Office of Audits
Office of Inspector General
U.S. General Services Administration

U.S. General Services Administration Office of Inspector General Cybersecurity Act Assessment

Audit Number A160062

August 10, 2016

Introduction

This report presents the results of the U.S. General Services Administration (GSA) Office of Inspector General's assessment of GSA's information technology (IT) policies and practices, as required under the Cybersecurity Act of 2015 (the Act).[1] The Act requires Inspectors General to report on the status of specific IT security management practices related to systems significant to national security or containing personally identifiable information. The Act refers to these systems as "covered systems." For each covered system, the Act required us to:

1. Describe and list the logical access policies and practices used by GSA, including whether appropriate standards were followed.
2. Describe and list GSA's privileged users' logical access controls and multi-factor authentication. If privileged user logical access controls or multi-factor authentication are not used, describe the reasons why.
3. Describe and list GSA policies and procedures to conduct software inventories and the licenses associated with such software.
4. Describe and list GSA's capabilities to monitor and detect exfiltration of sensitive data and other threats, including: (1) data loss prevention, (2) forensics and visibility, and (3) digital rights management. Describe how GSA uses these capabilities. If these capabilities are not being used, describe the reasons why.
5. Describe and list GSA's policies and procedures to ensure that entities, including contractors, providing services to GSA monitor and detect exfiltration of sensitive data and other threats, including: (1) data loss prevention, (2) forensics and visibility, and (3) digital rights management.

In accordance with the Act, we performed an assessment of GSA's 18 covered systems.[2] We structured our assessment to mirror the requirements enumerated in the Act and used procedures such as interviewing GSA information system security officials, compiling Agency questionnaire responses, and reviewing system-specific security documentation. Our assessment, while not a comprehensive audit or evaluation, provides a broad overview of relevant Agency system security policies and practices. Our office conducts audits and evaluations of these policies and practices as part of our on-going oversight efforts.[3]

Results of Assessment

GSA policies and procedures regarding access controls are generally consistent with significant government-wide policies and procedures, including relevant standards established by the National Institute of Standards and Technology (NIST) and Office of Management and Budget (OMB) guidance. For 11 of its 18 covered systems, GSA has implemented multi-factor authentication for privileged users consistent with government-

[1] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N-Cybersecurity Act of 2015, § 406, 129 Stat, 2242, 2984-85 (2015)

[2] A listing and description of these systems is included as ***Appendix A***.

[3] See, for example, *Management Alert Report: GSA Data Breach (JE16-004)*, May 12, 2016.

wide policies for information systems. For the 7 non-compliant covered systems, GSA relies on compensating controls for privileged user access. The Agency has also implemented appropriate automated or manual software and license inventory management practices in accordance with NIST standards. In addition, GSA has implemented numerous capabilities to protect against data loss or theft. Finally, GSA has created policies that require IT service providers to adhere to GSA IT security policies and procedures.

Logical Access Controls

GSA IT Security Policy (*i.e., GSA Order CIO 2100.1J*) provides general requirements for, among other things, logical access controls in GSA systems and systems operated on the Agency's behalf. The *GSA IT Security Policy* requires that Agency systems adhere to NIST standards and GSA procedural guidance on logical access controls to the maximum extent possible. The general logical access control requirements in this policy include, but are not limited to:

(1) All GSA systems must implement logical access controls in order to authorize or restrict the activities of users and system personnel to authorized transactions and functions;
(2) Information system accounts must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Reviews and validations of system and staff users' accounts are required to be completed annually to ensure the continued need for system access; and
(3) Information systems must enforce the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.

GSA IT Security Procedural Guide for Access Control (*i.e., CIO-IT-Security-01-07*) sets forth guidance for the implementation of access controls in GSA systems. This includes processes for choosing and managing access controls, along with a set of access controls recommended by NIST, such as session time-outs and disabling inactive accounts. In addition, access controls implemented for each covered system are documented in specific and unique system security plans.

We determined that access control policies for non-privileged users generally adhere to appropriate standards for logical access controls, including requirements set forth in NIST Special Publications, Federal Information Processing Standards (FIPS), OMB guidance, and industry best practices.

