compliance with FISMA	18
(U) List of Current Year Recommendations.....	19
(U) Appendices	
(U) A. Scope and Methodology	21
(U) B. Followup of Recommendations from the FY 2012 Audit of the Broadcasting Board of Governors Information Security Program	25
(U) C. Management Response	28

(U) Executive Summary

(U) In accordance with the Federal Information Security Management Act of 2002 (FISMA),¹ the Office of Inspector General (OIG) contracted with Williams, Adley & Company-DC, 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). The results are designed to assist OIG in providing responses to the Department of Homeland Security (DHS) *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*, dated November 30, 2012.

(U) The FY 2012 FISMA report² contained nine recommendations intended to address security deficiencies, and the most significant of these deficiencies involved BBG’s security standards and procedures, compliance enforcement authority, Plans of Action and Milestones (POA&M), and enterprise-wide and system-specific contingency plans. We reviewed BBG’s corrective actions to address weaknesses identified in OIG’s FY 2012 FISMA report. BBG closed four of nine recommendations in the FY 2012 report. The status of each recommendation from OIG’s FY 2012 report is presented in Appendix B of this report.

(U) Since FY 2012, BBG has taken the following steps to improve management controls:

- (U) Substantially improved the security awareness training compliance rate achieving 100 percent in FY 2013.
- (U) Improved the management of Active Directory to limit the amount of expired and inactive user accounts on the domain.

(U) Overall, we found that BBG had implemented an information security program and had made progress during FY 2013, but we identified control weaknesses that significantly impacted the information security program. If these control weaknesses were exploited, BBG could experience security breaches.

(U) Collectively, the control weaknesses we identified in this audit represent a significant deficiency, as defined by OMB Memorandum M-12-20,³ to enterprise-wide security. The weakened security controls could adversely affect the confidentiality, integrity, and availability of information and information systems. A further compounding factor is that BBG had not fully taken corrective action to remediate all of the control weaknesses identified in the FY 2012 FISMA report. This report contains 13 recommendations to address security deficiencies identified in eleven reportable areas, and we believe the most significant security deficiencies are the findings related to risk management framework (Finding A), continuous monitoring program (Finding B), enterprise-wide and system-specific contingency plan (Finding C), incident

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

² (U) *Audit of the Broadcasting Board of Governors Information Security Program* (AUD-IT-IB-13-04, Nov. 2012).

³ (U) OMB Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Sept. 27, 2012.

response and reporting program (Finding D), and the Plans of Action and Milestones (POA&M) process (Finding E). Following is a summary of the findings:

- (U) In FY 2010,⁴ FY 2011,⁵ FY 2012 and FY 2013, OIG reported that BBG's risk management framework was not effective. (Finding A)
- (U) In FY 2013, OIG identified that the Office of the Chief Information Officer/Chief Technology Officer (CIO/CTO) did not have an overall continuous monitoring program for the agency. (Finding B)
- (U) BBG did not develop an enterprise-wide and system-specific contingency plan or perform any contingency testing. (Finding C)
- (U) BBG did not have effective incident response and reporting. (Finding D)
- (U) In FY 2013, OIG found that POA&M entries were not fully completed. (Finding E)
- (U) The Enterprise Networks and Storage Division, under the Office of the CIO/CTO, had not implemented procedures to ensure that remote access was granted only to computers that have security safeguards that comply with BBG's policies and procedures. (Finding F)

[Redacted] (b) (5)

- (U) BBG did not have effective identity and access management of their information systems. (Finding H)
- (U) BBG did not have a policy for role-based training. (Finding I)

(U) In addition, OIG found that BBG was in compliance with the Capital Planning and Contractor System requirements. (Finding J)

(U) Background

(U) BBG is an independent Federal agency supervising all U.S. Government-supported civilian international media. Broadcasters within the BBG network include the Voice of America, Radio Free Europe/Radio Liberty, the Middle East Broadcasting Networks, Radio Free Asia, and the Office of Cuba Broadcasting. BBG's mission is to inform, engage, and connect people around the world in support of freedom and democracy.

(U) 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

⁴ (U) *Review of the Broadcasting Board of Governors Information Security Program* (AUD/IT/IB-11-08, Nov. 2010).

⁵ (U) *Evaluation of the Broadcasting Board of Governors Information Security Program* (AUD/IT/IB-12-15, Nov. 2011).

provides a comprehensive framework for establishing and ensuring the effectiveness of management, operational, and technical controls over information technology (IT) that supports Federal operations and assets, and it provides a mechanism for improved oversight of Federal agency information security programs.

(U) On an annual basis, OMB provides guidance with reporting categories and questions to meet the current year's reporting requirements.⁶ 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.

(U) FISMA assigns specific responsibilities to Federal agencies, NIST, OMB and DHS⁷ to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to 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, chief information security 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.

(U) Objective

(U) The objective of this audit was to perform an independent evaluation of BBG's information security program and practices for FY 2013, which included testing the effectiveness of security controls for a subset of systems, as required.

(U) Results of Audit

(U) Overall, we found that BBG made progress in FY 2013 toward developing its information security program, but we identified control weaknesses that significantly impacted the information security program. To improve the information security program and to bring the program into compliance with FISMA, OMB, and NIST requirements, BBG needs to address the control weaknesses described.

(U) Finding A. Risk Management

(U) In FY 2010, FY 2011, and FY 2012, OIG identified risk management framework deficiencies in BBG's information security program. According to NIST Special Publication (SP) 800-37, Revision 1,⁸ the risk management framework emphasizes:

(U) ... (i) building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical

⁶ (U) DHS *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*, Nov. 2012.

⁷ (U) OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and Department of Homeland Security (DHS)*, July 6, 2010.

⁸ (U) NIST SP 800-37, rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, sec. 1.1, Feb. 2010.

security controls; (ii) maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes; and (iii) providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems.

(U) NIST SP 800-39⁹ lists the four steps of the risk management process, which are Risk Framing, Risk Assessment, Risk Response, and Risk Monitoring.

