OIG HIGHLIGHTS

View Report AUD-IT-IB-16-17

November 2015
OFFICE OF AUDITS
Information Technology Division

(U) Audit of the Broadcasting Board of Governors Information Security Program

(U) What OIG Audited

(U) Acting on OIG's behalf, Williams, Adley & Company-DC, LLP (Williams, Adley), an independent public accounting firm, conducted this audit to determine the effectiveness of the Broadcasting Board of Governors (BBG) information security program and whether security practices in FY 2015 complied with applicable Federal laws, regulations, and information security standards.

(U) What OIG Recommends

(U) OIG made three recommendations to improve BBG's information security program. Specifically, OIG is recommending that BBG (1) develop a strategy to realign information technology resources; (2) develop and implement an organization-wide information security risk management strategy; and (3) define and implement the [Redacted] (b) (5)

(U) Based on BBG's responses to a draft of this report, OIG considers all recommendations resolved, pending further action.

(U) What OIG Found

~~(SBU)~~ Overall, Williams, Adley identified control weaknesses that significantly impacted BBG's information security program. While BBG has taken some action to improve its information security program since our last assessment in FY 2014, Williams, Adley continued to find that BBG was not in compliance with Federal laws, regulations, and information security standards. Specifically, Williams, Adley found that BBG had not fully developed and implemented an organization-wide risk management strategy to identify, assess, respond to, and monitor information security risk at all levels of the organization because, according to a senior BBG official, BBG chose to prioritize its resources on operations and not information security.

~~(SBU)~~ In addition, although BBG had established a [Redacted] (b) (5) [redacted] Therefore, Williams, Adley concludes, based on the Council of the Inspectors General on Integrity and Efficiency *ISCM Maturity Model For FY 2015*,[1] BBG is performing ISCM activities in a [Redacted] (b) (5) [redacted]

(U) Overall, Williams, Adley identified control deficiencies in [redacted] [Redacted] (b) (5) [redacted]

[1] **(U)** DHS, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, June 2015.
[2] **(U)** See Appendix D: FY 2015 Continuous Monitoring Maturity Model for additional details.

OIG
Office of Inspector General
U.S. Department of State • Broadcasting Board of Governors

AUD-IT-IB-16-17 | Office of Audits | November 2015

(U) Audit of the Broadcasting Board of Governors Information Security Program

INFORMATION TECHNOLOGY DIVISION

WILLIAMS ADLEY

Audit of the Broadcasting Board of Governors' Information Security Program

November 5, 2015

Office of Inspector General
U.S. Department of State and the Broadcasting Board of Governors
Washington, DC

Williams, Adley & Company-DC, LLP has performed an audit of the Broadcasting Board of Governors' (BBG) information security program. We audited BBG's compliance with the Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014; Office of Management and Budget requirements; and National Institute of Standards and Technology standards. We performed this audit under Contract No. SAQMMA15F0980. 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
Certified Public Accountants / Management Consultants
1030 15th Street, NW, Suite 300W • Washington, DC 20005 • (202) 371-1397 • Fax: (202) 371-9161
www.williamsadley.com

(U) CONTENTS

(U) OBJECTIVE

(U) The objective of this audit was to determine the effectiveness of the Broadcasting Board of Governors (BBG) information security program and whether security practices in FY 2015 complied with laws, regulations, and standards established by the Federal Information Security Management Act of 2002 (FISMA),[1] as amended by the Federal Information Security Modernization Act of 2014;[2] the Office of Management and Budget (OMB); and the National Institute of Standards and Technology (NIST). Specifically, the audit assessed BBG's information security program and related practices for risk management and continuous monitoring, which include configuration management, identity and access management, incident response and reporting, security training, plans of action and milestones (POA&Ms), remote access management, contingency planning, and contractor systems. See Appendix A for the scope and methodology for this audit and Appendix B for follow-up to the recommendations from the FY 2014 audit.

(U) BACKGROUND

(U) BBG is an independent Federal agency that supervises all U.S. civilian international broadcasting. BBG broadcasters distribute programming in 61 languages to an estimated weekly audience of 215 million people via radio, television, the Internet, and other news media. BBG works to serve as an example of a free and professional press, reaching a worldwide audience with news, information, and relevant discussions. The International Broadcasting Bureau, a significant component of BBG, maintains the global distribution network over which all BBG-funded news and information programming is distributed. The International Broadcasting Bureau also performs administrative functions such as financial management, human resources, and IT support. For example, BBG's Chief Information Officer (CIO) is part of the International Broadcasting Bureau.

(U) BBG, as well as its contractors, depends on information systems and electronic data to carry out essential mission-related functions. The security of these systems and networks is vital to protecting national and economic security, public health and safety, and the flow of commerce. As such, these information systems are subject to serious threats that can have adverse effects on organizational operations (that is, missions, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation by exploiting both known and unknown vulnerabilities to compromise the confidentiality, integrity, or the availability of information being processed, stored, and transmitted by those systems.

[1] (U) Public Law 107-347 Title III, Federal Information Security Management Act of 2002, December 2002.

[2] (U) Public Law 113-283, Federal Information Security Modernization Act of 2014, December 2014.

(U) Risk Management

(U) Because of the risk posed to information systems, it is crucial that organizations take appropriate steps to secure information and information systems. To manage risk to information, senior executives must be committed to making risk management a fundamental business requirement. This top-level, executive commitment ensures that sufficient resources are available to develop and implement an effective, organization-wide risk management program. In addition, senior executives must recognize that explicit, well-informed risk-based decisions are crucial in order to balance the benefits of using information systems against the risk of those same information systems being the channels through which attacks, environmental disruptions, or human errors cause business failures.

(U) To assist in making those explicit, well-informed risk-based decisions, a comprehensive process must be in place that requires the organization to:

(U) (1) *Frame risk (that is, establish the context for risk-based decisions)* - The purpose of framing risk is to produce a risk management strategy that addresses how the organization intends to assess risk, respond to risk, and monitor risk. The frame establishes a foundation for managing risk and defines the boundaries for risk-based decisions within the organization. In addition, the risk framing component and the associated risk management strategy also include any strategic-level decisions on how risk is to be managed by senior executives.

(U) (2) *Assess risk* - The purpose of assessing risk is to identify threats to the organization, vulnerabilities, the harm that may occur given the potential exploitation of those vulnerabilities, and the likelihood that consequences will occur. The result is a determination of risk—that is, the degree of impact and likelihood of that impact occurring.

(U) (3) *Respond to risk* - The purpose of risk response is to provide a consistent, organization-wide, response to risk in accordance with the organizational risk frame by developing alternative courses of action, evaluating the alternative courses of action, determining appropriate courses of action consistent with organizational risk tolerance, and implementing risk responses based on selected courses of action.

(U) (4) *Monitor risk on an ongoing basis* - The purpose of risk monitoring is to: (1) verify that planned risk response measures are implemented and information security requirements derived from organizational business functions are satisfied; (2) determine the ongoing effectiveness of risk response measures after being implemented; and, (3) identify risk-impacting changes to organizational information systems and the environments in which those systems operate. This monitoring leverages Information Security Continuous Monitoring (ISCM) activities, which provide awareness of threats, vulnerabilities, and the effectiveness of deployed security controls, to assist in making risk-based decisions.

(U) Based on these objectives, information security risk management must be a holistic, organization-wide activity that involves the entire organization. With all individuals directly influenced by the risk frame established by senior executives, organizational culture becomes a key factor in determining how risk is managed within an organization.

(U) Organizational culture refers to the values, beliefs, and norms that influence the behaviors and actions of the senior executives and individual members of organizations. As such, cultural influences and impacts affect all levels of the organization. Senior executives, both directly and indirectly, set the stage for how the organization responds to various approaches to managing risk. Senior executives establish the risk tolerance for organizations both formally (for example, through publication of strategy and guidance documents) and informally (for example, through actions that get rewarded and penalized, the degree of consistency in actions, and the degree of accountability enforced). The direction set by senior executives and the understanding of existing organizational values and priorities are major factors that determine how risk is managed within the organization.

(U) Continuous Monitoring Program

(U) To assist in securing systems, Federal agencies leverage ISCM activities, which provide awareness of threats, vulnerabilities, and the effectiveness of deployed security controls, to assist in making risk-based decisions from the organization and information systems perspectives. ISCM is intertwined with risk management at every level of the organization. Specifically, ISCM gives agency officials access to security-related information on demand and enables timely management, assessment, and response to security issues as part of an agency's information security risk management framework.