Privileged User Access Controls

GSA has implemented multi-factor authentication for privileged system users (including system administrators) at the individual system level for 11 of the 18 covered systems. For each of these systems, privileged users are required to login using their multi-factor authentication credentials, including a username, password, and personal identity verification card or token.

GSA has not implemented multi-factor authentication for privileged user access at the individual system level as required by NIST guidance for the remaining seven covered systems. However, all users – including privileged users – must first provide multi-factor authentication as part of their login to GSA's network in order to access these systems. GSA IT security officials cited a number of reasons for not implementing multi-factor authentication for these systems, including:

- No contractual requirement for use of multi-factor authentication to access the system;
- Implementation of multi-factor authentication is time and cost prohibitive;
- Planned replacement or retirement of the system;
- Customer resistance to use of multi-factor authentication at the individual systems level; and/or
- Compensating controls, such as the required use of multi-factor authentication to access GSA's network and background checks.

Software and License Inventory Management

GSA has policies and procedures in place for software inventories and licenses. Specifically, *GSA IT Security Procedural Guide for Managing Enterprise Risk* (*i.e., CIO-IT-Security-06-30*) includes the Agency's general requirement for maintaining software inventories. Additionally, GSA mandates compliance with the software and license management controls included in *NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations*, as part of the Agency's overall IT security policy.

The Agency has also implemented *CIO Software License Management (i.e., GSA Order 2108.1)*. This policy sets forth GSA's requirements for:

- Establishing a software management program that oversees software licensing in GSA;
- Establishing and maintaining a software license management repository;
- Removing software no longer included in the IT Standards Profile or no longer under proper licensing agreements;[4] and
- Reporting licensing information to GSA IT for inclusion in the GSA Software License Management Repository.

[4] The IT Standards Profile is GSA's set of hardware, software, and industry standards prescribed to ensure the integrity of the Agency's IT infrastructure.

Furthermore, specific procedures and controls related to maintaining software inventories and their associated licenses are documented within the system security plans for each covered system. We reviewed the security plans for the 18 covered systems and found that 14 use automated tools for software inventory management, such as BMC *Blade Logic Operations Manager*, BMC *Remedy Asset Management,* IBM *Rational ClearCase*, and IBM *BigFix*. For the remaining four systems, GSA manually tracks software inventories and licenses in spreadsheets.

Prevention of Sensitive Data Loss

GSA has a number of data loss prevention measures currently in place. These measures include:

- Intrusion detection systems, firewalls, and security incident and event management systems, implemented at the network level to perform data exfiltration (*e.g.,* data theft or leakage) detection and monitoring;
- The GSA Security Operations Center dashboard configured to detect potentially malicious network activity and provide notification of network traffic destined for suspected unauthorized internet recipients;
- Outbound e-mail filters to protect social security numbers in Google *Gmail* and GSA's *MailGate*;
- *Cloudlock* which identifies and prevents excessive document sharing in the Google environment;
- Web application firewalls which have filters that can detect and block social security number and credit card number leakage from the GSA network; and
- Malicious software detection programs such as McAfee *VirusScan Enterprise*.

GSA also uses forensics capabilities, such as Access Data *Forensics Toolkit,* to provide visibility related to user activities, including reviewing logs and audit trails. This allows Agency IT security personnel to investigate security incidents as needed.

According to GSA IT officials, the Agency does not use digital rights management at this time due to its limited availability. Furthermore, digital rights management is not required by NIST 800-53. GSA officials stated that they will consider using these technologies when they become readily available via GSA's IT service providers.

Controls Over IT Service Providers

The *GSA Procedural Guide to Security Language for IT Acquisition Efforts* (*i.e., CIO-IT-Security-09-48*) establishes IT security language for inclusion in GSA's IT acquisitions. This language is required for all statements of work where the information system is supported by an IT service provider. These contractual clauses require the service provider to adhere to GSA IT security policies and all IT security requirements for federal information and information systems, such as the Federal Information Security Management Act, NIST standards, and OMB guidance. These requirements include items such as proper access controls, configuration management, and contingency planning.

