

UNCLASSIFIED

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

Office of Audits

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

Report Number AUD/IT-10-09, November 2009

~~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 was prepared by the Office of Inspector General (OIG) 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 by OIG periodically as part of its responsibility to promote effective management, accountability and positive change in the Department of State and the Broadcasting Board of Governors.

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

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

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

A handwritten signature in black ink, appearing to read "H. W. Geisel", written in a cursive style.

Harold W. Geisel
Acting Inspector General

UNCLASSIFIED

TABLE OF CONTENTS

Section	Page
EXECUTIVE SUMMARY	1
BACKGROUND	3
OBJECTIVE	5
RESULTS OF 2009 FISMA REVIEW	7
All Systems Were Not Certified and Accredited	7
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)	
(b) (2)	9
All Employees and Contractors Did Not Take the Security Awareness Training Course	10
Configuration Management Policies Were Developed and Published	12
Inventory Management Policies Were Developed and Implemented	13
Information Security Incident Response Plan Was Updated and Implemented	13
Privacy Program Has Improved	15
LIST OF RECOMMENDATIONS	17
ABBREVIATIONS	19
APPENDICES	
A. Scope and Methodology	21
B. Follow-up of Recommendations From the FY 2008 FISMA Report	23
C. Broadcasting Board of Governors Response	25

EXECUTIVE SUMMARY

In response to the Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. § 3545 et seq.), the review team performed an annual independent evaluation of the information security program at the Broadcasting Board of Governors (BBG). The review team reviewed BBG's progress in addressing FISMA information management and information security program requirements per FISMA and other statutory requirements, including Office of Management and Budget (OMB) guidance. The review team assessed performance in various areas, including certification and accreditation (C&A), plans of action and milestones (POA&M), security awareness and training, configuration management, inventory, incident reporting, and privacy requirements. Since FY 2008, BBG has taken steps to improve management controls, which include the following:

- Developed configuration management policies.
- Improved the identification and management of inventory systems using Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- Updated and implemented its Information Security Incident Response Plan to include Breach Notification Policy and Incident Management Policies.
- Improved implementation of privacy programs, including the development and implementation of privacy awareness training for all Federal employees and contractors.

However, further improvements are needed. Specifically, BBG should take the following actions:

- Develop policies and procedures for C&A, and conduct C&A on all seven of its "moderate-level" systems as categorized in FIPS Publication 199. This C&A testing includes the development of a system security plan for all systems and testing and monitoring the effectiveness of the information security policies, procedures, practices, and security controls on an ongoing basis with the frequency based on risk, but no less than annually.
- Ensure that all weaknesses that are identified during reviews, including C&A, and that require remediation are tracked in BBG's POA&M system, and cre-

ate and implement POA&M policies and processes that are in compliance with OMB guidelines and National Institute of Standards and Technology recommendations. Additionally, BBG should ensure that milestones include reasonable scheduled completion dates, timely tasks, and progress steps. BBG should also require that each identified weakness include the estimated cost to remediate and that these estimates, along with the severity of the weakness, be used to prioritize the weakness for timely correction.

- Require all Federal employees and contractors to take the security awareness training before they are granted log-in privileges to the system, offer the training on a regular basis and monitor employees' compliance, and develop security awareness policy that makes the course mandatory per OMB guidance.

Management Comments

BBG management concurred with all three of the report's recommendations.

For recommendation 1, BBG stated that it would conduct C&A testing on the three systems it determined had the "highest priority" by the end of the third calendar quarter of 2010 and develop systems security plans for the remaining eight "lower priority" systems by the end of the fourth quarter of 2010. For recommendation 2, BBG stated that it will track all weaknesses and create reasonable milestones, prioritize the weaknesses, and remediate the weaknesses on a timely basis. For recommendation 3, BBG stated that it will require all of its new employees and contractors to take the security awareness training course either before access is granted or immediately afterwards and that they take the course annually. BBG also stated that it will offer the training course on a "24/7 basis" instead of just 2 months out of the year. It further stated that it will monitor compliance with the information security awareness policy that it plans to develop and publish by the end of the second calendar quarter of 2010.