(U) To leverage ISCM effectively and to make risk-based decisions, an agency must first define a strategy based on organizational risk tolerance, which addresses monitoring activities at the organization, bureau, and information systems levels. Once a strategy is defined, it must be used to establish and implement an ISCM program where information security-related activities are performed, data is collected and analyzed, and information security risks are reported across the organization. To assist in achieving these objectives, security controls must be implemented consistently, operate as intended, produce the desired outcome with respect to meeting the security requirements for the system, and continue to be effective over time at the information systems level to support the monitoring requirements at the organization and bureau levels. These information security controls at the information systems level are implemented through the following key information security process areas:

- (U) Configuration Management – The purpose of configuration management is to manage the effects of changes or differences in configurations on an information system or network. Configuration management is an essential component of monitoring the status of security controls and identifying potential security-related problems in information systems. This information can help security managers understand and monitor the evolving nature of vulnerabilities as they appear in a system under their

responsibility, thus enabling managers to direct appropriate changes as required. The goal of configuration management is to make assets harder to exploit through better configuration.

- (U) Identity and Access Management – Users and devices must be authenticated to ensure that they are who or what they identify themselves to be. The goal of identity and access management is to ensure that users and devices are properly authorized to access information and information systems.

- (U) Incident Response and Reporting – The purpose of incident response and reporting is to determine the kinds of attacks that have been successful and position the organization to make a risk based decision about where it is most cost effective to focus its security resources. A well-defined incident response capability helps the organization detect incidents rapidly, minimize loss and destruction, identify weaknesses, and restore IT operations quickly.

- (U) Security Training – Establishing and maintaining a robust and relevant information security training process as part of the overall information security program is the primary conduit for providing a workforce with the information and tools needed to protect an agency's vital information resources. This will ensure that personnel at all levels of the organization understand their information security responsibilities to properly use and protect the information and resources entrusted to them. Organizations that continually train their workforce in organizational security policy and role-based security responsibilities will have a higher rate of success in protecting information.

- (U) POA&Ms – POA&Ms assist in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. POA&Ms track the measures implemented to correct deficiencies and to reduce or eliminate known vulnerabilities. POA&Ms can also assist in identifying performance gaps, evaluating an organization's security performance and efficiency, and conducting oversight. It is an essential part of the risk management process to track problems and to decide which issues to address, and shows an organization's efforts to address corrective action with a standard and centralized approach.

- (U) Remote Access Management – The goal of remote access management is to help deter, detect, and defend against unauthorized network connections/access to internal and external networks. Secure remote access is essential to an organization's operations because the proliferation of system access through telework, mobile devices, and information sharing means that information security is no longer confined within system

perimeters. Organizations also rely on remote access as a critical component of contingency planning and disaster recovery.[3]

- (U) Contingency Planning – Contingency planning involves the actions required to plan for, respond to, and mitigate damaging events. As such, the primary purpose of contingency planning is to give attention to rare events that have the potential for significant consequences and promoting first priority risk.

- (U) Contractor Systems – The primary purpose of contractor systems is to ensure that information systems operated by contractors and other external entities on behalf of the Federal Government meet all applicable security requirements.

(U) Federal Information Security Management Act

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

(U) FISMA assigns specific responsibilities to NIST, OMB, and the Department of Homeland Security (DHS) and other Federal agencies for the purpose of strengthening information system security throughout the Federal Government. In particular, FISMA requires the head of each agency to implement policies and procedures to cost effectively reduce IT security risks to an acceptable level. To ensure the adequacy and effectiveness of information system controls, FISMA requires agency program officials, CIOs, 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) In an effort to improve Federal cybersecurity, Congress enacted the Federal Information Security Modernization Act of 2014, which amended FISMA, on December 18, 2014. The act served to clarify and strengthen information security roles and responsibilities for OMB and DHS, placed an emphasis on assessing effectiveness, and reiterated the requirement for Federal agencies to develop, document, and implement an organization-wide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor.

(U) To assist agencies in implementing the requirements of FISMA, OMB and DHS annually issue metrics[4] providing guidance to agencies and OIG on how to meet FISMA evaluation and reporting requirements. Appendix C presents the 10 FISMA reportable areas for 2015.

[3] (U) OMB, *Annual Report to Congress: Federal Information Security Management Act*, accessed September 30, 2015.

[4] (U) DHS, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, June 2015.

(U) Continuous Monitoring Maturity Model

(U) As part of the updated FY 2015 DHS FISMA reporting metrics, dated June 19, 2015, the Council of Inspectors General on Integrity and Efficiency, DHS, OMB, NIST, and other stakeholders developed a maturity model for the continuous monitoring domain to provide perspective on the overall status of information security within an agency. The purpose of the Council of Inspectors General on Integrity and Efficiency maturity model, found in Appendix D, is to:

- (U) summarize the status of agencies' information security programs and their maturity on a 5-level scale,
- (U) provide transparency to agency CIOs, top management officials, and other interested readers of Office of Inspector General (OIG) FISMA reports about what has been accomplished and what still needs to be implemented to improve the information security program to the next maturity level, and
- (U) help ensure consistency across the OIGs in their annual FISMA reviews.

(U) AUDIT RESULTS

~~(SBU)~~ Overall, Williams, Adley & Company-DC, LLP (Williams, Adley) identified control weaknesses in [redacted] of the key information security process areas that significantly impacted BBG's information security program. While BBG has taken some action to improve its information security program since our last assessment in FY 2014, Williams, Adley continued to find that BBG was not in compliance with FISMA, OMB, and NIST requirements. Specifically, Williams, Adley found that [Redacted] (b) (5) [redacted] as defined by OMB Memorandum M-14-04.[7]

(U) Finding A: BBG Had an Ineffective Risk Management Strategy

~~(SBU)~~ Williams, Adley found that BBG had not established and implemented an effective organization-wide risk management strategy. The reason BBG did not have a fully developed and implemented organization-wide risk management strategy [Redacted] (b) (5) [redacted] is because, according to a senior BBG official, BBG chose to prioritize its resources on operations and not information

[7] (U) OMB Memorandum M-14-04, *FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 2013.

security. Without an effective risk management program, BBG is vulnerable to IT centered attacks and threats.

(U) According to NIST Special Publication (SP) 800-39,[8] effectively managing information security risk organization-wide requires the following key elements:

- (U) Assignment of risk management responsibilities to senior leaders/executives;
- (U) Ongoing recognition and understanding by senior leaders/executives of the information security risks to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems;
- (U) Establishing the organizational tolerance for risk and communicating the risk tolerance throughout the organization including guidance on how risk tolerance impacts ongoing decision-making activities; and
- (U) Establish accountability by senior leaders/executives for their risk management decisions and for the implementation of effective, organization-wide risk management programs.

(U) The NIST standard goes on to say that managing information security risk requires the involvement of the entire organization defined in three tiers, from senior leaders providing the strategic vision and top-level goals and objectives for the organization; to bureau leaders planning, executing, and managing projects; to system owners operating the information systems supporting the organization's business functions.

~~(SBU)~~ Using the approach described in the Federal Information Security Modernization Act of 2014, Williams, Adley evaluated whether BBG had established and implemented an effective organization-wide risk management strategy at all applicable levels of the organization (that is, at the organizational level and information systems level). At the organization level, Williams, Adley found that BBG had an approved continuous monitoring and risk management strategy;[9] [Redacted] (b) (5)

- ~~(SBU)~~ Clearly define key roles for implementing the strategy. For example, senior management roles and responsibilities were not defined and communicated across the organization.
- ~~(SBU)~~ Clearly document, communicate, and integrate information security risks as an input into BBG's consolidated list of all risks.

[8] (U) NIST SP 800-39, "Managing Information Security Risk," March 2011.

[9] (U) ISCM and Risk Management Strategy, April 2014.

- ~~(SBU)~~ Clearly document and define how to quantify the impact and likelihood of information security risks, from the organizational and information systems perspectives, to determine if those information security risks are acceptable or unacceptable.
- ~~(SBU)~~ Clearly define how it will integrate ISCM activities with organizational risk tolerance and business requirements.
- ~~(SBU)~~ Clearly define how ISCM information would be communicated to BBG officials in order for that information to be used to make risk-based decisions.[10]

(U) In addition, at the information systems level, Williams, Adley [redacted] This process is important as the risks identified from this effort should be communicated to BBG officials to incorporate into the risk-based decision making process in support of the business mission. Specifically, the assessment and authorization process is comprised of:

- (U) Assessments that provide a comprehensive analysis of security controls. Assessments are performed to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system.
- (U) Authorizations, which are the official management decision given by a senior agency official to authorize an information system and to explicitly accept the risk to BBG operations, assets, or individuals based on the implementation of security controls. At BBG, the authorizing official is the CIO. An authorization is the formal decision of the Information System Owner and the CIO to accept the remaining risk that results from operating the system. The authorization grants the system its Authorization to Operate.

(U) Williams, Adley also found that BBG has not effectively implemented an assessment and authorization process. Specifically, BBG:

- ~~(SBU)~~ Was unable to provide evidence of remediation of the findings from any of the three Security Assessment Reports[11] tested.

[10] (U) See Finding B for deficiencies identified in FY 2015 for BBG's ISCM program.

[11] (U) According to NIST SP 800-53, rev. 1 (June 2010), "Guide for Assessing the Security Controls in Federal Information Systems and Organizations," the output and end result of the security control assessment is the security assessment report, which documents the assurance case for the information system and is one of three key documents in the security authorization package developed by information system owners and common control providers for authorizing officials.