(U) BBG's risk management framework was not effective. In FY 2013, OIG identified the following deficiencies:

- (U) For all three systems tested, the Information Security Management Division did not adequately categorize system information types in the security plans. The Information Security Management Division identified data elements within the security plans as "other" instead of using NIST SP 800-60, Revision 1,¹⁰ elements such as Information System, Record Retention, and System and Network Monitoring. According to Federal Information Processing Standard (FIPS) 199,¹¹ "... the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the information system." Furthermore, NIST SP 800-60, Revision 1,¹² does not include the category "other" as a valid information type.
- (U) For all three systems tested, the Information Security Management Division did not perform annual security control assessments. NIST SP 800-53, Revision 3,¹³ states, "Subsequent to the initial authorization of the information system and in accordance with OMB policy, the organization assesses a subset of the security controls annually during continuous monitoring."
- (U) For two of three systems tested, the security plans did not include NIST SP 800-53, Revision 3, controls. OMB M-10-15¹⁴ states, "For legacy information systems, agencies are expected to be in compliance with NIST standards and guidelines within one year of the publication date unless otherwise directed by OMB. The one year compliance date for revisions to NIST publications applies only to the new and/or updated material in the publications. For information systems under development or for legacy systems undergoing significant changes, agencies are expected to be in compliance with the NIST publications immediately upon deployment of the information system."

⁹ (U) NIST SP 800-39, *Managing Information Security Risk*, app. E, March 2011.

¹⁰ (U) NIST SP 800-60, rev. 1, *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, Aug. 2008.

¹¹ (U) FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, Feb. 2004.

¹² (U) NIST SP 800-60, rev. 1, sec. C.3.5, *Information and Technology Management*.

¹³ (U) NIST SP 800-53, rev. 3, *Recommended Security Controls for Federal Information Systems*, CA-2 Security Assessments, Aug. 2009 (last updated May 2010).

¹⁴ (U) OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Section NIST Standards and Guidelines, April 2010.

- (U) BBG did not complete a Privacy Impact Assessment for its Privacy Information Enclave. OMB M-12-20¹⁵ states, “Although neither Section 208 of the E-Government Act, nor OMB’s implementing guidance mandate agencies conduct [privacy impact assessments] on electronic systems containing information about Federal employees (including contractors), OMB encourages agencies to scrutinize their internal business processes and the handling of identifiable information about employees to the same extent they scrutinize processes and information handling procedures involving information collected from or about members of the public (OMB Memorandum 03-22, Section ILB.3.a.)”

(U) According to a BBG management official, BBG had to focus on daily operations instead of devoting resources to implementing a risk management framework for its information systems. System Owners, Information Owners, and the CIO/CTO did not perform the data categorization for BBG’s systems. In addition, BBG management stated that the security authorization automated system caused inaccurate data elements to be transferred over to the security authorization packages. Finally, System Owners and the CIO/CTO used the outdated NIST SP 800-53, Revision 2,¹⁶ controls, instead of the most current NIST SP 800-53, Revision 3, controls, to conduct the security authorization process.

(U) Without a risk management program, BBG cannot prioritize, assess, respond to, and monitor information security risk, which leaves BBG vulnerable to outside attacks and insider threats.

(U) Recommendation 1. OIG recommends that the System Owners, Information Owners, and the Chief Information Officer/Chief Technology Officer assess the data categorization for information systems, in accordance with Federal Information Processing Standard 199, and implement the corresponding National Institute of Standards and Technology Special Publication 800-53, Revision (Rev.) 3, controls, if necessary.

(U) Management Response: BBG concurred with the recommendation, stating that it will ensure that all FISMA systems are properly categorized and have implemented all the necessary security controls provided in NIST SP 800-53, Revision 3.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that all FISMA systems are properly categorized and all necessary NIST SP 800-53, Revision 3, security controls are implemented.

(U) Recommendation 2. OIG recommends that the System Owners and Chief Information Officer/Chief Technology Officer prioritize resources to perform security impact analyses to assess the differences in National Institute of Standards and

¹⁵ (U) OMB Memorandum M-12-20, Sept. 27, 2012.

¹⁶ (U) NIST SP 800-53, rev. 2, *Recommended Security Controls for Federal Information Systems*, Dec. 2007.

Technology Special Publication 800-53, Revision 3, control families and their impact to the state of security on the systems and reauthorize the systems.

(U) Management Response: BBG concurred with the recommendation, stating that it will update Security Assessment Reports and Risk Assessment Reports for all BBG FISMA systems to ensure that all systems can be reauthorized.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that all FISMA system Security Assessment Reports and Risk Assessment Reports have been updated.

(U) Recommendation 3. OIG recommends that the Broadcasting Board of Governors prioritize resources to perform a privacy impact assessment for the Privacy Information Enclave in accordance with Office of Management and Budget Memorandum M-12-20.

(U) Management Response: BBG concurred with the recommendation, stating that the Chief Information Officer will prioritize resources to ensure that a privacy impact analysis is performed for the Privacy Information Enclave.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that a privacy impact analysis has been performed for the Privacy Information Enclave.

(U) Finding B. Continuous Monitoring Management

(U) NIST SP 800-137¹⁷ states, “Information security continuous monitoring is maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.”

(U) According to OMB¹⁸ guidance, “A well designed and well managed continuous monitoring program can effectively transform an otherwise static and occasional security control assessment and risk determination process into a dynamic process that provides essential, near real time security status related information” to senior leaders. Senior leaders can use this information to take “appropriate risk mitigation actions and make cost effective, risk based decisions regarding the operation of their information systems.”

(U) In FY 2013, OIG found that although the Office of the CIO/CTO was in the process of implementing a continuous monitoring program with the acquisition of automated tools for vulnerability assessment and patch management, they did not have an overall continuous monitoring program for the agency. Specifically, the continuous monitoring program did not

¹⁷ **(U)** NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, Executive Summary, Sept. 2011.

¹⁸ **(U)** OMB, *Fiscal Year 2010 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002*, sec. A. Continuous Monitoring and Remediation, March 2010.

address the assessment of selected security controls (including system-specific, hybrid, and common controls).

(U) According to NIST SP 800-53, Revision 3,¹⁹ the organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes a configuration management process, security impact analysis, ongoing security control assessment, and reporting the security state of the system to appropriate organizational officials.

(U) According to a BBG management official, the CIO/CTO in coordination with the Information Security Management Division had to focus on daily operations instead of prioritizing resources to implement a continuous monitoring program strategy. Therefore, the agency did not finalize an enterprise-wide continuous monitoring program strategy to assist system owners in evaluating various control deficiencies.

(U) Not having a robust continuous monitoring program prevents an organization from understanding the security state of the information system over time. It also prevents the organization from effectively monitoring a dynamic network environment with changing threats, vulnerabilities, technologies, missions, and business functions. Without a well-designed and well-managed continuous monitoring program, potential damage to the agency systems could occur which may result in system downtime, data manipulation/loss, or operational failure.

