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

AUD-IT-16-45 | Office of Audits | August 2016

Information Report: Description of Policies and Computer Security Controls for Select Department of State Covered Systems

INFORMATION REPORT

Summary of Project

The Consolidated Appropriations Act, 2016,[1] 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.[3] Specifically, the Consolidated Appropriations 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. Information related to national security data is covered in a classified annex to this information report.

Acting on the Office of Inspector General's behalf, Williams, Adley & Company-DC, LLP (Williams Adley), an independent public accounting firm, collected information about Department of State (Department) computer systems and reviewed security controls for six covered systems. Specifically, Williams Adley selected and reviewed 4 systems from a Department-provided listing of 216 systems (Electronic Medical Records System (eMED), Integrated Personnel Management System (IPMS), Consular Consolidated Database (CCD), and Consular Lookout and Support System (CLASS)) that provide access to PII. In addition, Williams Adley reviewed 2 National Security Systems (NSS) from a Department-provided listing of 60 systems (Chief of Mission and Special Embassy Programs Database (NSDD 38), and Principal Officers Executive Management System (POEMS)).

This report describes the policies and controls used by the Department for 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 only two of the six systems reviewed (eMED and IPMS) had system-specific logical access control policies.

---

[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 the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2984, Section 406, the term "covered system" means 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.

[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.

However, all six systems reviewed had System Security Plans (SSP), which documented the security controls at the system level as required.

With respect to access and multi-factor authentication, Williams Adley found the Department has not fully implemented multi-factor authentication at the entity level; however, it had implemented other logical access compensating controls to govern privileged user access. Four of the six systems reviewed (eMED, CCD, CLASS, and one NSS) had either fully or partially implemented multi-factor authentication to government system-level privileged user logical access. The two systems that did not utilize multi-factor authentication to govern logical access of privileged users (IPMS and one NSS) relied on username and password combinations. Nevertheless, all six systems had some type of logical access controls in place.

With respect to why logical access controls or multi-factor authentication are not being used, according to Department officials, two of the six systems (IPMS and one NSS) did not implement multi-factor authentication to govern system-level privileged user access because functional capabilities are not available. According to Department officials, IPMS is currently planning multi-factor implementation, while the one NSS is waiting for the Department to provide the functional capabilities necessary to implement multi-factor authentication to govern privileged user logical access.

With respect to information security management practices used for covered systems, Williams Adley found the Department uses a federated model to manage software inventory. In addition, the Department has implemented a defense-in-depth information system program. Further, the Department monitors network traffic, detects and responds to incidents, and scans for security compliance and vulnerabilities. However, the Department has only partially implemented a data loss prevention system and has not implemented digital rights management technology.

With respect to policies and procedures that ensure information security management practices are effectively implemented by other entities such as contractors, Williams Adley found the Department has a number of policies related to this topic. The relevant Department policies and procedures are established within the Department's Foreign Affairs Manual (FAM).

The Bureau of Information Resource Management, the Executive Secretariat's Office of Information Resource Management, and the Bureau of Diplomatic Security, provided comments to a draft of this report. Because the comments were marked sensitive, the comments have been reprinted, in their entirety, in the classified annex of this report (AUD-IT-16-45A).

OBJECTIVE

The Consolidated Appropriations Act, 2016,[6] 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).

BACKGROUND

The Department is the U.S. Government's principal agency for helping to build and sustain a more democratic, secure, and prosperous world composed of well-governed states. The Department's mission is carried out by geographic and functional bureaus that provide policy guidance, program management, administrative support, and in-depth expertise. The Department has an extensive overseas presence, with 275 posts worldwide. The Department, as

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

well as its contractors, depends on IT systems and electronic data to carry out essential mission-related functions. The security of these systems and networks is vital to the Department's mission. 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.

The Department has implemented a federated organizational structure[7] defined by functional bureaus and relevant Department personnel to govern and implement information security. The Department stakeholders involved in the information security program include:

- the Bureau of Information Resource Management (IRM);
- the Bureau of Diplomatic Security (DS), Security Infrastructure Directorate (SI);
- the Bureau of Administration, Global Information Services, Office of Information Programs and Services, Privacy Division; and
- Information system managers and owners (from various bureaus and offices).

IRM, directed by the Chief Information Officer, is responsible for developing and disseminating information security policies in accordance with applicable Federal standards and the administration of the Department's network infrastructure. In addition, IRM is responsible for ensuring the accreditation, authorization, and availability of Department IT systems and operations.[8] IRM significantly relies on information system owners to identify and implement the necessary and required information security controls to protect the information systems.

DS has statutory authority to develop and disseminate information security policies at the Department level.[9] Furthermore, DS/SI supports the current and emerging needs of the Department by ensuring the security of the Department's global information and information systems.[10] DS/SI consists of the Office of Cybersecurity (DS/SI/CS), the Office of Information Security, the Office of Personnel Security and Suitability, and the Insider Threat Program. According to Department officials, DS/SI manages the handling of sensitive information, administers the Department's cybersecurity program, and protects Department information systems via a defense-in-depth program.[11]

The Bureau of Administration, Global Information Services, Office of Information Programs and Services, Privacy Division is responsible for ensuring compliance with Federal privacy mandates, promoting privacy protection awareness, and building public trust by implementing best

[7] A federated organizational structure is an approach that emphasizes a controlled sharing of responsibilities and exchange of information between semi-autonomous, decentralized organizations.

[8] 1 FAM 272, "Office of Information Assurance/Chief Information Security Officer," May 2011.

[9] 22 U.S. Code § 4802 - Responsibility of Secretary of State, (a) Security functions.

[10] 1 FAM 262.7-1, "Office of Information Security", June 2015.

[11] A defense-in-depth concept is when multiple layers of security controls are placed throughout an IT system.

practices.[12] The Privacy Division has the responsibility to ensure privacy protection while still promoting the consistent implementation of Department-wide Federal privacy policies and statutory requirements.[13] The Privacy Division is responsible for working with relevant information system owners to protect PII data collected by Department information systems by assisting in the completion of Privacy Impact Assessments and the remediation of PII loss. Furthermore, the Privacy Division is responsible for governing the Department's compliance with the federally-mandated System of Record Notices[14] requirement.

Information system owners are critical to the operation of the Department's information security program. All information system owners are required to identify and implement comprehensive information security controls to protect the Department's information systems. The Department has adapted a federated model for information security because of the differences in hardware and software capabilities of and between different information systems.[15] For example, according to a Department official, information system owners are responsible for identifying PII prior to implementing their information system.