- ~~(SBU)~~ Did not justify the CIO's decision to accept risk for any of the three Authorization to Operate documents tested.

(U) Further, with respect to BBG systems, of 22 systems tested:

- ~~(SBU)~~ BBG did not depict the system accreditation boundary, which includes people, processes, and information technology, within the System Security Plan for one system (5 percent)—[Redacted] (b) (5)
- (U) One system (5 percent)—[Redacted] (b) (5) —was not included within the system inventory.

(U) In addition, Williams, Adley found that the Federal Risk and Authorization Management Program[12] approval status was not documented for two cloud-based systems tested—[Redacted] (b) (5)

~~(SBU)~~ The reason BBG did not have a fully developed and implemented organization-wide risk management strategy [Redacted] (b) (5) is because, according to a senior BBG official, BBG chose to prioritize its resources on operations and not information security. For example, instead of focusing on effectively establishing and implementing its risk management strategy at all applicable levels of the organization, BBG chose to focus its resources on handling day-to-day operations.

(U) In order to achieve its core missions, BBG personnel must be able to access information systems at any time and from any location, domestic and abroad. BBG's information systems and sensitive information rely on the confidentiality, integrity, and availability of its comprehensive and interconnected infrastructure utilizing various technologies around the globe. Managing information security risk effectively throughout the organization is critical to achieving this mission successfully. However, without a centralized approach to communicating information security risks, BBG cannot have an effective risk management program. The consequence of an ineffective risk management program can affect all levels of the organization. For example, at the organizational level, BBG is vulnerable to IT centered attacks and threats.

(U) Williams, Adley has annually identified the same systemic and pervasive information security weaknesses across BBG's IT security posture since FY 2010. To date, BBG leadership has not been able to remediate those identified information security weaknesses. Without a sufficient risk management program, system owners cannot appropriately prioritize resources to manage information security risks to protect information systems and sensitive data from attacks and threats. For example, new vulnerabilities discovered in an information system may have systemic

[12] (U) According to U.S. General Services Administration, the Federal Risk and Authorization Management Program is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services, <http://www.gsa.gov/portal/category/102371>, accessed on October 8, 2015.

implications that extend agency-wide. Those same vulnerabilities may trigger changes to the organizational information security architecture or may require an adjustment to the organizational risk tolerance.

Recommendation 1: (U) OIG recommends that the Chief Information Officer develop a strategy to realign information technology resources to balance operational needs with the need for an effective information security risk management strategy.

(U) Management Response: The CIO concurred with this recommendation. BBG plans to realign IT resources to perform effective information security risk management.

(U) OIG Reply: OIG considers the recommendation resolved because the CIO agreed to implement it. This recommendation will be closed when OIG receives and accepts documentation demonstrating the CIO has developed a strategy to realign information technology resources to balance operational needs with the need for an effective information security risk management strategy.

[Redacted] (b) (5)

[Redacted] (b) (5)

BBG cannot fully and effectively execute its overall organization-wide information security program.[14]

~~(SBU)~~ Using the approach described in the Federal Information Security Modernization Act of 2014, Williams, Adley evaluated whether BBG established and implemented [Redacted] (b) (5)

At the organization level, Williams, Adley found that BBG had established a continuous monitoring strategy, as reported in its FY 2014 FISMA report.[15]

[Redacted] (b) (5)

[13] **(U)** [Redacted] (b) (5) due to the nature of the risk management deficiency, Williams, Adley reported risk management as a separate finding (Finding A).

[14] **(U)** See Appendix E of this report for criteria used to assess continuous monitoring.

[15] **(U)** *Audit of the Broadcasting Boards of Governors Information Security Program* (AUD-IT-IB-15-13, October 2014).

using risk-based decision making, [Redacted] (b) (5) For example, BBG has [Redacted] (b) (5)

Furthermore, the strategy did not:

- ~~(SBU)~~ Define how [Redacted] (b) data would be communicated to BBG leadership and how that data would be leveraged to make risk-based decisions. To communicate data to BBG leadership, information should be delivered in ways that enable those individuals to make informed risk-based decisions.
- ~~(SBU)~~ Define [redacted] roles and responsibilities.
- ~~(SBU)~~ Define how BBG would [Redacted] (b) (5) to identify and communicate information security risks across all levels of the organization.[17]
- ~~(SBU)~~ Define how BBG would [Redacted] (b) (5) to appropriately assess the information security risks for BBG's security boundaries and assets.

(U) During FY 2015, BBG took action, such as implementing products and tools[18] designed to address Active Directory[19] (AD) account management, increasing patch management[20] efforts, and improving asset management.[21] BBG also took action to improve security training by internally developing system-owner role-based training courses. However, during this audit, Williams, Adley continued to find security control deficiencies at the information systems level, which Williams, Adley has reported annually since FY 2010. Collectively, the control deficiencies Williams, Adley identified during this audit represent a [Redacted] (b) (5) Because Williams, Adley has consistently identified similar control deficiencies over the past 6 years throughout BBG's systems, it is indicative of a systemic agency-wide problem. In FY 2015, Williams, Adley identified deficiencies with configuration management, identity and access management, incident response and reporting, security training, POA&Ms, remote access management, contingency planning, and contractor systems.

---

[16] **(U)** According to DHS, the Continuous Diagnostics and Mitigation Program provides Federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Congress established the program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources, <www.dhs.gov/cdm>, accessed on September 29, 2015.

[17] **(U)** See Finding A of this report for deficiencies identified in FY 2015 for BBG's risk management program.

[18] **(U)** Williams, Adley noted the following tools used at BBG—Microsoft System Center Configuration Manager and internally developed scripts to scan for out of policy AD accounts.

[19] **(U)** According to TechNet, AD is a directory service created by Microsoft for the Windows domain network, which provides the capability to centrally manage network users and system information while enforcing BBG's security standards and standardizing network configuration, <https://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx>, accessed on October 5, 2015.

[20] **(U)** According to NIST SP 800-40, rev. 3 (July 2013), "Guide to Enterprise Patch Management Technologies," patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems.

[21] **(U)** According to NIST Interagency Report 7693, "Specification for Asset Identification 1.1" (June 2011), asset management is the ability to identify assets based on some set of data known about them.

(U) Configuration Management

- ~~(SBU)~~ BBG has [Redacted] (b) (5) operating within its environment, as well as the [Redacted] (b) (5) operating system operating on 619 (23 percent) of 2,661 workstations, [Redacted] (b) (5)
- [Redacted] (b) (5)
  - [Redacted] (b) (5)
  - [Redacted] (b) (5)
  - [Redacted] (b) (5)
- ~~(SBU)~~ BBG's IT Change Management Policy[26] did not document testing procedures. In addition, there were no specifications regarding types and categories of possible changes.
- [Redacted] (b) (5)
- [Redacted] (b) (5)
- [Redacted] (b) (5)

~~(SBU)~~ Identity and Access Management

- ~~(SBU)~~ BBG did not have the policies and procedures for [Redacted] (b) (5)
- ~~(SBU)~~ As of June 2015, not all BBG employees had Personal Identity Verification cards.[28] Specifically, only 914 (59 percent) out of 1,550 employees and contractors had Personal Identity Verification credentials.

[Redacted] (b) (5)

[24] **(U)** According to NIST SP 800-128, "Guide for Security-Focused Configuration Management of Information Systems," (August 2011), a [Redacted] (b) (5)

[Redacted] (b) (5)

[26] **(U)** Technology Services & Innovation, "Change Management Policy," November 2010.

[27] **(U)** [Redacted] (b) (5)

- ~~(SBU)~~ Of five new user AD accounts tested, one (20 percent) did not have a new user request form submitted for account creation.
- ~~(SBU)~~ Of 2,850 AD accounts reviewed:

[Redacted] (b) (5)

~~(SBU)~~ Incident Response and Reporting

(U) Williams, Adley performed a separate effort focused on the operating effectiveness of BBG's incident response and reporting process area. While this effort will be reported separately, Williams, Adley identified deficiencies that impact compliance with the Federal Information Security Modernization Act of 2014,[31] such as incidents being miscategorized through human error, which diminished the incident response and reporting program's operating effectiveness. In addition, BBG did not consistently comply with prescribed categorization guidelines, reporting requirements, and remediation timelines.

(U) Security Training

(U) Although BBG took action to address previously identified security training weaknesses by initiating system owner role-based training courses in FY 2015, BBG has not fully implemented an effective security training process. Specifically, Williams, Adley found:

- (U) BBG did not finalize a policy for role-based training for employees and contractors with significant security responsibilities until June 2015.

---

[28] (U) According to the Chief Information Officers Council, "Personal Identity Verification Interoperability For Non-Federal Issuers," (v1.0.0, May 2009), a Personal Identity Verification card is a government-issued credit card-sized identification that contains a contact and contactless chip.