(U) Recommendation 4. OIG recommends that the Chief Information Officer/Chief Technology Officer, in coordination with the Information Security Management Division, finalize and implement an enterprise-wide continuous monitoring strategy that includes a continuous monitoring policy and assesses the security state of information systems in a manner consistent with Federal Information Security Management Act requirements, Office of Management and Budget policy, and applicable National Institute of Standards and Technology guidelines.

(U) Management Response: BBG concurred with the recommendation, stating that it is reviewing NIST SP 800-53, Revision 4, guidance and planned to implement the new features of the guidance in its continuous monitoring program, policies, and procedures. In addition, BBG stated that its participation in the Continuous Diagnostic Mitigation program sponsored by the Department of Homeland Security will strengthen its internal monitoring controls.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that BBG has implemented features of NIST SP 800-53, Revision 4, as it relates to its continuous monitoring program.

¹⁹ (U) NIST SP 800-53, rev. 3, CA-7 Continuous Monitoring.

(U) Finding C. Contingency Planning

(U) In FY 2010, FY 2011, and FY 2012, OIG reported that BBG did not develop and implement contingency planning and testing policies and procedures compliant with NIST requirements. Specifically, BBG did not complete its enterprise-wide and system-specific contingency plans or conduct contingency tests. NIST SP 800-34, Revision 1,²⁰ states, “contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods.”

(U) In FY 2013, OIG concluded that BBG had not developed an enterprise-wide and system-specific contingency plan or performed any contingency testing. According to NIST SP 800-34, Revision 1,²¹ the document defines the following seven-step contingency process that an agency may apply to develop and maintain a viable contingency planning program for BBG’s IT systems: “(a) develop a contingency planning policy statement, (b) conduct a business impact analysis, (c) identify preventive controls, (d) create contingency strategies, (e) develop an information system contingency plan, (f) ensure plan testing, training, exercises, and (g) ensure plan maintenance.” Also, according to NIST SP 800-53, Revision 3,²² the organization develops a contingency plan for the information system that: identifies essential missions and business functions and associated contingency requirements; provides recovery objectives, restoration priorities, and metrics; addresses contingency roles, responsibilities, assigned individuals with contact information; addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and is reviewed and approved by designated officials within the organization. According to NIST SP 800-53, Revision 3,²³ the organization “... tests and/or exercises the contingency plan for the information system.”

(U) According to a BBG management official, BBG’s Office of the CIO/CTO had to focus on daily operations instead of devoting resources to developing the contingency plans and testing for BBG information systems. However, 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. As a result, BBG may be unable to resume operations in an efficient and effective manner. BBG could not reconstitute operations if there was an extended outage and/or disaster.

(U) Recommendation 5. OIG recommends that the Chief Information Officer/Chief Technology Officer prioritize resources to complete entity-wide and system specific contingency planning documents for all information systems and conduct necessary

²⁰ (U) NIST SP 800-34, rev. 1, *Contingency Planning Guide for Federal Information Systems*, Executive Summary, May 2010.

²¹ (U) *Ibid.*, p. V.

²² (U) NIST SP 800-53, rev. 3, CP-1 Contingency Planning Policy and Procedures and CP-2 Contingency Plan.

²³ (U) *Ibid.*, CP-4 Contingency Planning Testing and Exercise.

testing in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, and NIST SP 800-53, Revision 3.

(U) Management Response: BBG concurred with the recommendation, stating that its Disaster Recovery and Business Continuity Manager will continue the development and planning of entity-wide and system specific contingency plans.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing a complete entity-wide contingency plan and system specific contingency plans and testing results.

(U) Finding D. Incident Response and Reporting

(U) In FY 2010, FY 2011, and FY 2012, OIG identified security incident program deficiencies in BBG's information security program. According to NIST SP 800-61, Revision 2,²⁴ incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services. In April 2013, BBG implemented RedMine as its primary incident tracking tool, which should increase detection, and reporting capabilities within the agency.

(U) In FY 2013, OIG noted that BBG did not have effective incident response and reporting. Specifically, BBG's Computer Security Incident Management Policy did not have all of the following components in its incident response life cycle:

- (U) Preparation.
- (U) Detection and Analysis.
- (U) Containment, Eradication and Recovery.
- (U) Post-Incident Activity.

(U) According to a BBG management official, BBG's Information Security Management Division had focused on daily operations instead of prioritizing resources to review a comprehensive incident response policy that was compliant with Federal regulations. According to NIST SP 800-61, Revision 2,²⁵ establishing an incident response capability should include the following actions:

- (U) Creating an incident response policy and plan.
- (U) Developing procedures for performing incident handling and reporting.
- (U) Setting guidelines for communicating with outside parties regarding incidents.
- (U) Selecting a team structure and staffing model.

²⁴ (U) NIST SP 800-61, rev. 2, *Computer Security Incident Handling Guide*, Executive Summary, Aug. 2012.

²⁵ (U) *Ibid.*

- (U) Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies).
- (U) Determining what services the incident response team should provide.

(U) BBG may not be detecting, identifying, containing, eradicating, and recovering from security incidents. Lack of incident response and reporting could result in a shutdown of BBG information systems, which would affect its operational mission.

(U) Recommendation 6. OIG recommends that the Information Security Management Division update and implement its incident response policy in accordance with National Institute of Standards and Technology Special Publication 800-61, Revision 2.

(U) Management Response: BBG concurred with the recommendation, stating that it will update and implement the incident response policy.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that BBG's incident response policy has been updated and implemented in accordance with NIST SP 800-61, Revision 2.

(U) Finding E. Plans of Action and Milestones

(U) In FY 2010, FY 2011, and FY 2012, OIG identified POA&M deficiencies in BBG's information security program. In FY 2013, OIG found that POA&M entries were not fully completed. According to NIST SP 800-64, Revision 2,²⁶

(U) A POA&M is "A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems."

(U) BBG's Office of the CIO/CTO had a deficient POA&M process. BBG failed to adhere to its own policy²⁷ of completing all the necessary elements of a POA&M. OIG found that for five of five (100 percent) systems tested in the POA&M database, BBG did not adequately assign resources (including resource hours), add expected time for completion or add milestone completion dates to remediate the security weaknesses and severity ratings for each corrective action (i.e., significant deficiency, reportable condition, or other).

