OIG

Office of Inspector General

U.S. Department of State • Broadcasting Board of Governors

AUD-IT-IB-16-44 Office of Audits August 2016

Information Report: Description of Policies and Computer Security Controls for Select Broadcasting Board of Governors Covered Systems

INFORMATION REPORT

Summary of Project

The Consolidated Appropriations Act, 2016,[1] (Act) Section 406, Federal Computer Security, requires the Inspector General of each covered agency[2] to submit a report that contains a description of controls utilized by covered agencies to protect sensitive information maintained, processed, and transmitted by a covered system. Specifically, the Act requires a description of controls utilized by covered agencies to protect two types of data contained within covered systems: personally identifiable information (PII) data and national security data.

Acting on the Office of Inspector General's behalf, Williams, Adley & Company-DC, LLP (Williams Adley), an independent public accounting firm, collected information about the Broadcasting Board of Governors (BBG) computer systems[3] and reviewed security controls for two of three systems identified by BBG containing PII systems: Privacy Information Enclave (PIE) and Identification Management System (IDMS).

This report describes the policies and controls used by BBG for each of the five specific topics identified in the Act: (1) logical access policies and practices; (2) logical access controls[4] and multi-factor authentication[5] used; (3) the reasons logical access controls or multi-factor authentication have not been used; (4) information security management practices used for covered systems; and (5) policies and procedures that ensure information security management practices are effectively implemented by other entities such as contractors.

With respect to logical access policies and practices, Williams Adley found that BBG did not have specific policies documenting logical access controls for PIE and IDMS. Instead, BBG documented logical access control policies for PIE and IDMS within System Security Plans (SSP). Each SSP included the relevant security controls at the system level as required.

With respect to access and multi-factor authentication, Williams Adley found that BBG does not use personal identity verification (PIV) multi-authentication to govern privileged user access to PIE. In addition, BBG permits remote access for privileged functions to PIE for compelling operational needs. BBG officials stated that there were no non-privileged user accounts on IDMS. Currently, there are two dedicated workstations that allow privileged

[1] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2984, Section 406.

[2] According to the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2984, Section 406, Federal Computer Security, the term "covered agency" means an agency that operates a covered system.

[3] According to a BBG official, BBG does not maintain any National Security Systems.

[4] According to the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2984, Section 406, the term "logical access control" means a process of granting or denying specific requests to obtain and use information and related information processing services.

[5] According to the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2984, Section 406, the term "multi-factor authentication" means the use of not fewer than 2 authentication factors, such as the following: (A) Something that is known to the user, such as a password or personal identification number. (B) An access device that is provided to the user, such as a cryptographic identified device or token. (C) A unique biometric characteristic of the user.

access to IDMS. Privileged users are required to have a PIV card and pin, or PIV card and biometrics information, to access IDMS. Remote access is not allowed. Also, IDMS is operated by a third-party vendor as a managed service and is configured with one privileged account that is managed, controlled, and protected by the vendor for system administration and maintenance purposes.

With respect to why logical access controls or multi-factor authentication are not being used, BBG officials stated that the multi-factor authentication was not completed due to insufficient funding. In addition, the IDMS system was not fully developed to implement physical access controls to BBG facilities and logical access controls to BBG PII systems in accordance with the multi-factor authentication. However, BBG has been invited to participate in the U.S. Department of Homeland Security's Credential Management Tool Procurement, which will supplement BBG's PIV card logical access capabilities.

With respect to information security management practices used for covered systems, according to BBG officials the agency has not implemented data loss prevention or digital rights management solutions at the agency level or for the PII systems reviewed (PIE and IDMS). However, BBG has established alternative controls at the entity level including: (1) implementing a policy prohibiting physical documented records containing PII from being sent or removed from BBG's premises; (2) implementing a policy preventing removal of portable storage devices that contain PII—considered data at endpoint—from BBG premises; (3) automatically logging remote access to BBG's network for accountability; (4) properly retiring PII to the National Archives and Records Administration or destroying it when documents or devices containing PII are no longer necessary; and (5) properly retiring hardware and portable storage media by sanitizing them before disposal by using a wipeout utility or physically destroying them.

With respect to policies and procedures that ensure information security management practices are implemented by other entities such as contractors, Williams Adley found that BBG has not developed information security policies and procedures to ensure that all contracted/hosted information systems that contain BBG PII are implementing information security management practices. BBG officials stated that BBG has been relying on Memoranda of Agreement and Interconnection Security Agreements to manage the security and privacy controls.

Williams Adley provided a description of other security management practices used by the agency. For example, BBG stated it is using separate tools to track licenses associated with the software assets for its PII systems. However, a BBG official acknowledged that the agency does not have information security policies and procedures documented at the agency level to manage software assets installed on the PII systems. BBG officials also stated that BBG has implemented limited intrusion detection tools to monitor its PII systems and provide forensics and visibility capability to detect and remediate information security threats. However, BBG officials acknowledged that the agency has not implemented any specific technology

solutions to manage its data loss prevention and digital rights management capabilities at the agency level and for the two PII systems reviewed.