[29] (U) The final clearance form is part of BBG out-processing and notifies the help desk to remove the user's AD account on their final day.

[30] (U) The account removal help desk ticket is required for each terminated user.

[31] (U) Public Law 113-283, Federal Information Security Modernization Act of 2014, December 2014.

- **(U)** Of five new users tested, one (20 percent) had not taken the new user security awareness training in accordance with the security awareness training policy.[32]

(U) POA&Ms

~~(SBU)~~ Since FY 2010, BBG's POA&Ms have not consistently provided sufficient detail, such as the resources required to address the security weaknesses, milestones used to measure progress toward completion, and severity ratings. Specifically, for the POA&Ms associated with three systems[33] tested in FY 2015, Williams, Adley found that BBG did not:

- **(U)** Allocate proper resources required to complete the POA&Ms for two systems (67 percent).
- **(U)** Complete milestone data for two systems (67 percent).
- **(U)** Provide scheduled completion dates for one system (34 percent).

(U) Remote Access Management

- [Redacted] (b) (5)
- **(U)** Of 22 new Virtual Private Network[34] users, BBG did not have a signed Virtual Private Network user acceptance form for 2 users (9 percent).

~~(SBU)~~ Contingency Planning

~~(SBU)~~ Since FY 2010, Williams, Adley has reported that BBG had not fully developed and implemented a contingency plan or procedures compliant with OMB and NIST requirements.[35] Specifically, BBG had not completed its organization-wide and system-specific contingency plans or conducted contingency tests.

[32] **(U)** BBG,"XI Broadcast Administrative Manual 300 Information Security Awareness and Role-Based Training Policy," June 2015.

[33]

[34] **(U)** According to NIST SP 800-77, "Guide to IPSec VPNs," (December 2005), a Virtual Private Network is a Virtual network built on top of existing networks that can provide a secure communications mechanism for data and internet protocol information transmitted between networks.

[35] **(U)** NIST SP 800-34, rev. 1, "Contingency Planning Guide for Federal Information System," May 2010.

(U) Contractor Systems

- **(U)** BBG policies did not describe the necessary oversight required by BBG for external systems. In addition, BBG did not describe the asset management inventory tool, lifecycle[36] workflow, and roles and responsibilities for all of the asset team members.
- **(U)** Of 22 total systems, 1 (5 percent) contractor system, [Redacted] (b) (5) was not included in the system inventory.
- **(U)** Of 13 external systems that require a mutually signed Interconnection Security Agreement,[37] 1 (8 percent) system, [Redacted] (b) (5) was not signed by the system owner.

(U) ISCM supports an organization's risk management program. Based on this, an effective risk management framework, in support of its core mission and business processes, must establish how ISCM activities[39] are incorporated into the risk-based decisions made throughout an organization. However, BBG has not fully established and implemented an effective organization-wide risk management framework. To establish how ISCM activities are incorporated into risk-based decisions made throughout an organization, criteria for those activities must be established. NIST SP 800-137[40] states, "The criteria for ISCM are defined by the organization's risk management strategy, including how the organization plans to assess, respond to, and monitor risk, and the oversight required to ensure that the risk management strategy is effective." Furthermore, "Security controls, security status, and other metrics defined and monitored by officials at this tier are designed to deliver information necessary to make risk management decisions in support of governance."[41] However, BBG did not define [Redacted] (b) (5) process areas, as defined by FISMA, including configuration management, identity and access

[36] **(U)** According to NIST, "The System Development Life Cycle (SDLC)," lifecycle is the multistep process that starts with the initiation, analysis, design, and implementation of the system, and continues through the maintenance and disposal of the system, <http://csrc.nist.gov/publications/nistbul/april2009_system-development-life-cycle.pdf>, accessed on October 5, 2015.

[37] **(U)** According to NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," (August 2002), the Interconnection Security Agreement specifies the technical and security requirements of the interconnection.

[38] **(U)** BBG, *System Interface and Security Interconnection Agreement between BBG and* [Redacted] (b) (5)

[39] **(U)** According to NIST SP 800-137, "ISCM for Federal Information Systems and Organization," (September 2011), ISCM activities include security controls, security status, and other metrics defined and monitored by agency leadership.

[40] **(U)** NIST SP 800-137, "ISCM for Federal Information Systems and Organization," September 2011.

[41] **(U)** Ibid.

[42] **(U)** According to NIST SP 800-137, "ISCM for Federal Information Systems and Organization," (September 2011), ISCM criteria includes security control volatility, system categorizations/impact levels, security controls or specific assessment objects providing critical functions, security controls with identified weaknesses, organizational risk tolerance, threat information, vulnerability information, risk assessment results, output of monitoring strategy reviews, and reporting requirements.

management, incident response and reporting, security training, POA&Ms, remote access management, contingency planning, and contractor systems, to support its management of risk.

(U) Leveraging ISCM activities effectively to make risk-based decisions throughout the organization is critical to achieving this mission. [Redacted] (b) (5) BBG is unable to prioritize its organizational goals and objectives and as a result, BBG cannot fully and effectively execute its overall organization-wide information security program. [Redacted] (b) (5), BBG cannot provide stakeholders, including senior officials, business owners, and information system owners, with a unified understanding of the information system security goals, allowing BBG to consistently monitor a dynamic network environment with changing threats, vulnerabilities, technologies, missions, and business functions of BBG.

(U) Based on the Council of the Inspectors General on Integrity and Efficiency *ISCM Maturity Model For FY 2015*,[43] [Redacted] (b) (5)

(U) [Redacted] (b) (5) are evident from the continued identification of many of the same control deficiencies in key information security process areas, including configuration management, identity and access management, incident response and reporting, security training, POA&Ms, remote access management, contingency planning, and contractor systems. Specifically, Williams, Adley continued to find the same systemic and pervasive information security weaknesses across its IT security posture since FY 2010. These key information security process areas have a direct impact on an effective organization-wide ISCM program. For example:

- ~~(SBU)~~ , BBG leaves its systems vulnerable to denial of service attacks, damage to the general support systems, and the potential introduction of security deficiencies.
- [Redacted] (b) (5)
- ~~(SBU)~~ [Redacted] (b) (5) , BBG leaves its systems vulnerable to denial of service attacks, damage to the general support systems, and the potential introduction of security deficiencies.

[43] **(U)** DHS, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, June 2015.
[44] **(U)** See Appendix D: FY 2015 Continuous Monitoring Maturity Model for additional details.

- (U) Without appropriate training of all personnel with access to BBG systems, including IT personnel with specific security responsibilities, users could compromise the security of the network, resulting in a loss of information; compromise Personally Identifiable Information; and introduce vulnerabilities to systems.
- (U) Without adequate identification, assessment, prioritization, and monitoring of corrective actions, the most important actions (highest security risks) affecting BBG may not be resolved within a timely manner, or communicated to senior management, thus exposing BBG's sensitive data, systems, and hardware to unauthorized access and potentially malicious attacks.
- [Redacted] (b) (5)
- ~~(SBU)~~ Without fully developed and implemented contingency plans that include business impact analyses, established and documented alternate sites for telecommunications, storage and processing, and backup strategies, BBG may be unable to access critical information and resources to perform mission critical business functions in the event of an extended outage and disaster.
- (U) By not documenting and enforcing the necessary oversight required by BBG for its external systems, there is an increased risk that BBG may be unaware of data that is collected and processed by its external systems and may be exposed to unauthorized access, use, disclosure, modification, or destruction.

Recommendation 2: (U) OIG recommends that the Chief Information Officer develop and implement an organization-wide information risk management strategy to identify, assess, respond to, and monitor information security risk at all levels of the organization in accordance with National Institute of Standards and Technology Special Publication 800-39. Specifically, the risk management strategy should align risk management decisions with business functions and objectives, which includes processes that respond to and monitor risk to operations and assets as well as performance-based outcomes by measuring, monitoring, and reporting risk management metrics to ensure that Broadcasting Board of Governors objectives are met.

(U) Management Response: The CIO concurred with this recommendation. BBG plans to define and implement policies, plans, procedures, training programs, and compliance assessment mechanisms for the agency's risk management program.

(U) OIG Reply: OIG considers the recommendation resolved because the CIO agreed to implement it. This recommendation will be closed when OIG receives and accepts documentation demonstrating the CIO has developed and implemented an organization-wide information risk management strategy to identify, assess, respond to, and monitor information security risk at all levels of the organization in accordance with NIST SP 800-39.

Recommendation 3: (U) OIG recommends that the Chief Information Security Officer define and implement the [Redacted] (b) (5)

including security controls, security status, and other metrics defined and monitored by the Broadcasting Board of Governors leadership in accordance with National Institute of Standards and Technology Special Publication 800-137.

(U) Management Response: The BBG Chief Information Security Officer (CISO) concurred with this recommendation. BBG plans to define and implement [Redacted] (b) (5) [redacted]

(U) OIG Reply: OIG considers this recommendation resolved because the CISO agreed to implement it. This recommendation will be closed when OIG receives and accepts documentation demonstrating the CISO has defined and implemented the [Redacted] (b) (5) [redacted] including security controls, security status, and other metrics defined and monitored by BBG leadership in accordance with NIST SP 800-137.