(U) According to a BBG management official, BBG's Office of the CIO/CTO had to focus on daily operations instead of devoting resources to adhere to its POA&M policy.

²⁶ (U) NIST SP 800-64, rev. 2, *Security Considerations in the System Development Life Cycle*, Oct. 2008.

²⁷ (U) *Information Security Plan of Action and Milestone (POA&M) Policy*, May 2, 2010 (last updated Feb. 9, 2012).

(U) BBG management will not have an accurate account of all system vulnerabilities, nor will it be able to adequately prioritize resources to remediate identified vulnerabilities. As a result, delays in the implementation of corrective actions may persist and leave information systems vulnerable to outside attacks and insider threats.

(U) Recommendation 7. OIG recommends the Chief Information Officer/Chief Technology Officer ensure that Broadcasting Board of Governors Plans of Action and Milestones (POA&M) include all required elements in accordance with its Information Security POA&M Policy, to include severity of the weakness, responsible organization, estimated funding resources, completion date, key milestones and changes, source of the weakness, and the status.

(U) Management Response: BBG concurred with the recommendation, stating that the Chief Information Officer will update the elements within their POA&M tracking sheet in an ongoing effort to improve internal information technology project governance.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that BBG has updated its POA&M tracking sheet with the required elements.

(U) Finding F. Remote Access Management

(U) In FY 2010, FY 2011, and FY 2012, OIG identified remote access deficiencies in BBG's information security program. BBG's remote access Virtual Private Network (VPN) agreement allows users to access the BBG network using personally owned computers. In addition, the VPN Agreement requires each user to have anti-virus software with up-to-date virus definitions. Additionally, BBG had not implemented procedures to ensure that remote access was granted only to computers that have proper security safeguards. According to OMB M-06-16,²⁸ the agency owned mobile computers use multifactor authentication and hard drive encryption to compensate for the lack of physical security controls when information is removed from or accessed from outside the BBG location. According to NIST SP 800-53, Revision 3,²⁹ "Multifactor authentication is authentication using two or more factors to achieve authentication. Factors include: (i) something you know; (ii) something you have; or (iii) something you are."

(U) The Enterprise Networks and Storage Division, under the Office of the CIO/CTO, had not implemented procedures to ensure that remote access was granted only to computers that have security safeguards that comply with BBG's policies and procedures.

(U) From a sample of 25 remote users tested, we identified the following deficiencies:

- (U) One user did not have an appropriate access authorization form completed.
- (U) Four users did not sign rules of behavior agreement form prior to gaining remote access.

²⁸ (U) OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006.

²⁹ (U) NIST SP 800-53, rev. 3, app. B, Glossary.

(U) According to a BBG management official, BBG's Enterprise Networks and Storage Division, under the Office of the CIO/CTO, had to focus on daily operations instead of devoting resources to implement remote access controls. In addition, BBG did not consider the information stored on removable media to be sensitive.

(U) BBG's VPN Agreement states, "By using VPN technology with personal equipment, users must understand that their computers are a de facto extension of the BBG network and subject to the same rules and regulations that apply to BBG-owned equipment, i.e., their computers must be configured to comply with BBG security requirements." The agreement further states, "All computers connected to the BBG network via VPN must use up-to-date virus-scan and virus definitions." According to NIST SP 800-53, Revision 3,³⁰

(U) "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."

(U) Without 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. The risks of introducing viruses, worms, or other malicious code into BBG's enterprise network are increased significantly resulting in a potential loss of data and/or compromise of agency systems. Weak remote access controls could allow hackers access to the network and insider threats could not be uniquely identified resulting in data spillage or system destruction.

(U) Recommendation 8. OIG recommends that the Enterprise Networks and Storage Division, under the Office of the Chief Information Officer/Chief Technology Officer, implement procedures to assess the adequacy of the security configurations of mobile computers that request access to the Broadcasting Board of Governors network and grant access only to properly configured and patched devices in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) Management Response: BBG concurred with the recommendation, stating that it had acquired a network access control management tool and configuration of the tool is pending.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that that the network access control management tool had been configured and implemented.

³⁰ (U) Ibid., AC-17 Remote Access.

(U) Finding G. Configuration Management

(U) OIG first reported in FY 2010 that BBG had not completed the development of procedures that govern routine and critical security configuration management processes. According to NIST SP 800-128,³¹

(U) “Configuration management comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.” Further, security-focused configuration management “... is the management and control of secure configurations for an information system to enable security and facilitate the management of risk.”³²

(U) In FY 2013, BBG implemented an entity-wide software deployment policy to strengthen its configuration management process. However, BBG was still in the process of gathering system information for the development of its standard security baseline configurations. [Redacted] (b) (5)

[Redacted] (b) (5)

(U) NIST SP 800-53, Revision 3,³³ states that the organization establishes and documents mandatory configuration settings for information technology products employed within the information system using organization-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements; and identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements. NIST SP 800-53, Revision 3,³⁴ also states, the organization identifies, reports, and corrects information system flaws.

(U) According to a BBG management official, BBG’s IT management had to focus on daily operations instead of devoting resources to developing procedures and guidance for configuration management processes. OIG’s vulnerability assessment was conducted at a time

³¹ (U) NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, 2.1.1, Aug. 2011.

³² (U) *Ibid.*, 2.1.3.

³³ (U) NIST SP 800-53, rev. 3, CM-6 Configuration Settings.

³⁴ (U) *Ibid.*, SI-2 Flaw Remediation.

when BBG was switching patching tools. [Redacted] (b) (5)

(U) Without proper implementation of policy and procedures that govern the performance of routine and critical processes, BBG leaves its systems vulnerable to the denial of service, damage to the general support system, or the potential introduction of security weaknesses. Potential damage to BBG systems could occur, which may result in system downtime, data manipulation/loss, or operational failure.

(U) Recommendation 9. OIG recommends that the Chief Information Officer/Chief Technology Officer verify that U.S. Government Configuration Baseline configuration standards are implemented and compliance with the implemented standards is periodically assessed in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) Management Response: BBG concurred with the recommendation, stating that it planned to use monitoring technology made available through the Department of Homeland Security's Continuous Diagnostic Mitigation program to verify the implementation and compliance of configuration standards in accordance with NIST SP 800-53, Revision 3.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that BBG has implemented U.S. Government Configuration Baseline standards and periodic compliance assessment is performed.