Although BBG management concurred with recommendation 1, it did not fully address the intent of the recommendation. However, taking into consideration possible budgetary and time constraints, the Office of Inspector General (OIG) has modified the recommendation and requests that BBG respond to the new recommendation (see recommendation 1 in section "All Systems Were Not Certified and Accredited").

Based on its response, OIG considers recommendation 1 unresolved and recommendations 2 and 3 resolved, pending further action. BBG's response is presented in its entirety as Appendix C.

BACKGROUND

Federal Information Security Management Act

The Federal Information Security Management Act of 2002 (FISMA), contained within the E-Government Act of 2002,¹ recognized the importance of information security to the economic and national security interests of the United States. It 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, contractor, or other source. FISMA 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.

FISMA assigns specific responsibilities to Federal agencies, the National Institute of Standards and Technology (NIST), and OMB in order to strengthen information system security. 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 security controls, FISMA requires agency program officials, Chief Information Officers (CIO), Senior Agency Officials for Privacy, and Inspectors General to conduct annual reviews of the agency's information security program and report the results to OMB.

Annually, OMB provides guidance with reporting categories and questions for meeting the current year's reporting requirements. OMB uses this data to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with FISMA.

¹ Pub. L. No. 107-347

UNCLASSIFIED

UNCLASSIFIED

OBJECTIVE

In accordance with FISMA, OIG initiated an annual review of BBG information security program and practices as related to FISMA.

The objective of the review was to evaluate the progress BBG had made in implementing an effective information security program and related practices since the last OIG annual FISMA review in FY 2008 (*Review of the Information Security Program at the Broadcasting Board of Governors* (AUD/IT-08-37, Oct. 2008)).

UNCLASSIFIED

UNCLASSIFIED

RESULTS OF 2009 FISMA REVIEW

ALL SYSTEMS WERE NOT CERTIFIED AND ACCREDITED

BBG needs to make significant improvements in its certification and accreditation (C&A) process. Specifically, for its 11 systems, BBG had performed the C&A process on only one system, the Central Infrastructure Domain, and that was in FY 2008. However, no annual and contingency plan tests were performed for this system, as required under FISMA. OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires agencies to develop system security plans (SSP). The SSP is an overview of the security requirements of the system and describes the controls in place or planned to meet those requirements. Also, 10 of the 11 systems did not have the SSPs required by FISMA and OMB. BBG officials said that the C&A process had been started on another system but had not been completed at the time of this review.

Standards and guidance for performing C&A are contained in NIST Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, and NIST SP 800-53, revision 2, *Recommended Security Controls for Federal Information Systems*. This guidance states that officials must be able to determine the risk to operations, assets, or individuals and the acceptability of that risk in view of the mission or business needs of their agencies. Officials must also weigh the appropriate factors and decide to either accept or reject the risk to their respective agencies. Security certification supports security accreditation by providing authorizing officials with information necessary to make credible, risk-based decisions about whether to place new information systems into operation or to continue using the current systems. Security accreditation includes the acceptance and management of risk—the risk to agency operations, agency assets, or individuals that results from the operation of an information system.

According to BBG officials, C&A was not performed on the other 10 systems because of the resignation of a key employee. In addition, BBG had not developed policies and procedures to support the C&A process.

Without C&A, BBG lacks a crucial management control that ensures that systems are properly assessed for risk, have been independently tested, and have identified and sufficiently mitigated weaknesses. Consequently, BBG management could not ensure that systems were operating without unacceptable risks or weaknesses.

UNCLASSIFIED

Also, not testing BBG systems' contingency plans may potentially mislead management to believe that the systems will operate properly during an emergency or service disruption. Loss of BBG systems would limit BBG management's ability to perform its mission, including its critical functions in serving the public.