BBG responded to a draft of this report on August 1, 2016. In its response, BBG proposed alternative language to protect sensitive details about security controls involving PII, in addition to providing additional details about its policies and procedures intended to protect PII. BBG's comments were considered and incorporated in this report when appropriate. BBG's comments are reprinted in Appendix D.

OBJECTIVE

The Consolidated Appropriations Act, 2016, Section 406, Federal Computer Security, requires the Inspector General of each covered agency to submit a report, which shall include information collected from the covered agency regarding computer systems for the following topics:

A. A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.
B. A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.
C. If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.
D. A description of the following information security management practices used by the covered agency regarding covered systems:
    i. The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.
    ii. What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including –
        I. data loss prevention capabilities;
        II. forensics and visibility capabilities; or
        III. digital rights management capabilities.
    iii. A description of how the covered agency is using the capabilities described in clause (ii).
    iv. If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.
E. A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph D above. See Appendix A for the purpose, scope, and methodology; and Appendix B for a list of access controls for information systems with PII for privileged users.

BACKGROUND

BBG is an independent Federal agency that supervises all U.S. Government civilian international broadcasting. BBG works to serve as an example of a free and professional press, reaching a worldwide audience with news, information, and relevant discussions. BBG broadcasters distribute programming in 61 languages via radio, television, the internet, and other news media. 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 BBG Chief Information Officer (CIO) has overall responsibility for managing the information security program with support of key personnel including a Chief Information Security Officer (CISO) and a Senior Agency Official for Privacy. The CISO is primarily responsible for drafting information security policies and procedures, maintaining the Information Security Program Policy, developing and implementing a plan for agency compliance with the policy, monitoring compliance with the policy, and informing the CIO of any failure to comply. Furthermore, the CISO is responsible for coordinating the identification and analysis of threats, coordinating the BBG Computer Security Incident Response Team responses to information security incidents, and reporting to agency management. The CISO is also responsible for coordinating the selection and implementation of information security defenses; coordinating agency awareness efforts; and coordinating agency compliance efforts, including system security assessments and authorization recommendations to the CIO. The Senior Agency Official for Privacy has overall responsibility and accountability for ensuring BBG's implementation of information privacy protections, including BBG's full compliance with Federal laws, regulations, and policies relating to information privacy.

Cyber Security Trends

According to a Government Accountability Office (GAO) report,[6] since FY 2006, the number of information security incidents affecting Federal agencies information systems has steadily increased each year—rising from 5,503 in FY 2006 to 67,168 in FY 2014, an increase of 1,121 percent. In another GAO report,[7] the number of reported security incidents involving PII at Federal agencies has more than doubled in recent years—from 10,481 incidents in FY 2009 to 27,624 incidents in FY 2014. Recent examples that highlight the impact of such incidents include:

- The BBG CIO stated[8] that, "when I first came on board in 2009, every single server in this agency was controlled by the Chinese cyber army and they could have literally dropped

[6] GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices* (GAO-14-354, April 2014).
[7] GAO, *Information Security: Federal Agencies Need to Better Protect Sensitive Data* (GAO-16-194T, November 2015).
[8] According to the media, <http://federalnewsradio.com/cybersecurity/2016/04/broadcasting-board-governors-kicked-chinese-network-remains-vigilant-cyber-attacks-continue/>, accessed on May 23, 2016.

this agency with one key stroke. Fortunately they chose never to do so, but at the same time we knew they were exfiltrating literally gigabyte upon gigabyte of information every day."

- The Director of the Office of Personnel Management acknowledged[9] that the number of individuals with data compromised from the personnel records incident in 2015 was approximately 4.2 million. Two separate incidents involved the exfiltration of personnel records and background investigation data in two different information systems.

Federal Laws, Standards, and Guidelines

The Consolidated Appropriations Act, 2016, Section 406, Federal Computer Security, enacted on December 18, 2015, requires Inspectors General from each covered agency[10] to provide a report containing a description of controls utilized by covered agencies to protect sensitive information maintained, processed, and transmitted by a covered system.[11] The Consolidated Appropriations Act requests a description of controls utilized by covered agencies to protect two types of data contained within covered systems: PII data and national security data.