Cyber Security Trends

According to a Government Accountability Office (GAO) report,[16] 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,[17] 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 Director of the U.S. Office of Personnel Management acknowledged[18] that the number of individuals with data compromised from the personnel records incident in

[12] According to the Department of State Privacy Division website, <http://www.state.gov/m/a/privacy/index.htm.>; see also 5 FAM 460, The Privacy Act and Personally Identifiable Information, March 2016.
[13] Ibid.
[14] 1 FAM 214.2-9, Privacy Division, May 2009; Privacy Act of 1974, 5 U.S.C. § 552a. According to the Bureau of Administration's Global Information Services Office of Information Programs and Services Privacy Division intranet site, "the Privacy Act of 1974 establishes safeguards for the protection of certain records, which the Federal government collects and maintains on United States citizens and aliens lawfully admitted for permanent residence. The Privacy Act only pertains to information that is maintained in a system of records (herein after called 'system'), while a 'record' is defined as an item of information about an individual, including his or her name or some other identifier. A 'system of records' is distinguished from other kinds of personal records in that a record in the system is retrieved by an individual's name or other personal identifier," <http://a.m.state.sbu/sites/gis/ips/prv/SitePages/System%20of%20Records%20Notices.aspx>, accessed on June 10, 2016.
[15] 12 FAM 641, "General," April 1996.
[16] GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices* (GAO-14-354, April 2014).
[17] GAO, *Information Security: Federal Agencies Need to Better Protect Sensitive Data* (GAO-16-194T, November 2015).
[18] According to "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.

2015 was approximately 4.2 million. Two separate incidents involved the exfiltration of personnel records and background investigation data in two different information systems.

- In FY 2014, the Department reported multiple network intrusions that caused unscheduled downtimes; loss of productivity; and, in some cases, loss of data.[19]

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 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. 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[20] and the Health Insurance Portability and Accountability Act of 1996.[21] 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.[22]

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.[23]

For information systems that process, transmit, or contain PII, the National Institute of Standards and Technology (NIST) published NIST Special Publication (SP) 800-53 which provides a catalog of security and privacy controls for Federal information systems and organizations. [24] For example, NIST SP 800-53 provides a process for selecting information security controls to protect organizational operations (including mission, functions, image, and reputation),

[19] Department of State, Cybersecurity Strategy, August 2015.
[20] Privacy Act of 1974, 5 U.S.C. § 552a (December 1974).
[21] Health Insurance Portability and Accountability Act of 1996, Pub. Law No. 104-191, (August 1996).
[22] According to the U.S. Department of Health and Human Services, <http://www.hhs.gov/hipaa/for-professionals/privacy/>, accessed on June 10, 2016.
[23] OMB, Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (May 2007).
[24] NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," "AT-4 Security Training Records," January 2014.

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.

National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," outlines the roles and responsibilities for securing NSS, consistent with applicable law, Executive Order 12333,[25] as amended, and other Presidential directives.

For NSS, the Committee on National Security Systems' Instruction No. 1253[26] provides the Federal government with guidance on the first two steps of the Risk Management Framework. This instruction builds on and is a companion document to NIST SP 800-53.

Department Personally Identifiable Information and National Security Systems

According to Department officials, the Department has 276 covered systems that include 216 systems that process, store, or transmit PII and 60 NSS. Williams Adley judgmentally selected for review 6 (4 PII systems and 2 NSS) of 276 covered systems identified by Department officials.[27] Specifically, Williams Adley reviewed the following systems:

- Electronic Medical Records System (eMED),
- Integrated Personnel Management System (IPMS),
- Consular Consolidated Database (CCD),
- Consular Lookout and Support System (CLASS),
- Chief of Mission and Special Embassy Programs Database (NSDD 38), and
- Principal Officers Executive Management System (POEMS)[28]

Electronic Medical Records System

According to Department documentation, eMED enables the Office of Medical Services to provide a single authoritative source of information to manage employees' electronic medical information. This system consists of a primary application and seven subordinate components:

- Laserfiche,
- MED Customer Dashboard,
- History and Physical Lookup,
- Clearance Lookup,

[25]United States Intelligence Activities, December 4, 1981.

[26] Committee on National Security Systems Instruction No. 1253, "Security Categorization and Control Selection for National Security Systems," March 2014.

[27]Refer to Appendix A: Purpose, Scope, and Methodology.

[28] All discussion about NSS is in the classified annex to this information report.

- Subjective Objective Assessment and Plan of Care,
- Claims, and
- MED Fax Services.

The Department explained that eMED provides a secure and standardized infrastructure to track, maintain, and protect Department employees' and dependents of employees' medical information (for example, medical clearance decisions and medical records). All medical information is stored on a secure Oracle database and is accessible to eMED users via a client application. This client application provides patient information to authorized users within the Office of Medical Services in the Washington, D.C., metropolitan area and at Department posts worldwide.[29]

Integrated Personnel Management System

According to Department documentation, IPMS is the underlying technical architecture for a group of 70 applications owned and operated by the Bureau of Human Resources. IPMS is a program initiative with a mission to modernize the bureau's IT infrastructure in order to streamline business processes, maintain accurate data, and ensure compliance with amended legislations and regulations. This system consists of five core components:

- the Global Employee Management System,
- Human Resources Online,
- the Post Personnel System,
- Executive Agency Personnel Support, and
- the HR Knowledge Center.

IPMS maintains, processes, and stores PII for Civil Service and Foreign Service employees, locally employed staff, contractor employees, dependents, Foreign Service consular agents, applicants for Civil Service and Foreign Service employment, other U.S. Government agency employees under Chief of Mission authority, and resident U.S. citizens employed by missions abroad. According to the Department, IPMS system components, in aggregate, create a consistent workflow process to allow the Bureau of Human Resources to reduce transaction processing, enhance Department-wide data sharing capabilities, and improve data integrity and quality.[30]

Consular Consolidated Database

According to Department documentation, CCD is a data warehouse based on commercially procured software that contains current and archived data from all of the Bureau of Consular Affairs' post databases. The collected PII is used for visa and American citizen services work. This system provides a near real-time aggregate of all Bureau of Consular Affairs transaction activity collected domestically and at the Department's 275 posts worldwide. CCD serves as a gateway

[29] According to the System Security Plan (SSP) revision 7.10 for eMED v02.02.01, dated August 2014.
[30] According to the SSP v4.1 for IPMS v2.02.00, dated February 2016.

to the Automated Biometric Identification System,[31] as well as the Department's Facial Recognition system. Specifically, CCD delivers three primary functions:

- Allows for the ability to generate reports to authorized CCD users.
- Provides authorized users with data entry interfaces to CCD.
- Delivers emergency recovery and restoration data of Department post databases.[32]

Consular Affairs Lookout and Support System

According to Department documentation, CLASS supports the mission of the Bureau of Consular Affairs to facilitate travel by issuing travel documents to U.S. and foreign citizens. Specifically, this system provides the Department's passport agencies, posts, and border inspection agencies the ability to collect and look up needed information to perform name checks related to visa and passport applicants. The system consists of two parallel but separate databases housing visa and passport information. The Bureau of Consular Affairs collects necessary PII from applicants and uses CLASS to enable Department personnel to determine whether a particular applicant is eligible or ineligible to receive a visa or passport. CLASS also contains records provided by other Federal organizations such as U.S. Immigration and Customs Enforcement and the Department of Health and Human Services.[33]

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.