(U) RECOMMENDATIONS

Recommendation 1: (U) OIG recommends that the Chief Information Officer develop a strategy to realign information technology resources to balance operational needs with the need for an effective information security risk management strategy.

Recommendation 2: (U) OIG recommends that the Chief Information Officer develop and implement an organization-wide information risk management strategy to identify, assess, respond to, and monitor information security risk at all levels of the organization in accordance with National Institute of Standards and Technology Special Publication 800-39. Specifically, the risk management strategy should align risk management decisions with business functions and objectives, which includes processes that respond to and monitor risk to operations and assets as well as performance-based outcomes by measuring, monitoring, and reporting risk management metrics to ensure that Broadcasting Board of Governors objectives are met.

Recommendation 3: (U) OIG recommends that the Chief Information Security Officer define and implement the [Redacted] (b) (5), including security controls, security status, and other metrics defined and monitored by the Broadcasting Board of Governors leadership in accordance with National Institute of Standards and Technology Special Publication 800-137.

(U) APPENDIX A: 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 (Williams, Adley), an independent public accountant, to determine the effectiveness of the Broadcasting Board of Governors (BBG) information security program and whether security practices in FY 2015 complied with laws, regulations, and standards established by FISMA,[2] as amended by the Federal Information Security Modernization Act of 2014;[3] the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). Specifically, the audit assessed BBG's information security program and related practices for risk management and continuous monitoring, which include configuration management, identity and access management, incident response and reporting, security training, plans of action and milestones, remote access management, contingency planning, and contractor systems.[4]

(U) FISMA, as amended by the Federal Information Security Modernization Act of 2014, 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 another source. To ensure the adequacy and effectiveness of these controls, FISMA requires the agency's inspector general or an independent external auditor perform annual reviews of the information security program and to report those results to OMB and the Department of Homeland Security. The FY 2015 FISMA guidance from the Department of Homeland Security is intended to assist OIGs in reporting FISMA performance metrics. The updated FY 2015 Department of Homeland Security FISMA reporting metrics, dated June 19, 2015,[5] include the Council of Inspectors General on Integrity and Efficiency maturity model[6] for the continuous monitoring domain to provide perspective on the summary of the status of the agency's information security continuous monitoring program on a 5-level scale.

(U) Williams, Adley performed this audit from April 2015 through July 2015. Williams, Adley conducted this audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that Williams, Adley plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on

[1] **(U)** Public Law 107-347 Title III, Federal Information Security Management Act of 2002, December 2002.

[2] **(U)** Ibid.

[3] **(U)** Public Law 113-283, Federal Information Security Modernization Act of 2014, December 2014.

[4] **(U)** Although risk management is a part of continuous monitoring, due to the nature of the risk management deficiency, Williams, Adley has reported risk management issues separately.

[5] **(U)** Department of Homeland Security, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, June 2015.

[6] **(U)** See Appendix D: FY 2015 Continuous Monitoring Maturity Model

our audit objectives. Williams, Adley believes that the evidence obtained provides a reasonable basis for our findings and conclusions based on the audit objective.

(U) To perform this audit, Williams, Adley interviewed BBG senior management, employees, and contractors to evaluate managerial effectiveness and operational controls in accordance with NIST and OMB guidance. Williams, Adley observed daily operations, obtained evidence to support its conclusions and recommendations, tested effectiveness of established controls, conducted sampling where applicable, and collected written documents to supplement observations and interviews. In addition, Williams, Adley reviewed system generated outputs where possible to support our conclusions.

~~(SBU)~~ In prior years, OIG made recommendations to BBG for each key FISMA area separately. Each recommendation was provided to address individual control deficiencies that were identified for the applicable key information security process areas. For example, OIG made 18 recommendations in FY 2014.[7] Since BBG's corrective actions towards addressing prior year recommendations have not resolved these deficiencies, OIG is no longer making recommendations to address individual control deficiencies identified within the key information security process areas. Instead, OIG is focusing its recommendations on addressing the underlying cause for all control deficiencies. The intent of these recommendations is to provide guidance on the first steps that BBG needs to take in the development and implementation of an effective information security program, which would include identifying, analyzing, reporting, and responding to information security weaknesses, using risk-based decision making, at all levels of the organization. Williams, Adley separately notified BBG of all control deficiencies identified during the FY 2015 audit period on August 14, 2015. In addition, Williams, Adley has included the status of all prior year recommendations from the FY 2014 FISMA report in Appendix B.

(U) Prior OIG Reports

~~(SBU)~~ Williams, Adley has conducted an annual FISMA audit of the information security program for BBG since FY 2010, in which OIG provided 14 recommendations related to a total 9 of the 11 FISMA reportable areas tested.[8] Specifically in FY 2010, Williams, Adley identified weaknesses in every area except incident response and reporting and oversight of contractor systems. In the FY 2014 FISMA audit report,[9] Williams, Adley issued 18 recommendations to improve BBG's information security programs. In 2015, OIG closed 6 of 18 recommendations from the FY 2014 report.[10]

---

[7] **(U)** OIG, *Audit of the Broadcasting Board of Governors Information Security Program (*AUD-IT-IB-15-13, October 2014).

[8] **(U)** OIG, *Audit of the Broadcasting Board of Governors Information Security Program (*AUD/IT/IB-11-08, November 2010).

[9] **(U)** AUD-IT-IB-15-13, October 2014.

[10] **(U)** See Appendix B for the status of prior year findings.

(U) Work Related to Internal Controls

(U) Williams, Adley reviewed BBG's internal controls to determine whether:

- (U) BBG has established an enterprise-wide continuous monitoring program that assessed the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) BBG has established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) BBG has established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines; and identified users and network devices.
- (U) BBG has established and maintained an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) BBG has established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) BBG has established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) BBG has established a plans of action and milestones program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines; and tracked and monitored known information security weaknesses.
- (U) BBG has established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) BBG has established an entity-wide business continuity and disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) BBG has established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services external to the organization.

(U) Deficiencies identified with BBG's internal controls are presented in the "Audit Results" section of this report.

(U) Use of Computer-Processed Data

(U) During the audit, Williams, Adley used computer-processed data to obtain samples and information regarding the existence of information security controls. Williams, Adley obtained data extracted from BBG databases, Microsoft Excel, Active Directory, and enterprise software applications. For example, Williams, Adley utilized the BBG Active Directory to obtain a listing of users on the BBG network for testing procedures in control area Identify & Access Management. In addition, Williams, Adley assessed the reliability of the computer-generated data primarily by comparing selected data with source documentation as well as interviewing BBG Information Security Management Division officials who are responsible for compiling these data. Williams,

Adley determined that the information was sufficiently reliable for assessing the adequacy of related information security controls.

(U) Detailed Sampling Methodology

(U) For all samples selected during the audit, Williams, Adley used non-statistical audit sampling techniques where applicable and appropriate. As guidance, Williams, Adley used the American Institute of Certified Public Accountants Audit Guide Audit Sampling. This guidance assists in applying audit sampling in accordance with auditing standards. The audit strategy for the FY 2015 FISMA review uses a risk-based approach.

(U) With respect to the sampling methodology employed, *Government Auditing Standards* indicate that either a statistical or judgment sample can yield sufficient and appropriate audit evidence. A statistical sample is generally preferable, although it may not always be practicable. By definition, a statistical sample requires that each sampling unit in the population be selected via a random process and have a known, non-zero chance of selection. These requirements often have posed a problem when conducting audits of BBG. All information systems, irrespective of size or importance, must have a chance to be randomly selected. Therefore, the exclusion of one or more of the small or insignificant systems cannot be allowed. All information systems—large and small—must have a chance to be randomly selected, and that chance must not be zero. However, BBG would undoubtedly deem many small or insignificant information systems too atypical in most instances to merit inclusion in our sample.

(U) Consequently, Williams, Adley employed another type of sample permitted by *Government Auditing Standards*—namely, a non-statistical sample known as a judgment sample. A judgment sample is a sample selected by using discretionary criteria rather than criteria based on the laws of probability. In this audit, Williams, Adley has taken great care in determining the criteria to use for sampling information systems. Moreover, Williams, Adley used, whenever practicable, random numbers to preclude the introduction of any bias in sample selection although a non-statistical technique was utilized. Williams, Adley acknowledges that it is possible that the information security deficiencies identified in this report may not be as prevalent or may not exist at all in other information systems that were not tested. However, a prudent person without any basis in fact would not automatically assume that these deficiencies are non-existent with other systems. Such a supposition would be especially ill-advised for an issue as important as information security.