Protection of personal information in the Federal government is mandated by the Privacy Act of 1974[12] and the Health Insurance Portability and Accountability Act of 1996.[13] The Privacy Act establishes controls over what personal information can be collected, maintained, used, and disseminated by Federal agencies. Within the Health Insurance Portability and Accountability Act, the Privacy Rule establishes national standards to protect individuals' medical records and other personal health information. The Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.[14]

The Office of Management and Budget (OMB) published Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," in May 2007. OMB M-07-16 requires all Federal agencies to develop and implement various security and operational requirements that Federal agencies must adhere to in order to sufficiently protect PII.[15]

---

[9] "Under Attack: Federal Cybersecurity and the OPM Data Breach: Hearing before the Committee on Homeland Security and Governmental Affairs," U.S. Senate (2015), <https://www.opm.gov/news/testimony/114th-congress/under-attack-federal-cybersecurity-and-the-opm-data-breach.pdf>, accessed on June 10, 2016.
[10] According to the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2984, Section 406, the term "covered agency" means an agency that operates a covered system.
[11] According to the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2984, Section 406, the term "covered system" shall mean a National Security System as defined in section 11103 of title 40, United States Code, or a Federal computer system that provides access to personally identifiable information.
[12] Privacy Act of 1974, 5 U.S.C. § 552a (December 1974).
[13] Health Insurance Portability and Accountability Act of 1996, Pub. Law No. 104-191, (August 1996).
[14] According to the U.S. Department of Health and Human Services, <http://www.hhs.gov/hipaa/for-professionals/privacy/>, accessed on June 10, 2016.
[15] OMB, Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," (May 2007).

For information systems that process, transmit, or contain PII, the National Institute of Standards and Technology (NIST) published NIST Special Publication (SP) 800-53, rev. 4,[16] which provides a catalog of security and privacy controls for Federal information systems and organizations. For example, NIST SP 800-53 provides a process for selecting information security controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk.

BBG's Personally Identifiable Information and National Security Systems

BBG identified three systems that had PII information in its current production environment. Williams Adley reviewed two of the three PII systems identified by BBG officials—the Privacy Information Enclave (PIE) and the Identification Management System (IDMS). BBG officials stated that the agency did not maintain any National Security Systems.

PIE was created as a repository for storing employee and vendor data used in BBG's administrative business processes. The data is mainly used to support payroll, human resources, financial, and business travel processes. PIE stores PII data including Social Security numbers, names, ages, dates of birth, home addresses, email addresses, occupations, salaries, and work history.

IDMS was developed to support the Homeland Security Presidential Directive 12[17] and other Federal standards and guidelines (Privacy Act of 1974,[18] OMB Memorandum M-05-24,[19] and Federal Information Processing Standard 201[20]) that established a requirement for a common identification standard for Federal employees and contractors. To support the implementation, IDMS provides a centralized platform to capture users' access data such as demographic and biometric information within the BBG personal identity verification (PIV) credential. Upon completion of the biometric verification of a cardholder, IDMS issues a PIV card for an employee or contractor to gain physical access to BBG facilities and logical access to BBG information systems. IDMS collects PII data including Social Security number, name, address, and security clearance level.

[16] NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," "AT-4 Security Training Records," January 2014.
[17] Homeland Security Presidential Directive 12,"Policies for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004.
[18] Privacy Act of 1974, 5 U.S.C. § 552a.
[19] OMB Memorandum M-05-24, "Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractors," August 5, 2005.
[20] Federal Information Processing Standards Publication 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors, "August 2013.

RESULTS

Section A. Logical Access Policies and Practices

The Act requires the Inspector General to provide a description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.

Agency-wide Logical Access Control Policies

BBG drafted agency-wide policies—"Computer Security Identification and Authentication Policy" and "Information Technology Acceptable Use Policy"—related to logical access controls in FY 2016.[21] The draft "Computer Security Identification and Authentication Policy" contains guidance on user account types (for example, service, shared, and administrator) and security configuration settings, such as password requirements. BBG also has developed a policy, entitled "Account Management Standard Operating Procedures," which documents BBG's account provisioning and deactivation process.

BBG has a PII policy, "Safeguarding Personally Identifiable Information Policy,"[22] which contains the administrative, technical, and physical safeguards to prevent unauthorized PII disclosure. For example, a user must use encryption (approved by the Deputy CIO) to store or transmit PII via agency email and a user is prohibited from utilizing his or her private email to transmit any PII. Also, remote access to PII must be approved by the Information System Security Officer (ISSO) and must utilize the technical solution implemented by the agency. The ISSO is responsible for auditing access to the PII system and monitoring for data breaches or unauthorized activity. In addition, users are required to report confirmed or suspected breaches to the CISO.

System-Level Logical Access Control Policies

Williams Adley found that BBG did not have specific policies documenting logical access controls for PIE and IDMS. Instead, BBG documented logical access control policies for PIE and IDMS within System Security Plans. Each System Security Plan included the relevant security controls at the system level in accordance with NIST SP 800-53 minimum security control requirements. Williams Adley compared BBG's logical access policies and procedures to Federal standards and determined that BBG did not consistently include Federal standards in its policies and procedures (see Appendix C).

[21] BBG is updating the draft "Computer Security Identification and Authentication Policy" based on recommendations from a previous Office of Inspector General audit—*Audit of the Broadcasting Board of Governors Information Security Program* (AUD-IT-IB-16-17, November 2015).