Department-wide Logical Access Control Policies

The Department's official policies and procedures (collectively known as directives) are maintained in the Foreign Affairs Manual (FAM) and associated Foreign Affairs Handbooks (FAH). The FAM and FAH are divided into volumes, and each volume has a specific theme. FAM and FAH volumes with relevant IT security information include 5 FAM, "Information Management," and 12 FAM, "Diplomatic Security," which includes chapters 500, "Information Security" and 600, "Information Security Technology." IRM and DS utilize the relevant Federal standards to build the information security policy governing logical access to Department covered systems.

[31] According to the CCD Privacy Impact Assessment, dated July 2015, the Automated Biometric Identification System is the Department of Homeland Security's commercial off-the-shelf technology providing automated fingerprint checking in addition to integration with other Federal biometric systems.
[32] According to the SSP rev. 4 for CCD v04.00.00, dated June 2015.
[33] According to the SSP rev. 4 for CLASS v03.00.00, dated September 2014.

Williams Adley obtained relevant Department policies associated with governing logical access to Department covered systems:

- 12 FAM 640, "Domestic and Overseas Automated Information System Connectivity" – This policy provides general Department network security requirements, including the Department's policy for controlling logical access to the Department's network.[34] Also, it is the responsibility of individual system managers to implement the required policies and controls identified in 12 FAM 640.[35] System managers must restrict network logical access to only those users who have a demonstrated need for such access, and who have been authorized in writing by their supervisors for specific access rights. Examples of logical access control policies identified in 12 FAM 640 include:

  - Unique user logon identification and passwords are utilized,
  - Default user identifications must be removed,
  - System access must be based on the principle of least privilege[36] and must be reviewed annually to be still required,
  - System access utilizing smartcard technology must be compliant with applicable NIST Standards,[37] and
  - Mandatory access control policies for multi-level automated information systems joined in a network have been implemented.[38]

- 12 FAM 620, "Unclassified Information System Security Policies" – This policy establishes the minimum Department mandatory security controls, including logical access controls, required to be implemented for Department unclassified and non-sensitive unclassified information and application systems (for example, PII systems).[39] The policy states that minimally required security controls are determined based on the information system's category level (low, moderate, or high impact) using NIST Federal Information Processing Standards publication 199, "Standards for Security Categorization of Federal Information and Information Systems." The 12 FAM 620 is also designed to align with NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations."[40] The Department requires the NIST SP 800-53, rev. 4, mandatory access controls and identification and authentication controls to be implemented on Department information systems (including covered systems). Specifically, system managers are required to implement the required logical access controls as established

[34] 12 FAM 641 a, "General," April 1996.
[35] 12 FAM 641 b.
[36] According to NIST SP 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems, "least privilege refers to the security objective of granting users only those accesses they need to perform their official duties. Data entry clerks, for example, may not have any need to run analysis reports of their database.
[37] 12 FAM 642.4-2, "Controlling Access to the Network," June 2008.
[38] 12 FAM 643.2-1, "Access Controls," June 2008.
[39] 12 FAM 621, "Purpose," December 2015.
[40] 12 FAM 621 c.

by 12 FAH-10 H-100, "Unclassified/SBU Information Security Controls I,"[41] and 12 FAH-10 H-130 "Identification and Authentication."[42] See Appendix B for a list of access controls for information systems with PII for privileged users.

Williams Adley obtained the following standards that address safeguarding access to PII data and sensitive information:

- 5 FAM 460, "The Privacy Act and Personally Identifiable Information" – This policy establishes the Department's entity-wide policy to comply with Privacy Act of 1974 requirements, as amended.[43] The Department requires that PII be appropriately safeguarded in accordance with Federal standards.[44] According to Department officials, it is the responsibility of each Department information system owner to identify and protect any PII collected, used, maintained, or disseminated by a Department-owned and -operated information system.

- 12 FAM 510, "Safeguarding National Security and Other Sensitive Information" – This policy establishes the scope, responsibilities, and necessary programs required to sufficiently safeguard Department-owned and -maintained national security and other sensitive information, including information maintained within Department NSS.[45] The Department has established an insider threat program to guard and control access to Department national security and other sensitive information. However, according to Department officials, it is the responsibility of individual system owners to identify and protect national security information maintained within Department NSS via implementation of system-level access controls and policies.

Within the FAM and FAH, IRM and DS list the relevant Federal standards, or authorities, that govern the specific Department policy. Refer to Appendix C for a comparison of the Department's logical access policies to relevant Federal standards.

System-Level Logical Access Control Policies

For the Department to address logical access controls at the system level, the applicable Department bureau, office, or system owner documents internal system-level access controls policies as necessary. For the six systems Williams Adley included in the review, two PII systems (eMED and IPMS) have documented logical access control policies, which are maintained at the bureau level. Specifically, the Office of Medical Services has developed and maintained a logical access control policy to govern logical access controls for the eMED system. The Bureau of Human Resources has developed and maintained a logical access control policy to govern

[41] 12 FAH-10 H-111, "Purpose," September 2014.
[42] 12 FAH-10 H-131, "Purpose," February 2016.
[43] According to 5 FAM 460, identified amendments include the E-Government Act of 2002 and OMB directives and guidance governing privacy.
[44] 5 FAM 461, "Scope," March 2016.
[45] 12 FAM 511.1, "Applicability," June 2011.

logical access controls for the IPMS system. Both system-level logical access control policies were developed in order to comply with Department FAM and FAH standards. The other four systems (CCD, CLASS, NSDD 38, and POEMS) did not have documented logical access controls policies.

In addition, the applicable bureau, office, or system owner documents established logical access controls within the System Security Plan (SSP).[46] Williams Adley found that the Department had documented and maintained SSPs for all six systems reviewed. Each SSP included the relevant security controls at the system level in accordance with NIST SP 800-53 minimum security control requirements. However, Williams Adley's review of the SSPs demonstrated that the logical access controls were not consistently updated to reflect and align with the most current logical access control policies developed at the system level (for example, personal identity verification policy).

Logical Access Control Practices

According to Department officials, the Department relies on Microsoft Active Directory to govern logical access to the Department's sensitive but unclassified (SBU)[47] and classified[48] networks. Active Directory is a directory service created by Microsoft for Windows domain networks. It provides a capability for the Department 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. Network users are identified and authenticated via the Department's personal identity verification cards to access the Department SBU network in accordance with Federal standards.[49] Network users are identified and authenticated via the Department's Classified-Public Key Infrastructure smart cards to access the Department's classified network in accordance with Federal standards.[50]

Furthermore, according to Department officials, the Department completed full personal identity verification and Classified-Public Key Infrastructure card implementation for regular (non-privileged) Department users at the end of 2015 to achieve compliance with Federal multi-factor authentication access standards. In addition, according to information provided by Department officials, the majority of Department applications (including PII and NSS systems) housed on the

[46] According to NIST SP 800-18, rev. 1, "Guide for Developing Security Plans for Federal Information Systems," the purpose of an SSP is to provide an overview of the security requirements of a system and describe controls in place or planned for meeting those requirements.