(U) Where Williams, Adley deemed it was appropriate, Williams, Adley used audit sampling techniques to perform audit procedures to less than 100 percent of the population to enable it to evaluate audit evidence of the items selected to assist in forming a conclusion concerning the population. Generally, for a large population of sample items (more than 2,000), Williams, Adley used non-statistical sampling methods to test 22 items.[11] For small populations and infrequently

[11] (U) *American Institute of Certified Public Accountants Audit Guide*, "AAG-SAM Appendix A," March 2012.

operating controls, Williams, Adley used guidance from the American Institute of Certified Public Accountants, as shown in Table A.1.

(U) Table A.1: Number of Items to Test From Small Populations

(U) Control Frequency and Population Size	(U) Items to Test
Quarterly (4)	2
Monthly (12)	2
Semimonthly (24)	3
Weekly (52)	5

(U) Source: *American Institute of Certified Public Accountants Audit Guide*, "Small Populations and Infrequently Operating Controls Table 3-5," March 2012.

(U) Williams, Adley followed this judgmental sampling methodology for these key process areas:

- (U) Continuous monitoring
- (U) Configuration management
- (U) Identity and access management
- (U) Risk management
- (U) Security training
- (U) Plans of action & milestones
- (U) Remote access management
- (U) Contingency planning

(U) Williams, Adley did not sample for the incident response and reporting key process area, as Williams, Adley reviewed the entire population of security incidents.

(U) APPENDIX B: FOLLOW-UP RECOMMENDATIONS FROM THE FY 2014 AUDIT OF THE BROADCASTING BOARD OF GOVERNORS INFORMATION SECURITY PROGRAM

(U) OIG has reviewed actions implemented by management to mitigate the findings identified in the FY 2014 Broadcasting Board of Governors (BBG) Federal Information Security Management Act of 2002 (FISMA) Report. The current status of each of the recommendations is as follows:

(U) **Recommendation 1:** OIG recommends that the Broadcasting Board of Governors perform a privacy impact assessment for its Office of Cuba Broadcasting Headquarters Network system, as required by National Institute of Standards and Technology Special Publication 800-37, Revision 1.

(U) *Status: Closed. OIG noted that the privacy impact assessments were performed for the systems noted in the recommendations from FY 2014.*

(U) **Recommendation 2:** OIG recommends that the Broadcasting Board of Governors perform a privacy impact assessment for its Privacy Information Enclave system, as required by National Institute of Standards and Technology Special Publication 800-37, Revision 1.

(U) *Status: Closed. OIG noted that the privacy impact assessments were performed for the systems noted in the recommendations from FY 2014.*

(U) **Recommendation 3:** OIG recommends that the Broadcasting Board of Governors update the Certification and Accreditation Policy and Procedures to identify the responsible organizations for conducting annual security control assessments.

(U) *Status: Closed. OIG noted that BBG updated its Certification and Accreditation related policy and procedures to identify the responsible organizations and positions for conducting annual security control assessments.*

(U) **Recommendation 4:** OIG recommends that the Broadcasting Board of Governors perform annual security control assessments on its Identity Management System.

(U) *Status: Closed. OIG noted that the annual security control assessment for Identity Management System was performed.*

(U) **Recommendation 5**: OIG recommends that the Director of Global Operations approve and implement a [Redacted] (b) (5) that assesses the security state of information systems and is consistent with National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) *Status: Resolved, pending further action. OIG noted that this recommendation remained open. As of our review,* [Redacted] (b) (5) *This recommendation can be closed when OIG receives and accepts documentation showing that BBG has formally approved a* [Redacted] (b) (5) *in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

~~(SBU)~~ **Recommendation 6**: OIG recommends that the Broadcasting Board of Governors approve and implement a contingency plan policy for [Redacted] (b) (5) contingency plans, as required by the National Institute of Standards and Technology, Special Publication 800-34, Revision 1.

~~(SBU)~~ *Status: Resolved, pending further action. OIG noted that this recommendation remained open. As of our review, BBG still had not approved and implemented a contingency plan policy for* [Redacted] (b) (5) *contingency plans. This recommendation can be closed when OIG receives and accepts documentation showing that BBG approved and implemented a contingency plan policy fo* [Redacted] (b) (5) *contingency plans, as required by NIST SP 800-34, Revision 1. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

~~(SBU)~~ **Recommendation 7**: OIG recommends that the Director of Global Operations complete and implement [redacted] contingency plans for all information systems and conduct necessary testing as required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, and NIST SP 800-53, Revision 4.

~~(SBU)~~ *Status: Resolved, pending further action. OIG noted that this recommendation remained open. As of our review, BBG still had not completed and implemente* [Redacted] (b) (5) *contingency plans for all information systems and had not conducted necessary testing. This recommendation can be closed when OIG receives and accepts documentation showing that BBG completed and implemente* [Redacted] (b) (5) *contingency plans for all information systems and conducted necessary testing as required by NIST SP 800-34, Revision 1, and NIST SP 800-53, Revision 4. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 8:** OIG recommends that the Director of Global Operations update server and workstation baseline procedures to include all of the U.S. Government Configuration Baseline configuration settings as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) *Status: Resolved, pending further action. OIG noted that this recommendation remained open. As of our review, BBG still had not updated server and workstation baseline procedures to include all of the U.S. Government Configuration Baseline configuration settings. This recommendation can be closed when OIG receives and accepts documentation showing that BBG updated server and workstation baseline procedures to include all of the U.S. Government*

Configuration Baseline configuration settings as required by NIST SP 800-53, Revision 4. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.

(U) **Recommendation 9:** OIG recommends that the Director of Global Operations remediate all critical vulnerabilities as they are identified through periodic scanning.

(U) *Status: Resolved, pending further action. OIG noted that this recommendation remained open. OIG found multiple critical vulnerabilities that were not remediated as of our review. This recommendation can be closed when OIG receives and accepts documentation showing that BBG remediated all critical vulnerabilities identified. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 10:** OIG recommends that the Director of Global Operations enforce the Broadcasting Board of Governors (BBG) Change Management Policy for all changes within the BBG environment.

(U) *Status: Resolved, pending further action. OIG noted that this recommendation remained open. As of our review, BBG still had changes that did not adhere to the BBG Change Management Policy. This recommendation can be closed when OIG receives and accepts documentation showing that BBG changes adhered to the BBG Change Management Policy. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 11:** OIG recommends that the Information Security Management Division update and implement the incident response policy and procedures to include preparation, detection and analysis, containment, eradication, recovery, and post-incident activity components as required by National Institute of Standards and Technology Special Publication 800-61, Revision 2.

(U) *Status: Resolved, pending further action. OIG noted that BBG had updated its incident response policy accordingly to include preparation, detection and analysis, containment, eradication, recovery, and post-incident activity components as required by NIST SP 800-61, Revision 2. However, BBG had not implemented the policy within the agency. This recommendation can be closed when OIG receives and accepts documentation showing that BBG implemented the incident response policy within the agency. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 12:** OIG recommends that the Information Security Management Division adhere to the *Computer Security Incident Management Policy*, when finalized, to include the appropriate category level for every documented incident.

(U) *Status: Resolved, pending further action. OIG noted that BBG had updated its incident response policy; however, it was noted that incidents were still missing the appropriate category levels. This recommendation can be closed when OIG receives and accepts documentation*

showing that BBG incidents received appropriate category levels. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.

(U) Recommendation 13: OIG recommends that the Director of Global Operations, in coordination with the system owners and the Office of the Chief Information Officer, ensure that Broadcasting Board of Governors' Plans of Action and Milestones (POA&M) include all required elements in accordance with the *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 latest status.

(U) *Status: Resolved, pending further action. OIG noted that while BBG is continuing to make progress on this recommendation, plans of action and milestones still continued to lack all the required elements in accordance with the Information Security Plans of Action and Milestones Policy, to include severity of the weakness, responsible organization, estimated funding resources, completion date, key milestones and changes, source of the weakness, and the latest status. This recommendation can be closed when OIG receives and accepts documentation showing that BBG plans of action and milestones include all required elements in accordance with the Information Security Plans of Action and Milestones Policy. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) Recommendation 14: OIG recommends that the Enterprise Networks and Storage Division implement procedures to assess the adequacy of the security configurations of remote computers that request access to the Broadcasting Board of Governors' (BBG) network and grant access only to properly configured and patched devices, as required by BBG's Virtual Private Network (VPN) policy and VPN Access Acceptance Form.

(U) *Status: Resolved, pending further action. OIG noted that this recommendation remained open. As of our review, BBG still had not implemented procedures to assess the adequacy of the security configurations of remote computers that request access to the BBG network and to grant access only to properly configured and patched devices, as required by BBG's Virtual Private Network policy and Virtual Private Network Access Acceptance Form. This recommendation can be closed when OIG receives and accepts documentation showing that BBG implemented procedures to assess the adequacy of the security configurations of remote computers that request access to the BBG network and to grant access only to properly configured and patched devices, as required by BBG's Virtual Private Network policy and Virtual Private Network Access Acceptance Form. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) Recommendation 15: OIG recommends that the Enterprise Networks and Storage Division ensure that multiple personnel are trained, and utilize that training, to disable Virtual Private Network tokens after they are reported lost or stolen in accordance with National Institute of Standards and Technology, Special Publication 800-53, Revision 4.