[22] The Safeguarding Personally Identifiable Information Policy is BBG specific policy.

Logical Access Control Practices

According to BBG officials, Active Directory is used to manage users' logical access at the agency level. Active Directory is a directory service created by Microsoft for Windows domain networks. It provides a capability for BBG to centrally manage network groups, users, computers (servers and workstations), printers, network shares, and system information, while enforcing information security standards and standardizing network configuration across the agency.

BBG officials stated that BBG isolated the PIE system using a virtual environment and multiple layers of logical access controls. Only a limited number of dedicated workstations are granted privileges to access the PIE system and data. In addition, a server functions as the virtual desktop for users accessing the PIE system, which mitigates the risk of downloading PII data. BBG stated that only a small number of users and IT staff have access to the PIE system. The Enterprise Platforms Division Manager, who ultimately reports to the CIO, is responsible for account management, which includes routinely disabling temporary system accounts and automatically disabling inactive accounts.

Dedicated BBG workstations are required to gain access to the IDMS system. To access the IDMS front-end application, Enrollment Manager, a user must have a unique user account with role-based permissions. Based on the role, the user has the ability to access IDMS and perform specific actions or view specific information.

On a monthly basis, the IDMS Information System Owner reviews the list of IDMS users to verify that access is appropriate and terminated users have been disabled or removed. The ISSO manages IDMS user accounts with administrator privileges including establishing, activating, modifying, reviewing, disabling, and removing user accounts. The ISSO also reviews privileged information system accounts on a monthly basis.

Section B. Logical Access Controls for Privileged Users and Multi-Factor Authentication for Privileged Users

The Act requires the Inspector General to provide a description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.

Agency-wide Logical Access Controls and Multi-Factor Authentication

At BBG, privileged user accounts include Active Directory domain, server, and workstation administrator accounts. A BBG official stated that logical access controls are implemented for privileged user accounts, including having a member of the information security team review privileged user accounts' activities (for example, logs captured at the Active Directory level). In addition, privileged user accounts are reviewed as part of BBG's weekly continuous monitoring meetings. However, BBG officials acknowledged that the agency has not fully implemented

multi-factor authentication to access its PII systems. A list of identified logical access controls that govern privileged user access at both the agency level and system level is contained in Appendix B of this report.

System-level Logical Access Controls and Multi-factor Authentication

BBG does not use PIV multi-authentication to govern privileged user access to PIE. In addition, BBG permits remote access for privileged functions to PIE for compelling operational needs. If the access is from the internet, BBG allows users to access PIE using Remote Desktop Protocol with Entrust (hard token) login. All remote communications with PIE are handled through encrypted tunnels[23] via Transport Layer Security, Secure Shell, and Lightweight Directory Access Protocol.

BBG officials stated that there were no non-privileged user accounts on IDMS. Currently, there are two dedicated workstations that allow privileged access to IDMS. Privileged users are required to have a PIV card and pin, or PIV card and biometrics information, to access IDMS. Remote access is not allowed. Also, IDMS is operated by a third-party vendor as a managed service and is configured with one privileged account that is managed, controlled, and protected by the vendor for system administration and maintenance purposes.

Section C. Reasons for Not Having Minimum Logical Access Controls and Multi-Factor Authentication for Privileged Users

If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, the Act requires the Inspector General to provide a description of the reasons for not using such logical access controls or multi-factor authentication.

BBG officials stated that the multi-factor authentication was not completed due to insufficient funding. Further, the IDMS system was not fully developed to implement physical access controls to BBG facilities and logical access controls to BBG PII systems in accordance with the multi-factor authentication. However, BBG has been invited to participate in the U.S. Department of Homeland Security's Credential Management Tool Procurement, which will supplement BBG's PIV card logical access capabilities.

Section D. Other Information Security Management Practices

The Act requires the Inspector General to provide a description of the following information security management practices used by the covered agency regarding covered systems:

[23] According to NIST SP 800-46, "Guide to Enterprise Telework and Remote Access Security, "tunneling is a high-level remote access architecture that provides a secure tunnel between a telework client device and a tunneling server through which application traffic may pass.

i. The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

ii. What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including –

I. data loss prevention capabilities;

II. forensics and visibility capabilities; or

III. digital rights management capabilities.

iii. A description of how the covered agency is using the capabilities described in clause (ii).

iv. If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.

Software Inventory and Licenses

A BBG official acknowledged that the agency does not have entity-wide or system-level software asset management policies and procedures for either Microsoft or non-Microsoft software products. Software asset licenses are only tracked using separate tools at the system level. For example, Microsoft software products are normally purchased through an enterprise agreement where additional software must be obtained through a one-time purchase agreement. This enterprise agreement allows for software to be downloaded once after the licensing manager validates whether it was paid for. Consequently, BBG is able to determine the number of licenses used via the licensing management server. However, the licensing management server is used specifically for Microsoft products and not for tracking non-Microsoft software licenses. At the system level, the agency uses the Add/Remove program functionality to track installed software for the PIE system. Also, the agency leverages the System Security Plan to track software inventory for the IDMS system. Specifically, a section of the SSP lists software installed on IDMS.