[47] According to 5 FAM 870, "Networks," November 2015, OpenNet is the SBU network in the Department that provides access to standard desktop applications such as word processing and email.

[48] Per 5 FAM 870, ClassNet is one of two Department enterprise networks (OpenNet is the second). ClassNet provides an internal network for email and other processing of information up to the Secret level.

[49] Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004, requires mandatory, Government-wide standards for secure and reliable forms of identification issued by the Federal Government to its employees and Federal contractors.

[50] Exec. Order No. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011.

Department's SBU and classified networks can be accessed via single session sign-on based on the user's personal identity verification or Classified-Public Key Infrastructure credentials and provisioned role-based access controls as authenticated via Active Directory.

Williams Adley conducted interviews with key personnel representing the six systems selected and reviewed standard operating procedures (SOPs) documents that outline logical access practices (for example, how logical access is provided to system users). Williams Adley determined that the SOPs were developed to adhere to established logical access control policies as required by the Department FAM or FAH as well as applicable SSPs. Each SOP detailed that logical access control to each information system was based on the fundamental principle of least privilege and "need to know." Specifically, users' logical access to information and thus information systems is provisioned and restricted based on access control lists that permit access to only the information required for a user to complete job duties. Logical access to the Department networks and six covered systems requires management level approval prior to access being granted. In addition, mandatory annual security awareness and privacy training are required for all authorized Department users.

Section B. Logical Access Controls 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.

Department-wide Logical Access Controls and Multi-Factor Authentication

According to Department officials, the Department privileged user universe consists of four different levels of privileged user access, which is administered on a tiered basis as follows:

- Tier One: Enterprise Administrators
- Tier Two: Domain Administrators
- Tier Three: Organizational Unit Administrators
- Tier Four: Platform/System-level Administrators

Department officials stated that Tier One administrators have the greatest level of logical access privilege within the Department, while Tier Two and Tier Three administrators have the next highest level of logical access privilege required to conduct job responsibilities. Tier Four administrators are provisioned and granted access based on the requirements established by individual information system needs. According to Department officials, all Department privileged users have regular user accounts that are needed to access the Department's SBU and classified networks, and a separate administrative account needed to conduct administrative duties. Department officials also stated that privileged users for the first two tiers are administered and governed at the Department level by IRM. According to information provided by IRM in response to a draft of this report, tier three administrators are not controlled by IRM.

Specific system owners are responsible for governing the logical access of the Tier Four privileged users (for example, system administrators, application administrators, and database administrators).

According to Department officials, Tier One, Tier Two, and Tier Three privileged users are required to use multi-factor authentication, via Department issued smart cards, to logically access the Department's PII systems. However, Williams Adley confirmed with Department officials that multi-factor authentication has not been consistently implemented to access the Department's SBU network (which hosts Department PII systems). Further, multi-factor authentication is not fully implemented to govern privileged user logical access to the Department's classified network (which hosts NSS systems) at any privileged user level.

Although multi-factor authentication is not fully implemented, according to Department officials the Department has implemented a number of logical access compensating controls to govern privileged user access to Department covered systems. For example, the Department has implemented logging and monitoring capabilities to govern privileged user logical access. Specifically, Department officials stated that the Department implemented logging and monitoring capabilities via the use of two separate tools known as the Managed Access Request System (MARS) and Quest® ChangeAuditor® (ChangeAuditor) at the Department level. According to Department officials, MARS provides the capability to have an automated, auditable, and on-demand process to govern critical privileged user access.[51] However, Department officials also acknowledged that the MARS system is currently in pilot mode and can monitor only about half of the Department's privileged users at the Tier One, Tier Two, and Tier Three levels. To govern logical access of the remaining Department-level privileged users, the Department relies on the audit and monitoring tool ChangeAuditor. According to Department officials, ChangeAuditor provides the Department the capability to monitor privileged user access and is configured to alert IRM personnel via email if the system identifies abnormal account activity (for example, failed log-on attempts). In summary, mitigating logical access controls implemented to govern privileged user logical access include the logging and monitoring of privileged accounts (MARS) and the triggering of the alert system when abnormal or questionable activities are observed by the ChangeAuditor tool.

A list of identified logical access controls that govern privileged user access at both the Department-level and system-level is presented in Appendix B of this report.

System-level Logical Access Controls and Multi-factor Authentication

According to Department officials representing the six systems reviewed, additional logical access controls have been implemented to govern privileged user access to each system. Specifically, for the six systems, privileged user logging and monitoring capabilities are conducted utilizing some type of monitoring tool (for example, ChangeAuditor). The monitoring tools utilized to govern logical access of system-level privileged users were chosen by the

[51] IRM, "Active Directory Restructure Program Overview," March 24, 2016.

information system owners. According to Department officials representing the six systems, access to each of the selected systems is fully logged and reviewed by responsible system-level information security personnel (for example, Information System Security Officers) regularly. Furthermore, in order to ensure privileged user logical access is still required, information security personnel perform a review of each privileged user on their respective information system at least annually, for all systems reviewed. Williams Adley listed all documented logical access controls governing privileged user access implemented at the system level for the systems reviewed in Appendix B of this report.

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.

Department-level Description of the Reason for Not Using Multi-factor Authentication

At the Department and system levels, multi-factor authentication via smart card on the Department's SBU network has not been fully implemented throughout the Department for the privileged users. According to Department officials, the Department did not fully implement multi-factor authentication at all four tiers of Department privileged user access because the Department first focused on ensuring the highest-value privileged users accounts were governed by multi-factor authentication. Specifically, the Department utilized resources to protect the privileged users deemed by Department officials to have the highest level of privileged rights within the Department. The Department first focused on securing these privileged accounts with multi-factor authentication because these accounts are most targeted by cyber attackers, and thus if compromised, pose the greatest risk to the Department.

Department officials stated that the Department developed a Privileged User Improvement Program in March 2016. Specifically, for privileged users, Department officials stated that they are in the process of implementing the following initiatives:

- reduce and secure the number of the Organizational Unit administrators (as of January 2015, there were approximately 13,000 Organizational Unit admins globally);[52] this is planned to be completed by the end of December 2016;
- fully automate the privileged user provisioning process using MARS; this is planned to be completed by July 2016; and
- reduce and secure the number of privileged user and service accounts at the system level (as of January 2015, there were approximately 4,400 service accounts globally);[53] this is planned to be completed by December 2016.