(U) *Status: Closed. OIG noted that all lost or stolen Virtual Private Network tokens were disabled and accounted for in accordance with NIST, SP 800-53, Revision 4.*

(U) **Recommendation 16**: OIG recommends that the Director of Global Operations and system owners ensure that user accounts are properly maintained in accordance with Broadcasting Board of Governors' *Identification and Authentication Policy*.

(U) *Status: Resolved, pending further action. OIG noted that while BBG is continuing to make progress on this recommendation, user accounts were found to be out of compliance with BBG's Identification and Authentication Policy. This recommendation can be closed when OIG receives and accepts documentation showing that BBG user accounts are found to be in compliance with BBG's Identification and Authentication Policy. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 17:** OIG recommends that the Director of Global Operations, in coordination with the Office of Security, complete the issuance of Personal Identity Verification cards as required by Homeland Security Presidential Directive 12 and Office of Management and Budget guidelines.

(U) *Status: Resolved, pending further action. OIG noted that while BBG is continuing to make progress on this recommendation, as of our review, BBG had not completed the issuance of Personal Identity Verification cards as required by Homeland Security Presidential Directive 12 and Office of Management and Budget guidelines. This recommendation can be closed when OIG receives and accepts documentation showing that BBG completed the issuance of Personal Identity Verification cards as required by Homeland Security Presidential Directive 12 and Office of Management and Budget guidelines. OIG will follow up on the status of this recommendation during the FY 2016 FISMA audit.*

(U) **Recommendation 18:** OIG recommends that the Director of Global Operations finalize and implement a role-based security training policy, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) *Status: Closed. A policy for role-based training was approved in June 2015 for employees and contractors with significant security responsibilities.*

(U) APPENDIX C: FY 2015 FISMA REPORTABLE AREAS

(U) FISMA Reportable Area	(U) Definition
(U) Continuous Monitoring	(U) The purpose of continuous monitoring is to make hardware assets harder to exploit through hardware asset management, software asset management, secure configuration management, and vulnerability management.
(U) Configuration Management	(U) The purpose of configuration management is to manage the effects of changes or differences in configurations on an information system or network. Configuration management is an essential component of monitoring the status of security controls and identifying potential security-related problems in information systems. This information can help security managers understand and monitor the evolving nature of vulnerabilities as they appear in a system under their responsibility, thus enabling managers to direct appropriate changes as required. The goal of configuration management is to make assets harder to exploit through better configuration.
(U) Identity and Access Management	(U) Users and devices must be authenticated to ensure that they are who or what they identify themselves to be. The purpose of identity and access management is to ensure that users and devices are properly authorized to access information and information systems.
(U) Incident Response and Reporting	(U) The purpose of incident response and reporting is to determine the kinds of attacks that have been successful and position the organization to make a risk based decision about where it is most cost effective to focus its security resources. A well-defined incident response capability helps the organization detect incidents rapidly, minimize loss and destruction, identify weaknesses, and restore IT operations quickly.
(U) Risk Management	(U) The purpose of risk management focuses on how an organization is evaluating risk and prioritizing security issues.
(U) Security Training	(U) Establishing and maintaining a robust and relevant information security training process as part of the overall information security program is the primary conduit for providing a workforce with the information and tools needed to protect an agency's vital information resources. This will ensure that personnel at all levels of the organization understand their information security responsibilities to properly use and protect the information and resources entrusted to them. Organizations that continually train their workforce in organizational security policy and role-based security responsibilities will have a higher rate of success in protecting information.
(U) POA&Ms	(U) The purpose of POA&Ms is to assist in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. POA&Ms track the measures implemented to correct deficiencies and to reduce or eliminate known vulnerabilities. POA&Ms can also assist in identifying performance gaps, evaluating an organization's security performance

(U) FISMA Reportable Area	(U) Definition
	and efficiency, and conducting oversight. It is an essential part of the risk management process to track problems and to decide which issues to address, and shows an organization's efforts to address corrective action with a standard and centralized approach.
(U) Remote Access Management	**(U)** The purpose of remote access management is to help deter, detect, and defend against unauthorized network connections/access to internal and external networks. Secure remote access is essential to an organization's operations because the proliferations of system access through telework, mobile devices, and information sharing means that information security is no longer confined within system perimeters. Organizations also rely on remote access as a critical component of contingency planning and disaster recovery.
(U) Contingency Planning	**(U)** Contingency planning involves the actions required to plan for, respond to, and mitigate damaging events. As such, the purpose of contingency planning is to give attention to rare events that have the potential for significant consequences and promoting first priority risk.
(U) Contractor Systems	**(U)** The purpose of contractor systems is to ensure that information systems operated by contractors and other external entities on behalf of the federal government meet all applicable security requirements.

(U) Source: DHS, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics.*

(U) APPENDIX D: FY 2015 CONTINUOUS MONITORING MATURITY MODEL

(U) Level	(U) Definition
1 Ad-hoc	**(U)** Information Security Continuous Monitoring (ISCM) program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53, SP 800-137, Office of Management and Budget (OMB) Memorandum M-14-03, and the Chief Information Officer (CIO) ISCM Concept of Operations (CONOPS). • **(U)** ISCM activities are performed without the establishment of comprehensive policies, procedures, and strategies developed consistent with NIST SP 800-53, SP 800-137, OMB Memorandum M-14-03, and the CIO ISCM CONOPS. • **(U)** ISCM stakeholders and their responsibilities have not been defined and communicated across the organization. • **(U)** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. • **(U)** The organization lacks personnel with adequate skills and knowledge to effectively perform ISCM activities. • **(U)** The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. • **(U)** The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. • **(U)** ISCM activities are not integrated with respect to organizational risk tolerance, the threat environment, and business/mission requirements. • **(U)** There is no defined process for collecting and considering lessons learned to improve ISCM processes. • **(U)** The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions.

(U) Level	(U) Definition
2 **Defined**	**(U)** The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB Memorandum M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide. • **(U)** ISCM activities are defined and formalized through the establishment of comprehensive ISCM policies, procedures, and strategies developed consistent with NIST SP 800-53, SP 800-137, OMB Memorandum M-14-03, and the CIO ISCM CONOPS. • **(U)** ISCM stakeholders and their responsibilities have been defined and communicated across the organization, but stakeholders may not have adequate resources (people, processes, tools) to consistently implement ISCM activities. • **(U)** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. • **(U)** The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. • **(U)** The organization has identified and fully defined the ISCM technologies it plans to utilize in the ISCM automation areas. Automated tools are implemented to support some ISCM activities but the tools may not be interoperable. In addition, the organization continues to rely on manual/procedural methods in instances where automation would be more effective. • **(U)** The organization has defined how ISCM activities will be integrated with respect to organizational risk tolerance, the threat environment, and business/mission requirements. However, the organization does not consistently integrate its ISCM and risk management activities. • **(U)** The organization has defined its process for collecting and considering lessons learned to make improvements to its ISCM program. Lessons learned are captured but are not shared at an organizational level to make timely improvements. • **(U)** ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions.
3 **Consistently Implemented**	**(U)** In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions consistent with NIST SP 800-53, SP 800-137, OMB Memorandum M-14-03, and the CIO ISCM CONOPS. • **(U)** The ISCM program is consistently implemented across the organization, in accordance with the organization's ISCM policies, procedures, and strategies and NIST SP 800-53, SP 800-137, OMB Memorandum M-14-03, and the CIO CONOPS. • **(U)** ISCM stakeholders have adequate resources (people, processes, technologies) to effectively accomplish their duties.

(U) Level	(U) Definition
	• **(U)** The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. • **(U)** The organization has standardized and consistently implemented its defined technologies in all of the ISCM automation areas. ISCM tools are interoperable, to the extent practicable. • **(U)** ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements. • **(U)** The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes. • **(U)** ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations.
4 **Managed and Measurable**	**(U)** In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations. • **(U)** Qualitative and quantitative measures on the effectiveness of the ISCM program are collected across the organization and used to assess the ISCM program and make necessary changes. • **(U)** Data supporting ISCM metrics is obtained accurately, consistently, and in a reproducible format, in accordance with the organization's ISCM policies, procedures, and strategies and NIST SP 800-53, SP 800-137, OMB Memorandum M-14-03, and the CIO CONOPS. • **(U)** ISCM data is analyzed consistently and collected and presented using standard calculations, comparisons, and presentations. • **(U)** ISCM metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities, including situational awareness and risk response. • **(U)** ISCM metrics provide persistent situational awareness to stakeholders across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations, the organization's infrastructure, and security domains. • **(U)** ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (that is, System Security Plan Risk Assessment Report, Security Assessment Report, and Plans of Action and Milestones) up to date on an ongoing basis.
5 **Optimized**	**(U)** In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape. • **(U)** Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. • **(U)** The ISCM program is integrated with strategic planning, enterprise

(U) Level	(U) Definition
	architecture and capital planning and investment control processes. • **(U)** The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact.