Monitoring and Detection of Data Exfiltration and Other Threats (Data Loss Prevention, Forensics and Visibility, and Digital Rights Management)

BBG officials acknowledged that the agency did not implement data loss prevention or digital rights management solutions at the agency level or for the PII systems reviewed (PIE and IDMS). However according to BBG officials, BBG has established some alternative controls at the entity level including:

- Implementing a policy prohibiting physical documented records containing PII from being sent or removed from BBG's premises. Removal of such documents for work-related reasons, including telework, requires prior approval by an employee's direct supervisor and the ISSO and only the minimum amount of PII that is needed to accomplish work requirements can be removed.
- Implementing a policy preventing removal of portable storage devices that contain PII—considered data at endpoint—from BBG premises. Instead, BBG utilizes secure remote access technologies that allow remote access only via technologies that implement

secure and encrypted communication channels and do not allow local downloading, capture, copying, or printing.
- Automatically logging remote access to BBG's network for accountability. Specific systems containing PII data automatically log remote access as well as maintain an audit trail of the remote user's record access and actions. This audit data is retained for a minimum of 6 months.
- Properly retiring PII to the National Archives and Records Administration or destroying it when documents or devices containing PII are no longer necessary.
- Properly retiring hardware and portable storage media by sanitizing them before disposal by using a wipeout utility or physically destroying them. Hard copies of documents with PII must be shredded or destroyed in another manner.

At the BBG network infrastructure level, BBG officials stated the agency has implemented FireEye (a network monitoring and analysis tool) solution for host-based forensics capabilities. At the system level, BBG officials stated that BBG has deployed a system specific firewall and intrusion detection system for IDMS. Because PIE is hosted on a virtual environment, meaning downloading information is not possible, PIE has built in monitoring controls, which mitigates the risk of not having a separate monitoring tool.

Management's Reasons for Not Fully Implementing Data Exfiltration Controls

BBG officials stated that agency senior management made a risk-based decision not to implement data loss prevention and digital rights management solutions across the agency.

Section E. Entities That Provide Services to the Broadcasting Board of Governors

The Act requires the Inspector General to provide a description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph 4.

Williams Adley found that BBG had not developed information security policies and procedures for managing contracted/hosted information systems that contain BBG PII data. However, in response to a draft of this report, BBG stated that it had developed policies and procedures governing contracted/hosted information systems and provided the policies. Because the information was provided following fieldwork, Williams Adley was not able to thoroughly review and verify the policies provided by BBG was sufficient to secure PII data. In addition, according to BBG officials, all contracted/hosted systems that contain PII are managed or certified by the Department of Defense, OMB, or the Office of Personnel Management. These hosting entities are responsible for implementing the security and privacy controls in accordance with that agency's approved System Security Plan. Furthermore, BBG officials informed Williams Adley that the BBG has been relying on signed Memoranda of Agreement and Interconnection

Security Agreements with contracting/hosting entities to manage the security and privacy controls for the PII systems, whenever applicable.

APPENDIX A: PURPOSE, SCOPE, AND METHODOLOGY

The Consolidated Appropriations Act, 2016,[24] Section 406, Federal Computer Security, requires the Inspector General of each covered agency[25] to submit a report, which shall include information collected from the covered agency regarding computer systems for the following topics:

A. A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.
B. A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.
C. If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.
D. A description of the following information security management practices used by the covered agency regarding covered systems:
    i. The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.
    ii. What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including –
        I. data loss prevention capabilities;
        II. forensics and visibility capabilities; or
        III. digital rights management capabilities.
    iii. A description of how the covered agency is using the capabilities described in clause (ii).
    iv. If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.
E. A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph D above.

To fulfill its responsibilities under the Act, the Office of Inspector General, Office of Audits, contracted with Williams, Adley & Company-DC, LLP (Williams Adley), an independent public accounting firm, to provide a report on the description of the Broadcasting Board of Governors' (BBG) computer security controls for covered systems.

Williams Adley performed the review from April to June 2016. Williams Adley interviewed BBG officials to gain an understanding of BBG's current information security policies and procedures

[24] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2984, Section 406.

[25] According to the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2984, Section 406, Federal Computer Security, the term "covered agency" means an agency that operates a covered system.

relating to BBG's computer security controls for covered systems. According to BBG officials, BBG has three active covered systems containing PII that are owned and maintained by BBG. Williams Adley judgmentally selected two of the three systems—Privacy Information Enclave and Identification Management System—for review. Williams Adley collected and reviewed relevant written documents relating to the two PII systems to provide a description of the relevant controls for the covered systems. According to BBG officials, BBG does not have any National Security Systems.