(U) Recommendation 10. OIG recommends that the Chief Information Officer/Chief Technology Officer follow the Broadcasting Board of Governors Change Management Policy, to "test and disseminate Microsoft operating system and application patches released on the second Tuesday of each month in a way that ensures complete coverage of workstations and laptops while avoiding operational downtime by rigorously testing the patches prior to general release to ensure application compatibility and seamless functionality."

(U) Management Response: BBG concurred with the recommendation, stating that it planned to use monitoring technology made available through the Department of Homeland Security's Continuous Diagnostic Mitigation program to address the monthly vulnerabilities on workstations and servers.

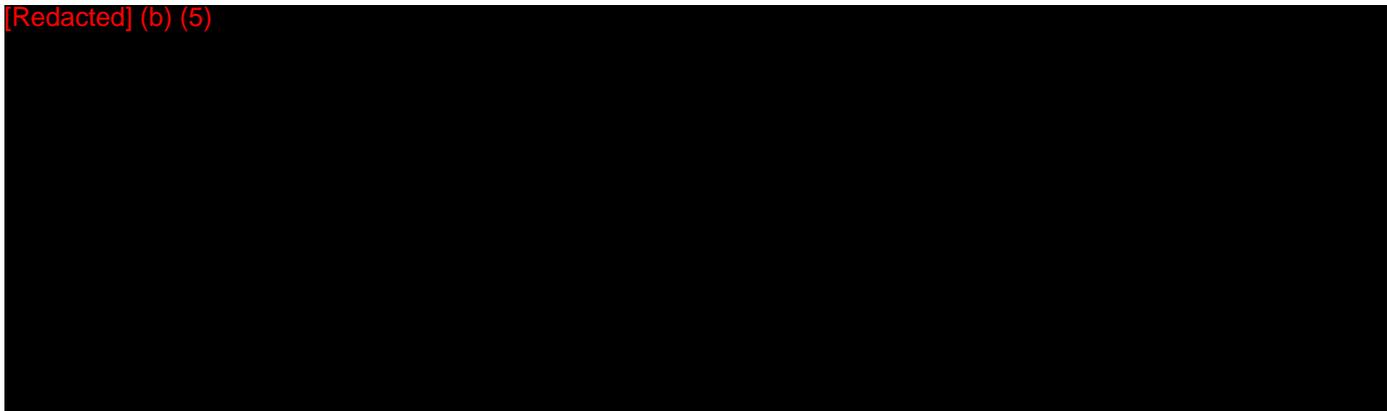
(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that critical patches have been implemented to address operating system and application vulnerabilities.

(U) Finding H. Identity and Access Management

(U) In FY 2010, FY 2011, and FY 2012, OIG identified deficiencies in BBG's identity and access management of Active Directory accounts. Identification and authentication is typically the first line of defense and used as a technical measure to prevent unauthorized access to systems. Homeland Security Presidential Directive 12³⁵ is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). The Office of Cuba Broadcasting accounts were not included in our test review because of migration to the Microsoft Office 365 email system. These accounts were segregated by BBG and undergoing maintenance due to the migration.

(U) In FY 2013, OIG found that although BBG had made significant improvements of managing its Active Directory accounts, they still did not have effective identity and access management of their information systems. Specifically, in FY 2013, excluding all accounts undergoing migration at Office of Cuba Broadcasting, we observed the following control deficiencies that had not been addressed by BBG's System Owners:

[Redacted] (b) (5)



(U) Although the control deficiencies identified are minor in scale, they should be promptly addressed because the weakest security point is where BBG is vulnerable to attack. BBG management should develop a process that considers the identified Active Directory vulnerabilities when developing or updating its identity and access management strategy and policy.

(U) In addition, only 65 of 2,280 (3 percent) employees and contractors were issued Personal Identity Verification (PIV) cards as of March 2013.

(U) According to the BBG's Identification and Authentication Policy and Password Policy, system owners are responsible for implementing the policy and procedures for their IT systems, including:

³⁵ (U) HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, Aug. 27, 2004.

- (U) Monitoring and taking actions to create and delete accounts.
- (U) Creating processes to change user account passwords every 90 days.
- (U) Creating processes to disable separating/terminating user accounts within 24 hours of notification, and removing these disabled accounts within a week of notification, unless the Security Manager determines that removing the disabled account would adversely affect operations.
- (U) Creating processes to review, quarterly, the use of guest, test, and shared accounts, and report such accounts and their justification to the Chief Information Security Officer. Unneeded accounts shall be disabled and/or deleted whenever possible.

(U) Homeland Security Presidential Directive 12³⁶ mandates a Federal standard for secure and reliable forms of identification. According to item four of the directive, the heads of executive departments and agencies shall "require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems."

(U) System Owners did not utilize their resources to update Active Directory user accounts based on the results from the bi-weekly automated script. In addition, PIV cards were not put in place because BBG purchased a Commercial Off the Shelf product in 2006 that was not compatible with their legacy security system until March 2013, which prevented the use of PIV cards within the agency.

(U) Without effective identity and access management, the risk of unauthorized access is significantly increased. Unauthorized access may result in the submission of false transactions, improper access to and dissemination of confidential data, and other malicious activities. Passwords can be easily hacked resulting in unauthorized access of BBG's information systems.

(U) Recommendation 11. OIG recommends that the Chief Information Officer/Chief Technology Officer and System Owners ensure that user accounts are properly maintained in accordance with Broadcasting Board of Governors (BBG) Identification and Authentication Policy and the BBG/IBB/VOA Password Policy.

(U) Management Response: BBG concurred with the recommendation, stating that the Chief Information Officer and System Owners will work together to strengthen information technology processes for managing user accounts to ensure that accounts are effectively managed in accordance with BBG's policies.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that accounts are effectively managed in accordance with BBG's policies.

(U) Recommendation 12. OIG recommends that the Office of Security, in coordination with the Chief Information Officer/Chief Technology Officer, complete the issuance of

³⁶ (U) Ibid.

Personal Identity Verification cards as required by Homeland Security Presidential Directive 12.

(U) Management Response: BBG concurred with the recommendation, stating that it will accelerate issuance of Personal Identification Verification cards to employees and contractors as much as practical within budget constraints. The Chief Information Officer will continue to assess progress and develop extensions into logical access control.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that the Office of Security has completed the issuance of Personal Identification Verification cards to employees and contractors.