Recommendation 1: The review team recommends BBG's Chief Information Officer:

- Develop policies and procedures for certification and accreditation (C&A).
- Conduct C&A on all seven of its “moderate-level” systems as categorized in Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. This C&A includes the development of a system security plan for all systems and testing and monitoring the effectiveness of the information security policies, procedures, practices, and security controls on an ongoing basis with the frequency depending on risk, but no less than

Management Response

BBG management concurred with the recommendation, stating that it would conduct C&A testing on the three systems it determined had the “highest priority” by the end of the third calendar quarter of 2010 and for the remaining eight “lower priority” systems by the end of the fourth quarter of 2010. However, BBG did not fully address the intent of the recommendation: to perform C&A on all 11 systems by the end of the third quarter of calendar 2010 instead of on just the three “highest priority” systems.

OIG understands, because of budgetary and personnel constraints, that BBG may not be able to perform C&A on all 11 systems by the time specified. Also, OIG is aware, based on the potential levels of impact on organizations if there is a breach of security (categorized in FIPS Publication 199), that BBG has seven systems categorized at the “moderate” level and three systems at the “low” level. Therefore, OIG has revised recommendation 1 and now recommends that BBG perform C&A on the seven “moderate-level” systems by the end of the third quarter of FY 2010.

OIG requests that BBG respond to the new recommendation. OIG will consider the recommendation resolved when BBG provides OIG documentation showing its plans for conducting or documentation showing that it has conducted C&A on all seven of the moderate-level systems by the time specified.

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)



(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

ALL EMPLOYEES AND CONTRACTORS DID NOT TAKE THE SECURITY AWARENESS TRAINING COURSE

BBG has improved its security awareness training course, to include peer-to-peer file sharing, in response to a finding in the FY 2008 FISMA report. The course addressed all NIST recommendations, such as Malicious Software, Unauthorized Software, Access Control, Loss of Availability, Computing Systems Availability, Disclosure of Personal Information, Sensitive Personal Information, and Peer-to-Peer File Sharing. However, BBG did not require that all new Federal employees and contrac-

UNCLASSIFIED

tors with log-in privileges take the security awareness training course before log-in privileges to the systems were granted or immediately after they were granted and annually as required. BBG tracked security awareness training attendance in a software tool called "Moodle." The review team found that in the past 2 years, approximately 52 percent of its employees had taken the course when it was offered annually. BBG required new employees to take the course within a year of employment and annually thereafter. However, the course was offered only 2 months during the calendar year.

FISMA² requires that agencies have sufficiently trained personnel to assist the agency in complying with FISMA and related policies, procedures, standards, and guidelines. FISMA also states the following:

[T]he required "agency wide information security program" shall include "security awareness training to inform personnel, including contractors . . . , of:

- (i) information security risks associated with their activities; and
- (ii) their responsibilities in complying with agency policies and procedures designed to reduce these risks(.)

NIST SP 800-53, revision 2, recommends that basic security awareness training be provided to all new information systems users (employees and contractors) before granting them log-in privileges to the system. It also states that employees should be provided with security awareness training annually to remind them of their responsibilities to protect information assets.

All employees did not take the security awareness course, even though BBG had a requirement that they take it. The review team found that BBG tracked and monitored individuals who had taken the course but did not ensure that everyone had taken it. BBG required only that new employees take the security awareness training course within a year of their employment, not prior to granting them log-in privileges to the system. In addition, BBG did not have a formal information security awareness policy. As such, there was no mandatory requirement for employees to take the course. Also, BBG provided the course only during a 2-month period instead of more frequently to ensure that the training requirement was met.

Security awareness training educates employees about the methods the agency has implemented to protect information assets, the controls implemented, and the risks to the organization if those controls are compromised. Employees who are not properly trained in computer security may cause, contribute to, or become victims of vulnerabilities or security breaches such as e-mail exploits, account or password sharing, inadequate safeguarding of passwords or computer resources, Internet misuse, corporate espionage, and social engineering.

² NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* (Oct. 2003).

Recommendation 3: The review team recommends BBG’s Chief Information Security Officer and Director of Human Resources:

- Require all BBG civilian employees and contractors to take the security awareness training before they are granted log-in privileges to the system.
- Offer the security awareness training on a regular basis, and monitor employees’ compliance.
- Develop security awareness policy that makes the security awareness course mandatory per Office of Management and Budget guidance.