In addition, GSA IT security officials cited the *GSA IT Security Policy* as the governing policy establishing the requirements for all systems, including contractor owned and operated systems and outsourced operations, to implement appropriate security safeguards throughout all phases of the systems' lifecycle (*e.g.,* design, implementation, and decommissioning). This policy requires that all GSA IT systems, including those operated by a contractor on behalf of GSA, must implement proper security controls according to the security categorization level in accordance with *FIPS Publication 199 – Standards for Security Categorization of Federal Information and Information Systems*; *FIPS Publication 200 – Minimum Security Requirements for Federal Information and Information Systems*; and *NIST Special Publication 800-53*.

Conclusion

GSA has implemented policies and procedures surrounding access to covered systems that are generally consistent with significant government-wide standards, requirements, and guidance. In addition, GSA has implemented multi-factor authentication for privileged users in accordance with government-wide policies for the majority of its covered systems. For the remainder of its covered systems, GSA relies on compensating controls for privileged user access. The Agency also uses automated or manual processes that conform to applicable standards to manage its inventory of software and licenses, and has deployed a number of measures designed to guard against loss of sensitive data. Finally, GSA has developed policies requiring the Agency's IT service providers to adhere to its own IT security policies and procedures.

If additional detail is needed about GSA's IT policies and procedures or individual covered systems, please contact Mr. R. Nicholas Goco, Assistant Inspector General for Auditing, at (202) 501-0374.

APPENDIX A – GSA Covered Systems

System	Description
The Comprehensive Human Resources Integrated System (CHRIS)	Houses GSA's human resource records.
Child Care Subsidy	Administers and processes all requests for the Child Care Subsidy Program.
E-Travel/E-Gov Travel	Supports Federal Government travel functions including research, booking, and ticketing.
Customer Engagement Organization	GSA's implementation of Salesforce.com cloud services, used for customer relationship management, employee collaboration, and shared development efforts.
Electronic Document Management System (EDMS)	A repository for documents such as the Public Buildings Service's computer-aided design drawings, resumes, and project documentation.
Enterprise Server Services (ESS)	Consists of directory management and server services. This includes the enterprise server infrastructure and the authentication/authorization/ accounting infrastructure.
Enterprise Physical Access Control System (E-PACS)	Controls personnel entry into GSA-managed facilities in the Washington, D.C. metropolitan area and restricted access areas within those facilities.
Federal Business Opportunities (FBO)	Allows contractors to search for, monitor, and retrieve information on federal business opportunities.
Federal Personal Identity Verification (USAccess)	Provides common, shared infrastructure and services to assist federal agencies in the implementation of Homeland Security Presidential Directive 12. These services include: enrollment services; systems infrastructure through a centralized personal identity verification Identity Management System; card production facility; and card activation, finalization, and issuance.
Federal Procurement Data System – Next Generation (FPDS-NG)	Collects government agencies' contract data for reporting purposes, such as tracking small business goals, showing the geographical placement of contracts, and summarizing contract data for a specific contractor.

GSA Credential and Identity Management System (GCIMS)	Provides critical security protection services to hosted applications used by the GSA enterprise and the public user community.
Enterprise Organization of Google Apps and Salesforce	Enterprise Cloud Services is a general support system with applications hosted by Google and Salesforce. The Google and Salesforce applications provide IT services to GSA.
SmartPay	Purchase card management system.
GSAJobs Hiring Management System (GSAJobs)	Used by GSA Office of Human Resources Management as a tool for automation of staffing and human resource management related functions.
Payroll Accounting and Reporting System (PAR)	Provides payroll functionality from initial hire through final payment at separation and submission of retirement records to the Office of Personnel Management.
Personal Property Sales Program, Sales Automation System (SASy)	Comprised of several applications that support the sale and auction of surplus federal personal property and real estate, as well as the reverse auctioning of government commodities and services.
System for Award Management (SAM)	Comprised of systems that facilitate every phase of the acquisition lifecycle: requirement definition, acquisition planning, synopsis and solicitation, screening and evaluation, award, and contract administration.
The Museum System (TMS)	Provides collection management capabilities for the GSA art collection. Used by museums and other organizations, including private corporations, to catalog art and archival collections, along with exhibitions, loans, and other related events.

APPENDIX B – DISTRIBUTION

Administrator (A)

Chief Information Officer (I)

Chief Administrative Services Officer (H)

GAO/IG Audit Response Division (H1G)

Assistant Inspector General for Auditing (JA)