(U) Finding I. Security Training and Awareness

(U) In FY 2013, OIG found that although BBG had made progress over the past two years to bring Security Awareness training compliance from 25 percent to 100 percent in FY 2013, it still did not have a policy for role-based training. NIST 800-16³⁷ states, “Federal agencies and organizations cannot protect the integrity, confidentiality, and availability of information in today’s highly networked systems environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them.”

(U) Although the Information Security Management Division revised its security awareness-training program in July 2012 to include both online and in-person training, it did not have a policy for role-based training. Therefore, key IT personnel with security responsibilities had not taken specialized role-based security training. According to NIST SP 800-53, Revision 3,³⁸ the organization provides role-based security-related training before authorizing access to the system or performing assigned duties and the frequency of training thereafter is organizationally-defined.

(U) According to a BBG management official, BBG’s Information Security Management Division had to focus on daily operations instead of devoting resources to developing a policy and ensuring key personnel with security responsibilities receive adequate role-based (specialized) training.

(U) Without the completion of role-based annual security training, IT and security personnel may be unaware of new risks that may compromise the confidentiality, integrity, and availability of data. Users could compromise the security of the network resulting in a loss of operations, compromise of Personally Identifiable Information and introduction of vulnerabilities to the system.

³⁷ (U) NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, sec. 1.1, Apr. 1998.

³⁸ (U) NIST SP 800-53, rev. 3, AT-3.

(U) Recommendation 13. OIG recommends that the Information Security Management Division, in coordination with the Chief Information Officer/Chief Technology Officer, prioritize resources to develop and implement a role-based security training program in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) Management Response: BBG concurred with the recommendation, stating that it will take steps to develop and implement a role-based information technology security program in accordance with NIST Guidance.

(U) OIG Analysis: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts documentation or evidence showing that BBG has implemented a role-based information technology security program.

(U) Finding J. Compliance with Federal Information Security Management Act Requirements

(U) In FY 2013, OIG found that BBG was in compliance with the Capital Planning and Contractor System requirements. There were no prior year weaknesses that carried over to FY 2013 for these two areas.

(U) For Contractor Systems, we noted that the agency had 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 agency.

(U) For Capital Planning, there have been no major IT investments or capital investments funding for the year. However, OIG suggests the Chief Information Officer/Chief Technology Officer implement processes and procedures to cross-reference POA&M information, including costs, to the capital planning budget process with a Unique Investment Identifier for any future IT acquisitions.

(U) List of Current Year Recommendations

(U) Recommendation 1. OIG recommends that the System Owners, Information Owners, and the Chief Information Officer/Chief Technology Officer assess the data categorization for information systems, in accordance with Federal Information Processing Standard 199, and implement the corresponding National Institute of Standards and Technology Special Publication 800-53, Revision 3, controls, if necessary.

(U) Recommendation 2. OIG recommends that the System Owners and Chief Information Officer/Chief Technology Officer prioritize resources to perform security impact analyses to assess the differences in National Institute of Standards and Technology Special Publication 800-53, Revision 3, control families and their impact to the state of security on the systems and reauthorize the systems.

(U) Recommendation 3. OIG recommends that the Broadcasting Board of Governors prioritize resources to perform a privacy impact assessment for the Privacy Information Enclave in accordance with Office of Management and Budget Memorandum M-12-20.

(U) Recommendation 4. OIG recommends that the Chief Information Officer/Chief Technology Officer, in coordination with the Information Security Management Division, finalize and implement an enterprise-wide continuous monitoring strategy that includes a continuous monitoring policy and assesses the security state of information systems in a manner consistent with Federal Information Security Management Act requirements, Office of Management and Budget policy, and applicable National Institute of Standards and Technology guidelines.

(U) Recommendation 5. OIG recommends that the Chief Information Officer/Chief Technology Officer prioritize resources to complete entity-wide and system specific contingency planning documents for all information systems and conduct necessary testing in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, and NIST SP 800-53, Revision 3.

(U) Recommendation 6. OIG recommends that the Information Security Management Division update and implement its incident response policy in accordance with National Institute of Standards and Technology Special Publication 800-61, Revision 2.

(U) Recommendation 7. OIG recommends the Chief Information Officer/Chief Technology Officer ensure that Broadcasting Board of Governors Plans of Action and Milestones (POA&M) include all required elements in accordance with its Information Security POA&M Policy, to include severity of the weakness, responsible organization, estimated funding resources, completion date, key milestones and changes, source of the weakness, and the status.

(U) Recommendation 8. OIG recommends that the Enterprise Networks and Storage Division, under the Office of the Chief Information Officer/Chief Technology Officer, implement procedures to assess the adequacy of the security configurations of mobile

computers that request access to the Broadcasting Board of Governors network and grant access only to properly configured and patched devices in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) Recommendation 9. OIG recommends that the Chief Information Officer/Chief Technology Officer verify that U.S. Government Configuration Baseline configuration standards are implemented and compliance with the implemented standards is periodically assessed in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) Recommendation 10. OIG recommends that the Chief Information Officer/Chief Technology Officer follow the Broadcasting Board of Governors Change Management Policy, to “test and disseminate Microsoft operating system and application patches released on the second Tuesday of each month in a way that ensures complete coverage of workstations and laptops while avoiding operational downtime by rigorously testing the patches prior to general release to ensure application compatibility and seamless functionality.”

(U) Recommendation 11. OIG recommends that the Chief Information Officer/Chief Technology Officer and System Owners ensure that user accounts are properly maintained in accordance with Broadcasting Board of Governors (BBG) Identification and Authentication Policy and the BBG/IBB/VOA Password Policy.

(U) Recommendation 12. OIG recommends that the Office of Security, in coordination with the Chief Information Officer/Chief Technology Officer, complete the issuance of Personal Identity Verification cards as required by Homeland Security Presidential Directive 12.

(U) Recommendation 13. OIG recommends that the Information Security Management Division, in coordination with the Chief Information Officer/Chief Technology Officer, prioritize resources to develop and implement a role-based security training program in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) Scope and Methodology

(U) 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-DC, 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 2013.

(U) 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).² DHS uses this data to assist in oversight responsibilities and to prepare its annual report to Congress regarding agency compliance with FISMA.