Management Response and OIG Reply

BBG management concurred with the recommendation. Based on its response, OIG considers the recommendation resolved, pending further action.

CONFIGURATION MANAGEMENT POLICIES WERE DEVELOPED AND PUBLISHED

In March 2009, BBG published an agency-wide configuration management policy in response to an FY 2008 FISMA report recommendation. The review team reviewed and analyzed the policy and found that the policy addressed all applicable NIST controls. However, the review team could not verify that the policy was implemented because no systems had gone through the C&A process during FY 2009.

In addition, as required by OMB Memorandum M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, March 2007, BBG provided evidence, in the form of scan results, on its 2,172 Microsoft Windows XP workstations demonstrating successful implementation of Federal Desktop Core Configuration standards. The scans yielded an estimate of 86.59 percent compliance, measured as the ratio of total “pass” scan items to total scan items over all machines. This showed that BBG was working toward compliance with NIST SP 800-53 CM-6, *Configuration Settings*, for the systems that had not yet been subjected to the C&A process.

INVENTORY MANAGEMENT POLICIES WERE DEVELOPED AND IMPLEMENTED

BBG has made improvements in its inventory identification and management. In FY 2008, BBG identified 14 major FISMA reportable systems, which comprised 10 agency systems and four contractor systems. In March 2009, BBG consolidated its inventory into 11 systems, two of which were contractor systems. This consolidation was in response to an FY 2008 FISMA report recommendation that required BBG to develop, document, and implement formal procedures for inventory identification and management. Impact levels (High, Moderate, and Low) as identified in Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, were identified for BBG systems as required by OMB guidance.

INFORMATION SECURITY INCIDENT RESPONSE PLAN WAS UPDATED AND IMPLEMENTED

In response to an FY 2008 FISMA report recommendation, BBG improved its Information Security Incident Response Plan by updating its Incident Management Policies and to include the Privacy Breach Notification Policy and procedures in the plan.

FISMA³ requires agencies to establish procedures for detecting, reporting, and responding to security incidents. NIST SP 800-61, revision 1, *Computer Security Incident Handling Guide*, March 2008, provides guidance to agencies on establishing an effective incident response program. The guidance focuses on four phases: (1) preparation, (2) detection and analysis, (3) containment/eradication/recovery, and (4) post-incident activity. OMB Circular A-130, Appendix III, requires agencies to develop SSPs. These SSPs are an overview of the security requirements of the system and describe the controls in place or planned to meet those requirements. The SSPs also delineate the responsibilities for and the expected behavior of all individuals who access the system. The SSP is organized into three general classes of security controls: management, operational, and technical. Incident reporting is part of the operational security controls.

According to the Incident Response Plan, an incident should be reported if it involves the release or potential release of personally identifiable information (PII) or other sensitive information. This type of incident should be reported to the

³ Pub. L. No. 107-347 § 3544(b)7.

UNCLASSIFIED

agency's Chief Privacy Officer, and the Privacy Breach Notification Policy should be consulted to determine the procedures required to notify actual or potential victims. The review team obtained and analyzed incidents reported during the fiscal year and determined that there were no incidents relating to PII.

The review team reviewed the Incident Management Policies and compared the controls and requirements with those contained in NIST SP 800-61, revision 1, to ensure that all phases of incident response policies and plans were addressed. Only minor gaps were noted.

To verify that security incidents were being reported to the United States Computer Emergency Readiness Team (US-CERT),⁴ as required by BBG policy, the review team obtained Remedy⁵ tickets generated from September 1, 2008, to August 18, 2009. The review team performed a search on Remedy tickets based on the incident categories and found that the majority of tickets did not require a report to US-CERT or to law enforcement. Out of 25,408 incidents in the system, the review team identified the US-CERT categories shown in Table 1.