APPENDIX B: LIST OF ACCESS CONTROLS FOR INFORMATION SYSTEMS WITH PERSONALLY IDENTIFIABLE INFORMATION FOR PRIVILEGED USERS

Williams, Adley & Company-DC, LLP (Williams Adley) reviewed the Broadcasting Board of Governors' (BBG) policies, procedures, and practices for access controls at the agency-wide level and for two specific systems for privileged users of information systems with personally identifiable information—Privacy Information Enclave (PIE) and Identification Management System (IDMS)—and reported its findings in Table B.1.

Table B.1: Comparison of Broadcasting Board of Governors Access Controls Entity-wide and for Four Specific Systems to Access Controls Required by Standards

National Institute of Standards and Technology, Special Publication 800-53, rev. 4, Control	BBG Policies, Procedures, and Practices	
	Agency Level	System Level
PL-4 Rules of Behavior a. Agencies establish, and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage	Present at the system level	IDMS - BBG maintains Rules of Behavior for privileged users. PIE – None
AC-2 Account Management d. Specifies authorized users of the information system, group and role membership, and access authorizations and other attributes for each account j. Reviews accounts for compliance with account management requirements	BBG implemented a manually enforced Organizational Unit Structure and password standards for accounts with elevated privileges	IDMS – The Information System Security Officer must review privileged information system accounts at least monthly. PIE – Enterprise Platforms Division has automated scripts that audit all accounts for compliance with BBG policies weekly.
AC-17 Remote Access a. The organization establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed	Present at the system level	IDMS – Remote access permitting the execution of privileged commands and access to security-relevant information is strictly limited to XTec[a] contractor personnel for maintenance.

National Institute of Standards and Technology, Special Publication 800-53, rev. 4, Control	BBG Policies, Procedures, and Practices	
	Agency Level	System Level
b. The organization authorizes remote access to the information system prior to allowing such connections		PIE – BBG remote access is authorized thru Active Directory and Entrust multi-factor login. If the access is from Internet, VPN/Entrust token is needed.
AC-6 Least Privilege: The organization employs the principle of least privilege, allowing only authorized accesses for users that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Present at the system level	IDMS – IDMS uses a role-based permission system to control which actions a user may perform. PIE – All administrators are given only the privileges necessary to perform their specific tasks. This includes careful management of added privileges authorized only for a limited time.
IA-2 Identification and Authentication (Organizational Users): The information system uniquely identifies and authenticates organizational users.	Present at the system level	IDMS – The XTec ASA 1000[b] appliance includes the ability for IDMS AuthentX[c] users to connect to IDMS AuthentX server and log into the AuthentX application using their personal identity verification card and personal identification number, or personal identity verification card and biometrics. PIE – Entrust two factor is used for privileged accounts on Windows servers console logon.

[a] According to the IDMS System Security Plan Version 2.3, dated April 2015, BBG IDMS is supplied by the Vendor XTec.
[b] According to the IDMS System Security Plan Version 2.3, dated April 2015, the XTec ASA 1000 appliance is a single purpose appliance built on a customized embedded Windows Operating System to capture an individual's biometric data and photograph and in turn send the information to the BBG IDMS server.
[c] According to the IDMS System Security Plan Version 2.3, dated April 2015, AuthenX is a distributed client-server application running across BBG's internal IP network.

Source: Williams Adley prepared based on documentation provided by BBG.

APPENDIX C: COMPARISON OF POLICIES, PROCEDURES, AND PRACTICES AGENCY-WIDE AND FOR TWO SYSTEMS TO FEDERAL PERSONALLY IDENTIFIABLE INFORMATION STANDARDS

Williams, Adley & Company-DC, LLP (Williams Adley) compared Broadcasting Board of Governors (BBG) documented controls agency-wide and for two systems— Privacy Information Enclave (PIE) and Identification Management System (IDMS)—that include personally identifiable information (PII) with Federal requirements for PII outlined in Office of Management and Budget (OMB) Memorandum M-07-16 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev. 4, Appendix J, "Privacy Control Catalog." The results are reflected in Table C.1.

Table C.1: Comparison of Broadcasting Board of Governors Personally Identifiable Information Policies to Federal Requirements

Control	Description	Requirement	Agency Level	IDMS	PIE
1. Review and reduce the volume of PII	Agencies must review current holdings of all PII and reduce to the minimum necessary	OMB M-07-16	Yes	Yes	Yes
2. Reduce the use of Social Security numbers	a. Agencies must review the use of Social Security numbers in agency systems and programs to identify instances in which collection or use of the social security number is superfluous b. Agencies must participate in government-wide efforts to explore alternatives to agency use of Social Security numbers	OMB M-07-16	Yes	Yes	Yes
3. Encryption	Agencies must encrypt using only NIST-certified cryptographic modules for all data on mobile computers/ devices carrying agency data unless the data is determined not to be sensitive in writing by the	OMB M-07-16	Not applicable, as no sensitive data is stored on mobile devices	No	No