[52] IRM, "Active Directory Restructure Program Overview," March 24, 2016.
[53] Ibid.

System-level Description of the Reason for Not Using Multi-factor Authentication

As stated earlier, four of the six systems reviewed used multi-factor authentications. According to Department officials, two of the six systems (IPMS and one NSS) selected did not implement multi-factor authentication to govern system-level privileged user access because functional capabilities are not available. According to Department officials, IPMS is currently planning multi-factor implementation, while the one NSS is waiting for the Department to provide the functional capabilities necessary to implement multi-factor authentication to govern privileged user logical access.

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:

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

The Department uses a federated model to manage software inventory for covered systems. The Department has policies for software inventory, including 5 FAM 865, "Copyrighted Software"[54] and 5 FAM 915.11, "Software."[55] According to the FAM, the Sourcing Management Division, an office within IRM, manages the enterprise software licensing agreements for the Department. The FAM states that all Department employees and contractors must ensure that Government-acquired commercial software is safeguarded against licensing violations and copyright infringements. Department offices are encouraged to obtain multiple-user or site licenses when procuring software for a large number of users. The Department-wide Information Technology Change Control Board (IT CCB) manages changes to the Department's global IT environment and must approve any software installed on SBU and classified infrastructures up to the Secret level.

[54] 5 FAM 865, "Copyrighted Software," October 2012.
[55] 5 FAM 915.11, "Software," June 2005.

According to Department officials, IRM manages and tracks software inventory (for enterprise use) and makes data calls to the program offices to reconcile the authorized licenses. This is accomplished manually. Generally, the program offices are using the Department's enterprise software license agreements (for example, Microsoft Windows, Adobe Acrobat, and Citrix) and purchasing separate software licenses for their programs. Per 5 FAM 915.11-1, "Software Licensing,"[56] IRM's Asset Management Branch manages and tracks the enterprise agreements.

For all six systems reviewed, the Department consistently followed the documented software inventory and licensing process. System owners install software approved by the Department-wide IT CCB[57] or local change control board prior to the installation.[58] The system owners maintain the software inventory and licensing requirements. The system owners also update the SSPs to include the software inventory for each system.

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

According to Department officials, the Office of Information Assurance within IRM oversees the Department's information security program by coordinating and monitoring information security activities domestically and overseas.

Department officials also stated that the Department has implemented a defense-in-depth information security program. DS/SI/CS is responsible for implementing programs including policy and standards, cyber threat analysis, cyber incident response, global vulnerability scanning, and security auditing. Through various programs, DS/SI/CS monitors network traffic, detects and responds to incidents, and scans for security compliance and vulnerabilities. This office is responsible for assessing cybersecurity threats and emerging security technologies to ensure the protection of the Department's technology assets. In addition, it is responsible for recommending, developing, and coordinating clearance of computer, communications, and network security policies, standards, and guidelines.

---

[56] 5 FAM 915.11-1," Software Licensing," December 2008.

[57] According to the Bureau of Administration website, "the scope of the IT CCB encompasses changes that potentially impact the DoS IT environment. The scope includes unclassified infrastructures (OpenNet) and classified infrastructures (standalone or networked) through the Secret high level, and other environments as appropriate," <http://askadmin.a.state.gov/display/2/index.aspx?c=12&cpc=ULxOCA443pKs512Q14X530vupP4TwfI6dt2WJi7&cid=2&cat=&catURL=&r=0.339421272277832>, accessed on June 16, 2016.

[58] According to the Bureau of Administration website, "most changes are handled by local change control entities, such as bureau-level, post-level (alternatively, Information Management Officer [IMO]), and application-level change control. Those changes are required to be reported to their IT CCB Voting Representative and the IT CCB Change Manager. Changes not reported to the IT CCB are not considered to be valid. Where a local change control entity reports a change that impacts the DoS global IT Enterprise in a capacity greater than that for which the Local CCB can accept responsibility, the IT CCB will usurp review of that change request," <http://askadmin.a.state.gov/display/2/index.aspx?c=12&cpc=ULxOCA443pKs512Q14X530vupP4TwfI6dt2WJi7&cid=2&cat=&catURL=&r=0.339421272277832>, accessed on June 16, 2016.

According to Department officials, the cybersecurity programs are designed to provide senior Department officials with the information (for example, cyber threat reports, vulnerability analysis, and technical security evaluations) necessary to make risk-management decisions to properly protect the Department's sensitive information and global IT infrastructure.

Data Loss Prevention

According to Department officials, the Department has partially implemented on a limited basis (on the SBU network only), a data loss prevention system (DLP) to monitor and detect certain PII data (for example, Social Security numbers and credit card numbers) in emails sent from the SBU general support system to non-government and non-military email addresses. The DLP system is a commercial off-the-shelf network monitoring tool and is configured to monitor and detect a limited set of business rules on the enterprise email system. For example, an email is flagged for review by a Privacy Division analyst if it contains more than five identified instances of Social Security numbers (that is, five instances of nine-digit numbers). However, the DLP system does not prevent or block the Department from sending PII data through emails.

Forensics and Visibility

According to 1 FAM 262.4-1 (E),[59] DS's Office of Investigations and Counterintelligence, Computer Investigations and Forensics Division (DS/ICI/CIF) provides technical investigative support to the Department, including capabilities such as cyber investigations, digital forensic analysis, technical surveillance equipment, and operational support. The division investigates cybercrimes that target the Department; carries out related law enforcement and other security functions for the Department; and provides investigative support to all elements of the Department in the seizure or collection of digital, electronic, or computer-related evidence such as computers, camera systems, cell phones, and mobile devices. The division also provides forensic laboratory support (that is, collection, preservation, analysis, explanation, presentation, and litigation support) as it relates to digital, electronic, cellular, audio, or video evidence.

According to Department officials, DS/ICI/CIF focuses on performing cyber investigations for prosecution of potential criminals. The DS/ICI/CIF forensics process adheres to NIST guidance when performing forensic procedures.[60] Specifically, according to Department officials, DS/ICI/CIF agents and analysts adhere strictly to the "chain-of-custody" requirements throughout the performance of forensics procedures. The DS/ICI/CIF forensic framework includes collection of evidence (for example, affected hardware), examination of evidence (including forensic imaging), analysis of data using legally justifiable methods and established forensic techniques, and reporting analysis via documented results, to include actions taken and tools used, that would enable DS/ICI/CIF, if necessary, to present a case supported by admissible evidence in a court of law.

[59] 1 FAM 262.4-1(E),"Computer Investigations and Forensics Division (DS/ICI/CIF)," June 2015.
[60] NIST SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response," August 2006.