(U) Source: Department of Homeland Security, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics.*

(U) APPENDIX E: CRITERIA FOR FINDINGS

(U) Table E.1: Continuous Monitoring Requirements

(U) Law or Regulation	(U) Requirement
(U) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4	**(U)** NIST SP 800-53, rev. 4[a] requires that the organization establish a continuous monitoring strategy and implement a continuous monitoring program.
(U) NIST SP 800-137	**(U)** NIST SP 800-137[b] states, **"**The criteria for Information Security Continuous Monitoring (ISCM) are defined by the organization's risk management strategy, including how the organization plans to assess, respond to, and monitor risk, and the oversight required to ensure that the risk management strategy is effective." Furthermore, "Security controls, security status, and other metrics defined and monitored by officials at this tier are designed to deliver information necessary to make risk management decisions in support of governance."
(U) Council of the Inspectors General on Integrity and Efficiency ISCM Maturity Model For FY 2015	**(U)** In addition, the Council of the Inspectors General on Integrity and Efficiency ISCM Maturity Model For FY 2015[c] defines a Level 1 Ad-hoc maturity level as the following: **(U)** ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, Office of Management and Budget Memorandum M-14-03, and the Chief Information Officer ISCM Concept of Operations.

[a] **(U)** NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations,""CA-7 Continuous Monitoring," January 2015.
[b] **(U)** NIST SP 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations," "2.1.1 Tier-1 Organization," September 2011.
[c] **(U)** Department of Homeland Security, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, June 2015.

(U) Source: NIST SP 800-53, rev. 4; NIST SP 800-137; and Department of Homeland Security, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics.*

(U) Table E.2: Configuration Management Requirements

(U) Law or Regulation	(U) Requirement
(U) NIST SP 800-53, rev. 4	**(U)** NIST SP 800-53, rev. 4* states, **"**The organization identifies, reports, and corrects information system flaws."

* **(U)** NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," "SI-2 Flaw Remediation," January 2015.
(U) Source: NIST SP 800-53, rev. 4.

(U) Table E.3: Incident Response and Reporting Requirements

(U) Law or Regulation	(U) Requirement
(U) NIST SP 800-115	**(U)** NIST SP 800-115* states that the organization's information security assessment policy should address the following: 1. **(U)** Organizational requirements with which assessments must comply. 2. **(U)** Appropriate roles and responsibilities (at a minimum, for those individuals approving and executing assessments). 3. **(U)** Adherence to established methodology. 4. **(U)** Assessment frequency. 5. **(U)** Documentation requirements, such as assessment plans and assessment results.

* **(U)** NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment," "6.1 Developing a Security Assessment Policy," September 2008.

(U) Source: NIST SP 800-115.

(U) Table E.4: Security Training Requirements

(U) Law or Regulation	(U) Requirement
(U) XI Broadcast Administrative Manual 300 Information Security Awareness and Role-Based Training Policy	**(U)** The Information Security Awareness and Role-Based Training Policy[a] requires all new employees at agency headquarters to receive information security awareness training during their initial orientation. If circumstances prevent completion of the training during orientation, new employees are required to complete an on-line course at the time they receive their agency computer account from agency Technical Support Services staff.
(U) NIST SP 800-53, rev. 4	**(U)** NIST SP 800-53, rev. 4[b] states, the "organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training."

[a] **(U)** Broadcasting Board of Governors, XI Broadcast Administrative Manual 300 Information Security Awareness and Role-Based Training Policy, June 2015.

[b] **(U)** NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," "AT-4 Security Training Records," January 2015.

(U) Source: XI Broadcast Administrative Manual 300 Information Security Awareness and Role-Based Training Policy; and NIST SP 800-53, rev. 4.

(U) Table E.5: Plan of Action and Milestones Requirements

(U) Law or Regulation	(U) Requirement
(U) Office of Management and Budget Memorandum M-11-33	**(U)** Office of Management and Budget Memorandum M-11-33* states, "The required data elements are weakness, responsible organization, estimated funding resources, completion date, key milestones and changes, source of the weakness, and the status."

* **(U)** Office of Management and Budget Memorandum M-11-33, "FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management."

(U) Source: Office of Management and Budget Memorandum M-11-33.

(U) Table E.6: Remote Access Requirements

(U) Law or Regulation	(U) Requirement
(U) International Broadcasting Bureau IT Directorate Virtual Private Network Policy	**(U)** The Virtual Private Network Policy* states, "Approved International Broadcasting Bureau employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of Virtual Private Networks, which are a "user managed" service.

* **(U)** International Broadcasting Bureau Information Technology Directorate, "Virtual Private Network (VPN) Policy," June 2015.

Source: International Broadcasting Bureau Information Technology Directorate, Virtual Private Network Policy.

(U) Table E.7: Contingency Planning Requirements

(U) Law or Regulation	(U) Requirement
(U) NIST SP 800-34, rev. 1	**(U)** NIST SP 800-34, rev. 1[a] states: **(U)** An up-to-date Information Security Contingency Plan is essential for successful Information Security Contingency Plan operations. As a general rule, the Information Security Contingency Plan should be reviewed for accuracy and completeness at least annually, as well as upon significant changes to any element of the Information Security Contingency Plan, system, mission/business processes supported by the system, or resources used for recovery procedures. Deficiencies identified through testing should be addressed during plan maintenance. Elements of the plan subject to frequent changes, such as contact lists, should be reviewed and updated more frequently. **(U)** NIST SP 800-34, rev. 1[b] states, "the organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information."

[a] **(U)** NIST SP 800-34, rev. 1, "Contingency Planning Guide for Federal Information Systems," "13. How often should my ISCP be updated?" May 2010.
[b] **(U)** NIST SP 800-34, rev. 1, "Contingency Planning Guide for Federal Information Systems," "CP-6 Alternate Storage Site," May 2010.

(U) Source: NIST SP 800-34, rev. 1.

(U) APPENDIX F: BROADCASTING BOARD OF GOVERNORS RESPONSE

BROADCASTING BOARD OF GOVERNORS
UNITED STATES OF AMERICA

November 3, 2015

Mr. Norman P. Brown
Assistant Inspector General for Audits
Office of Inspector General
U.S. Department of State

Dear Mr. Brown:

The Broadcasting Board of Governors (BBG) has reviewed the Office of Inspector General (OIG) draft report, "Audit of the Broadcasting Board of Governors Information Security Program," AUD-IT-IB-16-XX, October 2015.

BBG appreciates the opportunity to address the report's recommendations as provided in the enclosure, and will continue to work with the OIG to improve the Agency's risk management program.

Please do not hesitate to contact us should you have any questions.

Sincerely,

John F. Lansing
Chief Executive Officer and Director

Enclosure

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

Enclosure

CONTROLLED UNCLASSIFIED INFORMATION
(UNCONTROLLED when removed from enclosure)

BBG's Response to OIG's Draft "Audit of the Broadcasting Board of Governors Information Security Program,"
Report Number AUD-IT-IB-16-XX, October 2015
Sensitive but Unclassified

(U) Recommendation 1. OIG recommends that the Chief Information Officer develop a strategy to realign information technology resources to balance operational needs with the need for an effective information security risk management strategy.

(U) BBG Response (October 30, 2015): The CIO concurs and will realign information technology resources to perform effective information security risk management.

(U) Recommendation 2. OIG recommends that the Chief Information Officer develop and implement an organization-wide information risk management strategy to identify, assess, respond to, and monitor information security risk at all levels of the organization in accordance with National Institute of Standards and Technology Special Publication 800-39. Specifically, the risk management strategy should align risk management decisions with business functions and objectives, which includes processes that respond to and monitor risk to operations and assets as well as performance-based outcomes by measuring, monitoring, and reporting risk management metrics to ensure that Broadcasting Board of Governors' objectives are met.

(U) BBG Response (October 30, 2015): The CIO concurs and will define and implement policies, plans, procedures, training programs, and compliance assessment mechanisms for the Agency's Risk Management Program.

(U) Recommendation 3. OIG recommends that the Chief Information Security Officer define and implement the [Redacted] (b) (5) including security controls, security status, and other metrics defined and monitored by the Broadcasting Board of Governors leadership in accordance with National Institute of Standards and Technology Special Publication 800-137.

(U) BBG Response (October 30, 2015): The BBG CISO concurs and will define and implement criteria for the Agency's [Redacted] (b) (5)

1

(U) ABBREVIATIONS

AD	Active Directory
BBG	Broadcasting Board of Governors
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CONOPS	Concept of Operations
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act of 2002
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&Ms	plans of action and milestones
SP	Special Publication

HELP FIGHT

FRAUD. WASTE. ABUSE.

1-800-409-9926
OIG.state.gov/HOTLINE

If you fear reprisal, contact the
OIG Whistleblower Ombudsman to learn more about your rights:

OIGWPEAOmbuds@state.gov