Control	Description	Requirement	Agency Level	IDMS	PIE
	Deputy Secretary or a senior-level individual				
4. Control Remote Access	Agencies must allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access	OMB M-07-16	Yes	Yes	Yes
5. Time-Out Function	Agencies must use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity	OMB M-07-16	No	No	No
6. Log and Verify	Agencies must log all computer-readable data extracts from databases holding sensitive information and verify each extract	OMB M-07-16	Yes	No	No
7. Ensure understanding of responsibilities	Agencies must ensure all individuals with authorized access to PII and their supervisors sign at least annually a document clearly describing their responsibilities	OMB M-07-16	No	No	Yes
8. Authority to collect (AP-1)	Agencies must determine and document the legal authority that permits the collection, use, maintenance and sharing of PII, either generally or in support of a specific program or information system need	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes
9. Purpose specification (AP-2)	Agencies must describe the purpose for which PII is collected, used, maintained, and shared in its privacy notices	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes

Control	Description	Requirement	Agency Level	IDMS	PIE
10. Governance and privacy program (AR-1)	a. Agencies must appoint a Senior Agency Official for Privacy/Chief Privacy Officer accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems b. Agencies must monitor Federal privacy laws and policy for changes that affect the privacy program c. Agencies must allocate sufficient resources to implement and operate the organization-wide privacy program d. Agencies must develop a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures e. Agencies must develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes

Control	Description	Requirement	Agency Level	IDMS	PIE
	f. Agencies must update privacy plan, policies, and procedures at least biennially				
11. Privacy Impact and Risk Assessment (AR-2)	a. Agencies must document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII b. Agencies must conduct Privacy Impact Assessments for information systems, programs, or other activities that pose a privacy risk	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes
12. Privacy requirements for contractors and service providers (AR-3)	a. Agencies must establish privacy roles, responsibilities, and access requirements for contractors and service providers b. Agencies must include privacy requirements in contracts and other acquisition-related documents	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes
13. Privacy monitoring (AR-4)	Agencies must monitor and audit privacy controls and internal privacy policy to ensure effective implementation	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes
14. Privacy awareness and training (AR-5)	a. Agencies must develop, implement, and update a comprehensive training and awareness strategy b. Agencies must administer basic privacy training and targeted, role-based privacy training for personnel having responsibility for PII or	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes

Control	Description	Requirement	Agency Level	IDMS	PIE
	activities involving PII at least annually c. Agencies must ensure that personnel certify acceptance of responsibilities for privacy requirements at least annually				
15. Privacy reporting (AR-6)	Agencies must develop, disseminate, and update reports to the Office of Management and Budget, Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates and to senior management	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No
16. Privacy-enhanced system design and development (AR-7)	Agencies must design information systems to support privacy by automating privacy controls	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No
17. Accounting of disclosures (AR-8)	a. Agencies must keep an accurate accounting of disclosures of information held in each system of records under its control b. Agencies must retain the accounting of disclosures for the life of the record or 5 years after the disclosure is made, whichever is longer c. Agencies must make the accounting of disclosures available to the person named in the record upon request	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No
18. Data Quality (DI-1)	a. Agencies must confirm to the greatest extent practicable upon	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No

Control	Description	Requirement	Agency Level	IDMS	PIE
	collection or creation of PII the accuracy, relevance, timeliness, and completeness of that information b. Agencies must collect PII directly from the individual to the greatest extent practicable c. Agencies must check for and correct, as necessary, any inaccurate or outdated PII used by its program or systems d. Agencies must issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information				
19. Data Integrity and Data Integrity Board (DI-2)	a. Agencies must document processes to ensure the integrity of PII through existing security controls	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes
20. Minimization of PII (DM-1)	a. Agencies must identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection b. Agencies must limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent c. Agencies must conduct an initial evaluation of PII holdings and establish and follow a schedule for regularly reviewing those holdings at least annually to ensure that only PII identified in the notice is collected	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No

Control	Description	Requirement	Agency Level	IDMS	PIE
	and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose				
21. Data retention and disposal (DM-2)	a. Agencies retain each collection of PII for an agency-defined time period to fulfill the purpose identified in the notice or as required by law b. Agencies dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with a National Archives and Records Administration - approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access c. Agencies must use agency-defined techniques or methods to ensure secure deletion or destruction of PII	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes
22. Minimization of PII Used in Testing, Training, and Research (DM-3)	a. Agencies must develop policies and procedures that minimize the use of PII for testing, training, and research b. Agencies must implement controls to protect PII used for testing, training, and research	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No
23. Consent (IP-1)	a. Agencies must provide means, where feasible and appropriate, for individuals to authorize the	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No