Based upon review of the Department's documentation and inquiries with Department officials, the Department uses automated tools (for example, intrusion detection systems and intrusion prevention systems) and vulnerability scanning to gain visibility into the Department's network. As discussed above, the Computer Incident Response Team operations provide near-real-time detection, collection, analysis, correlation, and reporting of cyber security events that pose a threat to the Department's networks. The intrusion detection systems sensors are placed throughout both the Department's SBU (OpenNet) and classified (ClassNet) networks. The ClassNet servers have host-based intrusion detection agents installed, which can monitor accesses and changes to critical system files and changes in user privileges. The OpenNet servers have network-based intrusion detection agents installed, which allow the monitoring of traffic on the network segment to detect attacks. A majority of host-based sensors are deployed on ClassNet, while network sensors are attached to servers inside and outside the Department's firewall, which connects with entities external to the Department through the internet.

DS/SI/CS (specifically the Evaluation and Verification Scanning branch) also performs scans to identify vulnerabilities on the Department's networks to assess the Department's security posture and the degree of compliance with the Department's security configuration standards.[61] The Department uses a commercially procured software for vulnerability scanning and security compliance testing. Vulnerability and compliance scans are run approximately every 7 days per system. The scan results are then moved into iPost. According to Department officials, iPost is a tool from the IRM's Enterprise Network Management that allows authorized users to access enterprise network and system monitoring data and also assess the risk scoring for the system. The Department uses iPost to monitor the security posture aspects of the IT infrastructure. Examples of the types of data in the iPost are server and workstation hardware and software inventory, patch status, security configuration compliance status, vulnerability testing results, user account compliance status, and network device information.[62]

In addition, Department officials stated that the Department does not have the full visibility capability to tell what systems are on the enterprise network (SBU general support system) as the enterprise network is segmented. According to Department officials, the Department uses Trusted Internet Connections,[63] which allow the Department to monitor about 70 percent of its network traffic. The remaining 30 percent of network traffic does not use Trusted Internet Connections and thus is not fully monitored. According to Department officials, the Department

[61] According to the DS intranet site, <https://intranet.ds.state.sbu/DS/SI/CS/MIRD/EV/default.aspx>, accessed on June 13, 2016.
[62] According to an IRM intranet site, <http://irm.m.state.sbu/sites/ops/ENM/NED/EMS/ipost/Pages/iPost.aspx>, accessed on June 13, 2016.
[63] According to the Department of Homeland Security website, "the purpose of the Trusted Internet Connections (TIC) Initiative, as outlined in OMB Memorandum M-08-05 is to optimize and standardize the security of individual external network connections currently in use by federal agencies, including connections to the Internet. The initiative will improve the federal government's security posture and incident response capability through the reduction and consolidation of external connections and provide enhanced monitoring and situational awareness of external network connections," <https://www.dhs.gov/trusted-internet-connections>, accessed on June 23, 2016.

is currently implementing technologies to ensure 100 percent of network traffic is monitored via Trusted Internet Connections.

Digital Rights Management

According to Department officials, the Department did not implement digital rights management technology[64] at the entity level or at the system-specific level. However, for the six systems reviewed, each system relies on various network application specific or monitoring controls as part of the access controls to safeguard the digital media content and proper usage of Department hardware. According to Department officials, the Department employs multiple layers of automated mechanisms to restrict users' access to media storage areas. It also conducts managerial audits of access attempts and access levels granted.

Management's Reasons for Not Implementing Data Exfiltration Controls

According to Department officials, the Department did not implement digital rights management technology at the Department level and system level because functional availability did not exist to implement across the Department. Also, the current Federal standards do not require digital rights management technology to be implemented throughout the Department. Furthermore, according to Department officials, the Department relies on information system owners to implement relevant security controls at the information-system level to secure and protect data. Department officials stated that the Department employs multiple layers of automated mechanisms to restrict users' access to media storage areas and to audit access attempts and access granted.

Section E. Entities That Provide Services to the Department of State

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 [Section D, above].

Conducting Department business through third party entities, including contractors, may require the extension of the Department's OpenNet and ClassNet networks to non-Department entities. A network extension under these circumstances is an expansion of OpenNet or ClassNet boundaries to include deployment of Department-approved hardware at a non-Department entity location. According to Department officials, a network extension does not involve an interconnection to another system or extranet. However, the establishment of these network

[64] According to the SANS Institute Reading Room, digital rights management "refers to protecting ownership/copyright of electronic content by restricting what actions an authorized recipient may take in regard to that content. [Digital rights management] gives digital-content publishers the ability to securely distribute high-value content such as periodicals, books, photographs, educational material, video, and research and to control the use of that content, preventing unauthorized distribution," <https://www.sans.org/reading-room/whitepapers/basics/digital-rights-management-overview-434>, accessed on July 5, 2016.

extensions must comply with Department regulations and contract provisions, and be documented via a memorandum of agreement, contract modification, or Form DD-254,[65] as appropriate. Furthermore, Department policy[66] requires that both DS/SI/CS and the Office of Information Assurance within IRM approve all network extensions, based on assessments of the requested extension's compliance with Department policy.

The Department's official policies and procedures for these extensions ensure that entities providing services to the Department are implementing the required information security management practices. The relevant Department policies and procedures are established within the Department's FAM, including 5 FAM, "Information Management," and 12 FAM, "Diplomatic Security," which includes chapter 600, "Information Security Technology." Williams Adley reviewed the following Department policies associated with the entities that are required to implement relevant information security management practices:

- 5 FAM 610, "Developing and Managing Information Technology Systems"[67] – This policy establishes Department standards for effective and efficient management of IT investments that project managers must adhere to throughout the system's life cycle. This policy applies to all Department organizations and entities as the authority governing management of major and non-major IT investments. The 5 FAM 612 provides requirements for project development, integration, modification, and maintenance of the Department IT systems, products, and services and applies to all Department personnel, as well as contractors involved in Department systems and program planning, development, modification, integration, operation, and maintenance.[68] As part of the management of IT investments, Department policy states that "All systems (including applicable contractor systems) and applications associated with any projects must be registered in the Information Technology Applications Baseline."[69]

- 5 FAM 1065, "Risk Management" – This policy includes Department policies for information system security control assessments,[70] system certification requirements,[71] criteria for independent certification,[72] penetration testing and vulnerability scanning,[73] unclassified non-Department-owned systems processing Federal information,[74] risk

[65] DD-254 is the "Department of Defense Contract Security Classification Specification" form.
[66] 12 FAM 642.4-4, "Connectivity with Non-Department of State (DOS) Systems or Extensions to Department Systems at Offsite Locations," December 2014.
[67] 5 FAM 611 a, "General," June 2009.
[68] 5 FAM 612 a, "Scope and Authority," February 2008.
[69] 5 FAM 611 e, "General," June 2009.
[70] 5 FAM 1065.1-1, "Information System Security Control Assessment," January 2009.
[71] 5 FAM 1065.1-2, "General Certification Requirements," January 2009.
[72] 5 FAM 1065.1-4, "Criteria for Independent Certification," February 2007.
[73] 5 FAM 1065.1-5, "Penetration Testing," November 2015, and 5 FAM 1065.5 "Vulnerability Scanning," February 2007.
[74] 5 FAM 1065.4-2, "Unclassified Non-Department-Owned Systems Processing Federal Information," February 2007.

