U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

DEC 19 2017

MEMORANDUM FOR: EMILY W. MURPHY
ADMINISTRATOR (A)

FROM: CAROL F. OCHOA CFO
INSPECTOR GENERAL (J)

SUBJECT: Fiscal Year 2017 Independent Evaluation of the U.S. General Services Administration's Compliance with the Federal Information Security Modernization Act of 2014 Report

This memorandum transmits KPMG LLP's (KPMG) evaluation report of GSA's compliance with the *Federal Information Security Modernization Act of 2014* (FISMA) for fiscal year 2017.

FISMA requires Inspectors General or an independent external auditor, as determined by the Inspector General of the agency, to perform an annual evaluation of their agency's security program and practices. Under a contract monitored by my office, KPMG, an independent public accounting firm, performed the evaluation to assess if GSA's information security program complied with FISMA. KPMG performed the evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation* and the Office of Management and Budget's (OMB) FISMA reporting guidance.

In connection with the contract, we reviewed KPMG's report and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, opinions on GSA's security program or conclusions about the effectiveness of GSA's internal controls or on whether GSA's security program complied with FISMA or conclusions on compliance with laws and regulations. KPMG is responsible for the attached report and the conclusions expressed in the report. However, our review disclosed no instances where KPMG did not comply with CIGIE's *Quality Standards for Inspection and Evaluation* and OMB's FISMA reporting guidance.

A draft report was provided to the GSA Office of the Chief Information Officer for review and comment. The Office of the Chief Information Officer's response to the draft report is included in its entirety in the attached final report.

The fiscal year 2018 FISMA independent auditors will follow up on the outstanding recommendations and evaluate the adequacy of corrective actions.

We appreciate the courtesies and cooperation extended to KPMG and our audit staff by GSA during the evaluation. If you have any questions, please contact R. Nicholas Goco, Assistant Inspector General for Auditing, at (202) 501-2322.

Attachment

KPMG LLP
1676 International Drive, Suite 1200
McLean, VA 22102

Carolyn Presley-Doss
Deputy Assistant Inspector General for Audit Policy and Oversight
General Services Administration
Office of Inspector General
1800 F St., NW, Suite 5037
Washington, DC 20405

December 11, 2017

Dear Ms. Presley-Doss,

We have submitted the following Federal Information Security Modernization Act (FISMA) report to the General Services Administration (GSA) Office of Inspector General (OIG):

- *Fiscal Year 2017 Independent Evaluation of the U.S. General Services Administration's Compliance with the Federal Information Security Modernization Act of 2014 Report*

This report was provided to you in this format pursuant to your written request as set forth in Contract GS-23F-8127H, Order Number GSH1416AA0136, and is subject in all respects to the terms and conditions of, including restrictions on disclosure of this deliverable to third parties.

Detailed within the FY 2017 FISMA Report are recommendations to address specific GSA and system-level deficiencies within GSA's information security program and practices. When developing plans of actions and milestones (POA&Ms) or corrective actions, management should assess whether these deficiencies are contained to their respective areas as described in this report or whether the recommendations should be considered for other systems, security control areas, or processes within GSA's information system security program.

Please let me know if you have any questions.

Kind regards,

James DeVaul

Fiscal Year 2017 Independent Evaluation of the U.S. General Services Administration's Compliance with the Federal Information Security Modernization Act of 2014 Report

November 29, 2017

KPMG LLP
1676 International Drive, Suite 1200
McLean, VA 22102

U.S. General Services Administration
Federal Information Security Modernization Act of 2014 Evaluation

Table of Contents

KPMG LLP
1676 International Drive
McLean, VA 22102

Administrator and Inspector General
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

Re: Fiscal Year 2017 Independent Evaluation of the U.S. General Services Administration's Compliance with the Federal Information Security Modernization Act of 2014 Report

This report presents the results of our independent evaluation of the U.S. General Services Administration's (GSA) information security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including GSA, to have an annual independent evaluation performed of their information security program and practices and to report the results of the evaluations to the Office of Management and Budget (OMB). OMB has delegated its responsibility for the collection of annual FISMA responses to the Department of Homeland Security (DHS). DHS in conjunction with OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the FY 2017 FISMA Reporting Metrics to collect these responses. FISMA requires that the agency Inspector General (IG) or an independent external auditor perform the independent evaluation as determined by the IG. GSA contracted with KPMG LLP (KPMG) to conduct this independent evaluation. The Office of Inspector General (OIG) monitored our work to ensure professional standards and contractual requirements were met.

We conducted our independent evaluation in accordance with CIGIE Quality Standards for Inspection and Evaluation and applicable American Institute of Certified Public Accountants (AICPA) standards.

The objective for this independent evaluation was to assess the effectiveness of GSA's information security program and practices for the period October 1, 2016 to September 30, 2017 for its information systems, including GSA's compliance with FISMA and related information security policies, procedures, standards, and guidelines. We based our work, in part, on a selection of GSA-wide security controls and a selection of system-specific security controls across 7 selected GSA information systems and 5 GSA contractor information systems. Additional details regarding the scope of our independent evaluation are included in Appendix I, *Objective, Scope and Methodology*. Appendix II, *Status of Prior-Year Findings,* summarizes GSA's progress in addressing prior-year recommendations. Appendix III contains a glossary of terms used in this report.