(U) We conducted the audit from April 2013 through September 2013. In addition, we performed the audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), FISMA, OMB, and National Institute of Standards and Technology (NIST) guidance. GAGAS require 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

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

- (U) DHS Inspector General FISMA Reporting Metrics.³
- (U) OMB Memoranda M-02-01, M-04-04, M-06-19, and M-12-20.⁴

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

² (U) OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and Department of Homeland Security (DHS)* July 6, 2010.

³ (U) Department of Homeland Security’s *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*, dated Nov. 30, 2012.

⁴ (U) 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; OMB Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Sept. 27, 2012.

- (U) BBG policies and procedures, such as the BBG *Computer Security Incident Management Policy*.
- (U) Federal laws, regulations, and standards, such as FISMA and those contained in OMB Circular No. A-130, Revised,⁵ and OMB Circular No. A-11.⁶
- (U) NIST Special Publications, Federal Information Systems Processing Publications (FIPS), other applicable NIST publications, and industry best practices.

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

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

(U) The audit covered the period October 1, 2012, to September 30, 2013. During the fieldwork, we took the following actions:

- (U) 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.
- (U) 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 2013 Inspector General Federal Information Security Management Act Reporting Metrics*, dated November 30, 2012.
- (U) Assessed programs for monitoring of security policy and program compliance and responding to security events, e.g., unauthorized changes detected by intrusion detection systems.
- (U) Assessed the adequacy of internal controls related to the areas reviewed. Control deficiencies identified during the review are included in this report.

⁵ (U) OMB Circular No. A-130, Revised, *Management of Federal Information Resources*, app. III, Security of Federal Automated Information Resources, Nov. 30, 2000.

⁶ (U) OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, Aug. 2011.

- (U) Evaluated BBG's remedial actions taken to address the previously reported information security program control weaknesses identified in OIG's *Audit of the Broadcasting Board of Governors Information Security Program* (AUD/IT/IB-13-04, Nov. 2012).

(U) Review of Internal Controls

(U) We reviewed BBG's internal controls to determine whether:

- (U) The agency had established an enterprise-wide continuous monitoring program that assessed the security state of information systems that were consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The agency had established and was maintaining a security configuration management program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The agency had established and was maintaining an account and identity management program that was generally consistent FISMA requirements, OMB policy, and applicable NIST guidelines and which identified users and network devices.
- (U) The agency had established and was maintaining an incident response and reporting program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The agency established a risk management program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The agency had established and was maintaining a security training program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The agency had established a POA&M program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracked and monitored known information security weaknesses.
- (U) The agency had established and was maintaining a remote access program that was generally consistent with NIST's and OMB's FISMA requirements.
- (U) The agency established and was maintaining an entity-wide business continuity/disaster recovery program that was generally consistent with NIST's and OMB's FISMA requirements.
- (U) The agency had established a program to oversee systems operated on its behalf by contractors or other entities, including agency systems and services residing in the cloud external to the agency.
- (U) The agency had established and maintained a capital planning and investment program for information security.

(U) Use of Computer-Processed Data

(U) 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.

(U) Sampling Methodology

(U) Generally, for a population of sample items, we used judgmental sampling to test 10 percent of the population or 25, whichever is less. The 10 percent guidance is based on 10 percent of a population of 250, which equals 25. Based on the internal control structure at BBG, we determined that the planned assessed level of control risk was MODERATE.

(U) Followup of Recommendations from the FY 2012 Audit of the Broadcasting Board of Governors Information Security Program

(U) The audit team reviewed actions implemented by management to mitigate the findings identified in the FY 2012 audit of the Broadcasting Board of Governors (BBG) information security program. The current status of each of the recommendations follows:

(U) 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.

(U) Status: Closed from FY 2012 report; this repeat recommendation has become Recommendation 10 (Finding G) in the FY 2013 report.

(U) 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.

(U) Status: Closed. The Certification and Accreditation Policy and Procedures were revised in April 2013 to designate BBG's Chief Information Officer as the Certifying Official for all Agency Information Systems. Also, the Certification and Accreditation (C&A) Policy and Procedures designate the CIO as the accrediting official for all agency systems.

(U) 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.

(U) Status: Closed from FY 2012 report; this repeat recommendation has become Recommendation 12 (Finding H) in the FY 2013 report.

(U) 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.

(U) Status: Closed. We reviewed the security incidents to ensure that they were properly reported to US-CERT.

(U) 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.

(U) Status: Closed. BBG developed a formal sanction process to disable user accounts for users who had not taken the Cyber Security Awareness training by the final due date. We inspected a sample of users, without exceptions, for the FY 2013 Cyber Security Awareness training to ensure that they had taken their training by the due date.

(U) 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.

(U) Status: Closed from FY 2012 report; this repeat recommendation has become Recommendation 7 (Finding E) in the FY 2013 report.

(U) 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.

(U) Status: Closed from FY 2012 report; this repeat recommendation has become Recommendation 8 (Finding F) in the FY 2013 report.

(U) 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.

(U) Status: Closed. A full implementation of BBG's system inventory has been completed for the agency within the FootPrints application at BBG. We compared the BBG FISMA Information Systems and Accreditation Boundaries within the agency with the current list of systems provided by BBG and noted no discrepancies.

(U) 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.

(U) Status: Closed from FY 2012 report; this repeat recommendation has become Recommendation 5 (Finding C) in the FY 2013 report.



Broadcasting Board of Governors
THE DIRECTOR OF THE
U.S. INTERNATIONAL BROADCASTING BUREAU

October 10, 2013

Mr. Steve A. Linick
Inspector General
Department of State

Dear Mr. Linick:

This is in response to the Office of Inspector General (OIG) draft report titled "Audit of the Broadcasting Board of Governors Information Security Program", Report Number AUD-IT-IB-13-XX issued September 2013.

The Broadcasting Board of Governors (BBG) has reviewed the report and provides its concurrence to all recommendations 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. Carol Prahl at (202) 203-^{(b) (2), (Redacted) (b) (6)} or Ms. Kelu Chao, Director, IBB Office of Performance Review at (202) 203-^{(b) (2), (Redacted) (b) (6)}.

Sincerely,

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

Richard M. Lobo
Director

Enclosure: As Stated

Enclosure

**BBG's Response to OIG's "Audit of the Broadcasting Board of Governors Information Security Program,"
Report Number AUD-IT-IB-13-XX, September 2013**

Recommendation 1: OIG recommends that the System Owners, Information Owners, and the Chief Information Officer/Chief Technology Officer assess the data categorization for information systems, in accordance with Federal Information Processing Standard 199, and implement the corresponding National Institute of Standards and Technology Special Publication 800-53, Revision 3, controls, if necessary.