analysis,[75] requests for deviations from Department baselines,[76] and the Department's system accreditation process.[77] In addition, 5 FAM 1065.3-1, "Requests for Interagency and Non-Department Connectivity" establishes the Department's policy regarding requests for interagency and non-Department connectivity. Specifically, 5 FAM 1065.3-1 advises:

- DS's Evaluation and Verification Program, in compliance with the Federal Information Security Management Act of 2002[78] reporting requirements, must evaluate and validate location-specific system security controls. Location-specific system security controls must be verified yearly as well as part of the systems authorization process.[79]

- IRM Office of Information Assurance special assessments personnel evaluate requests from bureaus requiring other agencies and non-Department entities to connect to Department information systems.[80] Furthermore, IRM Office of Information Assurance special assessments personnel must develop an assessment of risk to ensure that the requested connections meet the standards and guidelines set forth in NIST SP 800-47, and Department information security policies.[81]

- Connectivity requests must include:
    - A signed Memorandum of Agreement or Memorandum of Understanding;
    - An Interconnection Security Agreement; and
    - For commercial contractors and consultants with contractual relations with the Department, Form DD-254, Contract Security Classification Specification, or other document containing contract security requirements language specifying all information contained in a connectivity Memorandum of Agreement, Memorandum of Understanding, and/or Interconnection Security Agreement.[82]

[75] 5 FAM 1065.2, "Risk Analysis," February 2007.
[76] 5 FAM 1065.3-2, "Requests for Waivers, Exceptions, and Deviations," November 2015.
[77] 5 FAM 1065.4, "Systems Accreditation," January 2009.
[78] According to Public Law 113-283, the Federal Information Security Modernization Act of 2014 amends the Federal Information Security Management Act of 2002.
[79] 5 FAM 1065.4-1, "Department Information Systems," November 2015.
[80] 5 FAM 1065.3-1, "Requests for Interagency and Non-Department Connectivity," January 2009.
[81] Ibid.
[82] Ibid.

APPENDIX A: PURPOSE, SCOPE, AND METHODOLOGY

The Consolidated Appropriations Act, 2016,[1] Section 406, Federal Computer Security, requires the Inspector General of each covered agency[2] 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).

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 Department of State's (Department) computer security controls for covered systems.

[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] Table includes information for the systems where documentation was provided.

The Department's Bureau of Information Resource Management provided separate populations of 60 National Security Systems (NSS) as defined in Section 11103 of Title 40, United States Code, and 235 systems that provide access to personally identifiable information (PII). Williams Adley conducted inquiries with Department personnel and attempted to compare the lists of systems that provide access to PII to the list of Privacy Impact Assessments and System of Record Notices. According to Department officials, a full comparison was not possible based on the System of Record Notices. Consequently, Department officials provided a revised population to Williams Adley. According to Department officials, the Department has 276 covered systems, which includes 216 PII systems and 60 NSS. Williams Adley judgmentally selected 6 (4 systems that provide access to PII and 2 NSS) of 276 covered systems for review.

Williams Adley performed the review from April to June 2016. Williams Adley interviewed Department officials to gain an understanding of the Department's current information security policies and procedures relating to its computer security controls for covered systems. To provide a description of the relevant controls for the covered systems, Williams Adley limited its procedures to inquiries of Department personnel and reviews of written policies and procedures.

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 Department of State's policies, procedures, and practices for access controls at the entity-wide level and for four specific systems for privileged users of information systems with personally identifiable information and reported its findings in Table B.1. Williams Adley reviewed the Department of State's policies, procedures, and practices for access controls entity-wide and for two specific systems for privileged users of National Security Systems. The information on National Security Systems is reported in a separate classified annex to this report.

Table B.1: Comparison of Department 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	Department Policies and Practices	
	Entity-wide	System-Level[3]
AC-6 Least Privilege AC-6 Enhancement (2) Non-privileged access for nonsecurity functions	Present at system level	Electronic Medical Record System (e-MED) – eMED enforces the principle of least privilege by placing eMED users into workgroups, depending on their specific job functions. Integrated Personnel Management System (IPMS) – All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties. Consular Consolidated Database (CCD) – CCD enforces least privilege by employing logical access controls to restrict users to require functions and this applies to reassigned or transferred users as well. CCD – [Enhancement] CCD is configured to audit any use of privileged accounts, or roles, with access to organization-defined security functions or security-relevant information.

[3] Table includes information for the systems where documentation was provided.

National Institute of Standards and Technology Special Publication 800-53, rev. 4, Control	Department Policies and Practices	
	Entity-wide	System-Level[3]
		CCD – [Enhancement] All CCD personnel with privileged accounts are given a separate admin user ID (CAADM) with password to perform privileged functions. Administrators are prohibited from using CAADM account for any functions not associated with administrative duties (for example, email use or web browsing). Consular Lookout and Support System (CLASS) – CLASS uses discretionary access control, which defines and controls access between users and files/programs.
AC-17 Enhancement (4) Privileged Commands/Access	Present at system level	CCD and CLASS – Remote administration/maintenance is prohibited unless specifically authorized.
AU-2 Audit Events AU-2 Enhancement (4) Access by Subset of Privileged Users	Present at system level	eMED – Privileged functions (for example, direct database access or manipulation) are audited. CCD – In accordance with Bureau of Diplomatic Security configuration guides, auditing is enabled to track the addition, deletion, or modification of user or program access privileges. CCD – Audit-related privileges are limited to only individuals with privileged access and need to know.
AU-9 Protection of Audit Information	Present at system level	Audit information only available to privileged accounts.
IA-2 Enhancement (1) Network Access to Privileged Accounts IA-2 Enhancement (3) Local Access to Privileged Accounts	Present at system level	eMED – Privileged accounts (that is, database administrator accounts) require separate logon via database utility. CCD – Multi-factor authentication is implemented through the identification and authentication of the information system through both Active Directory and Public Key Infrastructure (Personally Identify Verification and HSPD-12) respectively.