Table 1. US-CERT Categories

US-CERT Category	Count	Percent of Total
Unauthorized Access	0	0%
Denial-of-Service	7	2%
Malicious Software	309	90%
Improper Use	3	1%
Attempted Unauthorized Access	23	7%
Total	342	100%

The review team found that the two tickets that should have been reported to US-CERT were not reported in a timely manner in accordance with BBG's Computer Security Incident Response Plan. This was because the two incidents were reported before the Incident Response Plan was published in July 2009.

⁴ US-CERT is the operational arm of the National Cyber Security Division at the Department of Homeland Security.

⁵ Remedy IT Service Management Suite is an integrated collection of products that work together to support a client's Information Technology Infrastructure Library (ITIL)-based infrastructure for Incident Management.

PRIVACY PROGRAM HAS IMPROVED

Privacy guidance and provisions for all Federal agencies are described in section 208 of the E-Government Act of 2002⁶ and OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003. Per the E-Government Act of 2002, agencies are required to conduct Privacy Impact Assessments (PIA) for electronic information systems and collection and make the assessments publicly available. Further, the agency must post privacy policies on agency Web sites and translate privacy policies into a standardized machine-readable format. OMB Memorandum M-03-22 provides additional guidance to the agencies and directs agencies to conduct reviews of how information about individuals is handled within their agency when they use electronic means to collect new information or when agencies develop or buy new systems to handle collections of PII.

The Associate CIO is the Senior Agency Official for Privacy and is responsible for implementing privacy programs. BBG provided and monitored attendance for its privacy awareness training, which was given annually to employees. BBG's administrative systems, such as payroll, accounting, human resources, and procurement/contracting, were outsourced to other Federal agencies. The systems were subject to FISMA controls and testing by the agencies that provide services, and BBG relied on these agencies to execute the PIA process.

For the systems maintained in-house, BBG used a Privacy Threshold Analysis (PTA) template that was developed by the U.S. Securities and Exchange Commission to identify systems that had privacy information. BBG completed two PTAs in FY 2009 and found that no systems were identified as containing PII.

⁶ Pub. L. No. 107-347, 116 stat. 2899, 44 U.S.C. § 101.

UNCLASSIFIED

UNCLASSIFIED

LIST OF RECOMMENDATIONS

Recommendation 1: The review team recommends BBG's Chief Information Officer:

- Develop policies and procedures for certification and accreditation (C&A).
- Conduct C&A of all seven of its “moderate-level” systems as categorized in Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. This C&A includes the development of a system security plan for all systems and testing and monitoring the effectiveness of the information security policies, procedures, practices, and security controls on an ongoing basis with the frequency depending on risk, but no less than annually.

(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Recommendation 3: The review team recommends BBG's Chief Information Security Officer and Director of Human Resources:

- Require all BBG civilian employees and contractors to take the security awareness training before they are granted log-in privileges to the system.

UNCLASSIFIED

- Offer the security awareness training on a regular basis, and monitor employees' compliance.
- Develop security awareness policy that makes the course mandatory per Office of Management and Budget guidance.

ABBREVIATIONS

BBG	Broadcasting Board of Governors
C&A	certification and accreditation
CIO	Chief Information Officer
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
IG	Inspector General
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	personally identifiable information
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analysis
SP	Special Publication
SSP	system security plan
US-CERT	United States Computer Emergency Readiness Team

UNCLASSIFIED

UNCLASSIFIED

APPENDIX A: SCOPE AND METHODOLOGY

The scope of the review was limited to the Inspector General's reporting categories (as listed) and questions included in Office of Management and Budget (OMB) Memorandum M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, August 20, 2009. The reporting categories included the following:

- Inventory
- Certification and Accreditation (C&A), Security Controls Testing, and Contingency Plan Testing
- Evaluation of Agency Oversight of Contractor Systems and Quality of Agency Inventory
- Evaluation of the Agency's Plan of Action and Milestones (POA&M) Process
- Inspector General (IG) Assessment of the C&A Process
- IG Assessment of the Agency's Privacy Program and Privacy Impact Assessment (PIA) Process
- Configuration Management
- Incident Reporting
- Security Awareness Training
- Peer-to-Peer File Sharing