TSI Response (October 11, 2013): BBG concurs. The BBG will work to ensure all FISMA systems are properly categorized and have implemented all the necessary security controls as provided in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3.

Recommendation 2: OIG recommends that the System Owners and Chief Information Officer/Chief Technology Officer prioritize resources to perform security impact analyses to assess the differences in National Institute of Standards and Technology Special Publication 800-53, Revision 3, control families and their impact to the state of security on the systems and reauthorize the systems.

TSI Response (October 11, 2013): BBG concurs. The BBG will update Security Assessment Reports and Risk Assessment Reports for all BBG FISMA systems to ensure that all systems can be reauthorized per OIG's recommendation.

Recommendation 3: OIG recommends that the Broadcasting Board of Governors prioritize resources to perform a privacy impact assessment for the Privacy Information Enclave in accordance with Office of Management and Budget Memorandum M-12-20.

TSI Response (October 11, 2013): BBG concurs. The CIO will prioritize resources to ensure this privacy impact analysis is completed.

Recommendation 4: OIG recommends that the Chief Information Officer/Chief Technology Officer, in coordination with the Information Security Management Division, finalize and implement an enterprise-wide continuous monitoring strategy that includes a continuous monitoring policy and assesses the security state of information systems in a manner consistent with Federal Information Security Management Act requirements, Office of Management and Budget policy, and applicable National Institute of Standards and Technology guidelines.

TSI Response (October 11, 2013): BBG concurs. The Agency is reviewing the recently released NIST 800-53 Revision 4 guidance and plans to implement the new features and flexibility of this guidance in BBG's continuous monitoring program, policies, and procedures. In addition, BBG is participating in the Continuous Diagnostic Mitigation

(CDM) program sponsored by the Department of Homeland Security (DHS). The BBG feels the CDM program will strengthen the BBG's internal monitoring controls.

Recommendation 5: OIG recommends that the Chief Information Officer/Chief Technology Officer prioritize resources to complete entity-wide and system specific contingency planning documents for all information systems, and conduct necessary testing in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, and NIST SP 800-53, Revision 3.

TSI Response (October 11, 2013): BBG concurs. The BBG's Disaster Recovery and Business Continuity Manager will continue with policy development and planning to address deficiencies. The CIO will continue to monitor progress with draft policies and procedures.

Recommendation 6: OIG recommends that the Information Security Management Division update and implement its incident response policy in accordance with National Institute of Standards and Technology Special Publication 800-61, Revision 2.

TSI Response (October 11, 2013): BBG concurs. The CIO will continue to expand on its policies and workflows to implement its current policies.

Recommendation 7: OIG recommends the Chief Information Officer/Chief Technology Officer ensure that Broadcasting Board of Governors Plan of Action and Milestones (POA&M) include all required elements in accordance with its Information Security POA&M Policy, to include severity of the weakness, responsible organization, estimated funding resources, completion date, key milestones and changes, source of the weakness, and the status.

TSI Response (October 11, 2013): BBG concurs. The CIO will expand on the data elements contained in the POA&M tracking sheet as efforts continue to mature the internal IT project governance.

Recommendation 8: OIG recommends that the Enterprise Networks and Storage Division, under the Office of the Chief Information Officer/Chief Technology Officer, implement procedures to assess the adequacy of the security configurations of mobile computers that request access to the Broadcasting Board of Governors network and grant access only to properly configured and patched devices in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

TSI Response (October 11, 2013): BBG concurs. The BBG has acquired a network access control management tools and configuration / implementation of this tool is pending.

Recommendation 9: OIG recommends that the Chief Information Officer/Chief Technology Officer verify that U.S. Government Configuration Baseline configuration standards are implemented and compliance with the implemented standards is periodically assessed in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

TSI Response (October 11, 2013): BBG concurs. BBG plans to use the monitoring technology made available through DHS's CDM program to verify implementation and compliance of configuration standards in accordance with NIST Special Publication 800-53, Revision 3.

Recommendation 10: OIG recommends that the Chief Information Officer/Chief Technology Officer follow the Broadcasting Board of Governors Change Management Policy, to "test and disseminate Microsoft operating system and application patches released on the second Tuesday of each month in a way that ensures complete coverage of workstations and laptops while avoiding operational downtime by rigorously testing the patches prior to general release to ensure application compatibility and seamless functionality."

TSI Response (October 11, 2013): BBG concurs. BBG plans to use the same DHS monitoring technology referred to in response to OIG recommendation #9 to address the monthly vulnerability in the agency's workstations and servers.

Recommendation 11: OIG recommends that the Chief Information Officer/Chief Technology Officer and system owners ensure that user accounts are properly maintained in accordance with Broadcasting Board of Governors (BBG) Identification and Authentication Policy and the BBG/IBB/VOA Password Policy.

TSI Response (October 11, 2013): BBG concurs. The CIO and system owners will review and strengthen IT processes that manage user accounts in accordance with BBG policies. BBG expects that these strengthened processes will eliminate the small number of account violations that still exist.

Recommendation 12: OIG recommends that the Office of Security, in coordination with the Chief Information Officer/Chief Technology Officer, complete the issuance of Personal Identity Verification cards as required by Homeland Security Presidential Directive 12.

TSI Response (October 11, 2013): BBG concurs. The BBG agrees to accelerate issuance of PIV cards to its employees and contractors as much as practical within the budget constraints imposed on the Agency. The CIO will continue to assess progress and develop extensions into logical access control for the Agency.

Recommendation 13: OIG recommends that the Information Security Management Division, in coordination with the Chief Information Officer/Chief Technology Officer, prioritize resources to develop and implement a role-based security training program in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

TSI Response (October 11, 2013): BBG concurs. The CIO will take steps to develop and implement a role-based IT security program, within budgetary limitations, in accordance with NIST guidance, during FY 2014.



**FRAUD, WASTE, ABUSE,
OR MISMANAGEMENT
OF FEDERAL PROGRAMS
HURTS EVERYONE.**

CONTACT THE
OFFICE OF INSPECTOR GENERAL
HOTLINE
TO REPORT ILLEGAL
OR WASTEFUL ACTIVITIES:

202-647-3320
800-409-9926
oighotline@state.gov
oig.state.gov

Office of Inspector General
U.S. Department of State
P.O. Box 9778
Arlington, VA 22219