National Institute of Standards and Technology Special Publication 800-53, rev. 4, Control	Department Policies and Practices	
	Entity-wide	System-Level[3]
		CLASS – [Enhancement] The Bureau of Information Resource Management, which manages the Public Key Infrastructure program, utilizes Personally Identify Verification and HSPD-12 smart cards to provide multi-factor authentication.
SA-7 User-Installed Software	5 FAM 827 Information Systems Management – User: Users are not allowed/prevented from installing software. The configuration settings prevent installing software without elevated privileges.	Follows the entity level control.
SI-3(3) Non-privileged Users	Present at system level	eMED – Non-privileged users are prevented from circumventing malicious code protection through Bureau of Information Resource Management control of Group Policy Objects and implementing adequate security policies.
PL-4 Rule of Behavior	Present at system level	IPMS – Rules of behavior indicate the assignment and limitation of system privileges.
CM-7 Least Functionality	Present at system level	CCD – Management and administrators ascribe to the principle of least privilege/functionality in accordance with applicable Bureau of Diplomatic Security configuration guides.
PS-6 Access Agreements	Present at system level	CLASS – Bureau of Information Resource Management provisions user accounts based upon the user access form they receive and users receive an access request from an authorized organizational individual requesting access.
SC-4 Information Shared Resources	Present at system level	CCD – Validate that each person with admin rights has proper authorization. CCD – Evaluate privileged versus non-privileged accounts to verify that access controls are granting the correct permissions. CLASS – Management reviews privileged versus non-privileged accounts to verify that

National Institute of Standards and Technology Special Publication 800-53, rev. 4, Control	Department Policies and Practices	
	Entity-wide	System-Level[3]
		access controls are granting the correct permissions.
SC-2 Application Partitioning	Present at system level	CLASS – CLASS separates user functionality from management functionality by logically and physically separating presentation layer from its data layer.
PS-3 Enhancement (3) Information With Special Protection Measures	Present at system level	CCD – The data center manager, the system manager, and the Information System Security Officer must work with the Bureau of Diplomatic Security or post personnel to ensure that all personnel with system administrator privileges to an AIS processing Department of State information or connected to a communications system have the minimum security clearance required for accessing that information.

Source: Williams Adley prepared based on documentation provided by the Department.

APPENDIX C: COMPARISON OF POLICIES, PROCEDURES, AND PRACTICES ENTITY-WIDE AND FOR FOUR DEPARTMENT OF STATE SYSTEMS TO FEDERAL PERSONALLY IDENTIFIABLE INFORMATION STANDARDS

Williams, Adley & Company-DC, LLP (Williams Adley) compared Department of State documented controls entity-wide and for four systems 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.

Williams Adley conducted a comparison of the Department of State documented controls for PII system users against Federal requirements outlined in OMB Memorandum M-07-16 and NIST 800-53, rev. 4, Appendix J, Privacy Control Catalog, for the selected National Security Systems. The information on National Security Systems is reported in a separate classified annex to this report.

Table C.1: Comparison of Department of State Personally Identifiable Information Policies to Federal Requirements

Control	Description	Requirement	Department Implemented	Electronic Medical Record System	Integrated Personnel Management System	Consular Consolidated Database	Consular Lookout and Support System
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	No	No	Yes	Yes	Yes
2. Reduce the use of Social Security number	a. Agencies must review the use of Social Security number 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 number	OMB M-07-16	No	No	Yes	No	No

Control	Description	Requirement	Department Implemented	Electronic Medical Record System	Integrated Personnel Management System	Consular Consolidated Database	Consular Lookout and Support System
3. Encryption	Agencies must encrypt using only NIST certified cryptographic modules all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive in writing by the Deputy Secretary or a senior-level individual	OMB M-07-16	Yes	Yes	Yes	Yes	Yes
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	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	Yes	Yes	Yes	Yes	Yes
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	Yes	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	Yes	Yes	Yes	No	No
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	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	Yes	Yes

Control	Description	Requirement	Department Implemented	Electronic Medical Record System	Integrated Personnel Management System	Consular Consolidated Database	Consular Lookout and Support System
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 f. Agencies must update privacy plan, policies, and procedures at least biennially	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes	Yes	Yes
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	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes	Yes	Yes

Control	Description	Requirement	Department Implemented	Electronic Medical Record System	Integrated Personnel Management System	Consular Consolidated Database	Consular Lookout and Support System
	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						
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	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	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 activities involving PII at least annually c. Agencies must ensure that personnel certify acceptance of responsibilities for privacy requirements at least annually	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes	Yes	Yes
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	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No	Yes	Yes

Control	Description	Requirement	Department Implemented	Electronic Medical Record System	Integrated Personnel Management System	Consular Consolidated Database	Consular Lookout and Support System
	accountability with specific statutory and regulatory privacy program mandates and to senior management						
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	No	No	No	Yes	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	Yes	Yes
18. Data Quality (DI-1)	a. Agencies must confirm to the greatest extent practicable upon 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	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes	Yes	Yes

Control	Description	Requirement	Department Implemented	Electronic Medical Record System	Integrated Personnel Management System	Consular Consolidated Database	Consular Lookout and Support System
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	No	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 and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No	Yes	Yes
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	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes	Yes	Yes

Control	Description	Requirement	Department Implemented	Electronic Medical Record System	Integrated Personnel Management System	Consular Consolidated Database	Consular Lookout and Support System
	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						
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	Yes	Yes	Yes	Yes
23. Consent (IP-1)	a. Agencies must provide means, where feasible and appropriate, for individuals to authorize the 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	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes	Yes	Yes

Control	Description	Requirement	Department Implemented	Electronic Medical Record System	Integrated Personnel Management System	Consular Consolidated Database	Consular Lookout and Support System
	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 and guidance for the proper processing of Privacy Act requests	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes	Yes	Yes
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 the PII to other authorized users of the 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	Yes	Yes	Yes	Yes
26. Complaint Management (IP-4)	Agencies must implement a process for receiving and responding to complaints,	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes	Yes	Yes

Control	Description	Requirement	Department Implemented	Electronic Medical Record System	Integrated Personnel Management System	Consular Consolidated Database	Consular Lookout and Support System
	concerns, or questions from individuals about the organizational privacy practices						
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 for all new or modified information systems containing PII	NIST SP 800-53, rev. 4, Appendix J	Yes	No	No	Yes	Yes
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	Yes	Yes
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	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes	Yes	Yes

Control	Description	Requirement	Department Implemented	Electronic Medical Record System	Integrated Personnel Management System	Consular Consolidated Database	Consular Lookout and Support System
	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 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	No	Yes	Yes	Yes

Control	Description	Requirement	Department Implemented	Electronic Medical Record System	Integrated Personnel Management System	Consular Consolidated Database	Consular Lookout and Support System
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 b. Agencies must ensure that its privacy practices are publicly available through organizational websites or otherwise	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes	Yes	Yes
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	Yes	Yes	Yes	Yes
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	NIST SP 800-53, rev. 4, Appendix J	Yes	Yes	Yes	Yes	Yes

Control	Description	Requirement	Department Implemented	Electronic Medical Record System	Integrated Personnel Management System	Consular Consolidated Database	Consular Lookout and Support System
	assess whether the sharing is authorized and whether additional or new public notice is required						

Source: Williams Adley prepared based on documentation provided by the Department.

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

oig.state.gov

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