The review team conducted this review in accordance with OMB guidance and Federal Information Security Management Act of 2002 (FISMA) recommendations which required that the team plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the review objectives. To accomplish this, the review team did the following:

- Reviewed prior FISMA reports and their supporting work papers.
- Interviewed Broadcasting Board of Governors (BBG) management to gain an understanding of the policies, procedures, and controls used to implement FISMA and OMB guidelines.
- Documented its understanding of the environment.
- Obtained and analyzed supporting evidence from management to determine whether the policies, procedures, and controls implemented operated effectively during the fiscal year.

UNCLASSIFIED

- Obtained and analyzed evidence to determine whether management had implemented corrective actions to close prior years' audit findings and recommendations.

During the review, the review team documented and communicated to management issues identified through Notices of Potential Finding and Recommendations. These notices were communicated to BBG management, who concurred with all of them and provided management responses.

APPENDIX B

FOLLOW-UP OF RECOMMENDATIONS FROM THE FY 2008 FISMA REPORT

The review team reviewed actions implemented by management to mitigate the control gaps identified in the FY 2008 FISMA report. The current status of each of those recommendations is as follows:

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

2009 Status – Closed. We reviewed the documented procedure for annual reviews of information systems and accreditation boundaries.

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

2009 Status – This is a repeat recommendation from the FY 2008 report. Combined with Recommendation 3, it has become Recommendation 2 in the FY 2009 report.

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

2009 Status – This is a repeat recommendation from the FY 2008 report. Combined with Recommendation 2, it has become Recommendation 2 in the FY 2009 report.

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

2009 Status – This is a repeat recommendation from the FY 2008 report. Combined with Recommendation 8, it has become Recommendation 1 in the FY 2009 report.

UNCLASSIFIED

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

2009 Status – Closed. BBG has updated its Information Security Incident Response Plan, dated July 29, 2009. According to the Incident Response Plan, an incident should be reported if it involves the release or potential release of personally identifiable information or other sensitive information. This type of incident is reported to the agency’s Chief Privacy Officer, and the provisions of the agency’s Privacy Breach Notification Policy should be consulted to determine the procedures required to notify actual or potential victims.

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

2009 Status – Closed. We reviewed the Information System Configuration Management Procedures dated May 2009 and found that they addressed all the elements of the Configuration Management Requirement in National Institute of Standards and Technology Special Publication 800-53.

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

2009 Status – This is a repeat recommendation from the FY 2008 report. Combined with recommendation 8, it has become Recommendation 1 in the FY 2009 report.

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

2009 Status – Closed. We reviewed the Incident Management Policy dated July 2009 and compared it with the Incident Response Plan and NIST SP 800-61. No exceptions were noted.

APPENDIX C



**BROADCASTING BOARD OF GOVERNORS
UNITED STATES OF AMERICA**

CONTROLLED UNCLASSIFIED INFORMATION
(UNCONTROLLED when removed from enclosure)

November 16, 2009

The Honorable Harold Geisel
Acting Inspector General
Office of Inspector General
U.S. Department of State

Dear Mr. Geisel:

This is in response to your letter of October 30, 2009, regarding the OIG draft report, *Review of the Information Security Program at the Broadcasting Board of Governors*. (Draft Report AUD/IT-09-XX, November 2009).

The Broadcasting Board of Governors (BBG) is grateful for the opportunity to review the OIG's draft report and appreciates the positive and constructive approach of OIG's team. This report will be helpful to us in our efforts to improve our management of the agency's information security program.

Enclosed as requested are our comments on the draft.

We thank you again for the opportunity to comment on the report. If you have any questions, please feel free to contact me or Mr. John Welch, Senior Advisor, International Broadcasting Bureau, at (202) 203-4545).

Sincerely,

A handwritten signature in black ink, appearing to read "J. Trimble", with a horizontal line extending to the right.

Jeffrey N. Trimble
Executive Director

Enclosure

1

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

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

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

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