Control	Description	Requirement	Agency Level	IDMS	PIE
	collection, use, maintenance, and sharing of PII prior to its collection b. Agencies must provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII c. Agencies must obtain consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII d. Agencies must ensure that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII				
24. Individual Access (IP-2)	a. Agencies must provide individuals the ability to have access to their PII maintained in its system(s) of records b. Agencies must publish rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records c. Agencies must publish access procedures in System of Records Notices d. Agencies must adhere to Privacy Act requirements and OMB policies	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No

Control	Description	Requirement	Agency Level	IDMS	PIE
	and guidance for the proper processing of Privacy Act requests				
25. Redress (IP-3)	a. Agencies must provide a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate b. Agencies must establish a process for disseminating corrections or amendments of PII to other authorized users of PII, such as external information-sharing partners and, where feasible and appropriate, notify affected individuals that their information has been corrected or amended	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No
26. Complaint Management (IP-4)	Agencies must implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No
27. Inventory of PII (SE-1)	a. Agencies must establish, maintain, and update an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII b. Agencies must provide each update of the PII inventory to the Chief Information Officer or information security official to support the establishment of information security requirements	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No

Control	Description	Requirement	Agency Level	IDMS	PIE
	for all new or modified information systems containing PII				
28. Privacy Incident Response (SE-2)	a. Agencies must develop and implement a Privacy Incident Response Plan b. Agencies must provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No
29. Privacy Notice (TR-1)	a. Agencies must provide effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII; (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary b. Agencies must describe: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No

Control	Description	Requirement	Agency Level	IDMS	PIE
	individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected c. Agencies must revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change				
30. System of Records Notices and Privacy Act Statements (TR-2)	a. Agencies must publish System of Records Notices in the Federal Register, subject to required oversight processes, for systems containing PII b. Agencies must keep System of Records Notices current c. Agencies must include Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes
31. Dissemination of Privacy Program Information (TR-3)	a. Agencies must ensure that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy/Chief Privacy Officer	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No

Control	Description	Requirement	Agency Level	IDMS	PIE
	b. Agencies must ensure that its privacy practices are publicly available through organizational websites or otherwise				
32. Internal Use (UL-1)	Agencies must use PII internally only for the authorized purpose identified in the Privacy Act and/or in public notices	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No
33. Information Sharing with Third parties (UL-2)	a. Agencies must share PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes b. Agencies must where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used c. Agencies must monitor, audit, and train its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII d. Agencies must valuate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No

Control	Description	Requirement	Agency Level	IDMS	PIE
	and whether additional or new public notice is required				

Source: Williams Adley prepared based on documentation provided by BBG.

APPENDIX D: BROADCASTING BOARD OF GOVERNORS RESPONSE

Broadcasting Board of Governors
United States of America

August 1, 2016

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

Dear Mr. Brown:

Thank you for the opportunity to respond to the draft Information Report: *Description of Policies and Computer Security Controls for Select Broadcasting Board of Governors Covered Systems.*

As we discussed with your staff and contractor during the meeting on July 27, 2016, we believe the draft wording of the report provides sensitive details about the security controls for our Privacy Information Enclave (PIE), and these details should not be released into the public sphere. We would propose the following alternative language, which covers the necessary details but does not risk compromising the security of the system, for the paragraph beginning at the bottom of page 7 of the draft report:

BBG officials stated that BBG isolated the PIE system using a virtual environment and multiple layers of logical access controls. Only a limited number of dedicated workstations are granted privileges to access the PIE system and data. In addition, a server functions as the virtual desktop for users accessing the PIE system, which mitigates the risk of downloading PII data. BBG stated that only a small number of users and IT staff have access to the PIE system. The Enterprise Platforms Division Manager, who ultimately reports to the CIO, is responsible for account management, which includes routinely disabling temporary system accounts and automatically disabling inactive accounts.

In addition, at the above-referenced meeting, IBB staff confirmed that IBB does have policies and procedures that address security and privacy controls for contracted/hosted systems. With respect to Section E of the report, the Agency has implemented policies and procedures to ensure that contractors are implementing security and privacy controls for information systems the Agency procures. The Agency's policy on granting authority to operate information systems (11 BAM 100) establishes procedures for ensuring contractors implement adequate security controls identified in NIST guidance. Also, the Agency's policy on safeguarding Personally Identifiable Information (PII) (11 BAM 200) requires the Agency's contracting officers to incorporate the Agency's PII policy into contracts as necessary and to monitor and enforce contractor compliance. Because the Agency's systems that contain PII are managed by other Federal agencies, 11 BAM 200 is currently applicable to service contractors whose work requires access to systems containing PII and would also be applicable to a contracted/hosted information system that contained PII if the Agency later procured one. We have attached these policies for your information and consideration.

Thank you again for the opportunity to respond and please do not hesitate to contact us should you have questions.

Sincerely,

John F. Lansing
Chief Executive Officer and Director

330 Independence Avenue, SW | Room 3300 | Cohen Building | Washington, DC 20237 | (202) 203-4545 | Fax (202) 203-4568

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