Consistent with applicable FISMA requirements, OMB policy and guidance, and National Institute of Standards and Technology (NIST) standards and guidelines, GSA established and maintained its information security program and practices for its information systems for the 5 cybersecurity functions[1] and 7 FISMA

[1] OMB, DHS, and CIGIE developed the FY 2017 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers (CIO) Council. In FY 2017 the 7 IG FISMA metric domains were aligned with the 5 cybersecurity functions of identify, protect, detect, respond, and recover as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

metric domains.[2] However, the program was not effective[3] because 1 cybersecurity function (Respond) was assessed at Managed and Measurable (Level 4) and the other 4 (Identify, Protect, Detect, and Recover) were assessed at the Consistently Implemented (Level 3). We also reported 15 deficiencies within 3 of the 5 cybersecurity functions and within 4 of the 7 FISMA metric domains that we identified during fieldwork as follows:

Cybersecurity Function: Identify

- Inventory definitions were not appropriately classified. (Risk Management)
- GSA did not have a formal review and acceptance process for contractor deliverables. (Risk Management)

Cybersecurity Function: Protect

- Two GSA information systems did not document the authorization and testing of application changes, operating system patches, and database patches. (Configuration Management)
- Five GSA information systems did not have a formal process for account authorization of privileged and non-privileged users. (Identity and Access Management)
- One GSA information system did not remove terminated privileged accounts in a timely manner. (Identity and Access Management)
- Two GSA information system's privileged operating system and database account reviews were not performed in accordance with GSA policy. (Identity and Access Management)
- Two GSA information system's session termination configuration settings were not configured in accordance with GSA policy. (Identity and Access Management)

Cybersecurity Function: Recover:

- A weekly full backup was not performed for 1 GSA information system. (Contingency Planning)

We have made 13 recommendations related to these control deficiencies that, if effectively addressed by management, should strengthen the respective GSA information systems and GSA's information security program. In a written response, the GSA CIO concurred with our findings and recommendations (see *Management Response*).

This independent evaluation did not constitute an engagement in accordance with *Generally Accepted Government Auditing Standards (GAGAS).* KPMG did not render an opinion on GSA's internal controls over financial reporting or over financial management systems as part of this evaluation. We caution that projecting the results of our evaluation to future periods or other GSA information systems not included in our selection is subject to the risks that controls may become inadequate because of changes in technology or because compliance with controls may deteriorate.

KPMG LLP

November 29, 2017

---

[2] As described in the DHS' *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0,* the 7 FISMA metric domains are: risk management, configuration management, identity and access management, security training, information security continuous monitoring, incident response, and contingency planning.

[3] The scoring methodology is described in the DHS' *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0* which requires a Managed and Measurable rating (Level 4) to be considered effective as determined by the entries in CyberScope.

BACKGROUND

Federal Information Security Modernization Act

Title III of the E-Government Act of 2002 (the Act), which was amended in 2014, commonly referred to as FISMA, focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The Act assigns specific responsibilities to agency heads and IGs in complying with requirements of FISMA. The Act is supported by OMB, agency security policy, and risk-based standards and guidelines published by NIST related to information security practices.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of FISMA and related OMB policies and NIST procedures, standards, and guidelines. FISMA directs federal agencies to report annually to the OMB Director, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies and procedures. OMB has delegated some responsibility to DHS in memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, for the operational aspects of federal cybersecurity, such as establishing government-wide incident response and operating the tool to collect FISMA metrics. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG.

FY 2017 Inspector General FISMA Reporting Metrics

For FY 2017, OMB, DHS, and CIGIE implemented changes to the IG FISMA reporting metrics to organize them around the 5 information security functions outlined in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): identify, protect, detect, respond, and recover. In addition, CIGIE implemented maturity models for the FY 2017 FISMA metric domains: risk management (RM), configuration management (CM), identity and access management (IA), security training (ST), and contingency planning (CP), and revised the information security continuous monitoring (ISCM) and incident response (IR) maturity models that were instituted in FY 2015 and FY 2016, respectively. **Table 1** shows the alignment of Cybersecurity Framework to the FISMA Metric Domains.

Cybersecurity Framework Security Functions	FY 2017 IG FISMA Metric Domains
Identify	Risk Management
Protect	Configuration Management Identity and Access Management Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Table 1: Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FY 2017 IG FISMA Metric Domains.

In the past, the ISCM and IR models had maturity levels for people, process, and technology. In FY 2017, CIGIE eliminated specific people, process, and technology elements and, instead, issued specific questions. These models have 5 levels: ad-hoc, defined, consistently implemented, managed and measurable, and optimized. The introduction of a 5-level maturity model is a deviation from previous DHS guidance over the CyberScope questions.

OVERALL EVALUATION RESULTS

Consistent with applicable FISMA requirements; OMB policy and guidance, and NIST standards and guidelines; GSA's information security program and practices for its information systems were established and have been maintained for the 5 cybersecurity functions and 7 FISMA metric domains. The FISMA program areas are outlined in the *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0* and were developed by DHS' Office of Cybersecurity and Communications Federal Network Resilience. The CyberScope functions and domains are:

- Identify
  - Risk management
- Protect
  - Configuration management
  - Identity and access management
  - Security training
- Detect
  - Information security continuous monitoring
- Respond
  - Incident response
- Recover
  - Contingency planning

However, while a security program has been implemented across GSA, we identified 15 deficiencies that we reported to GSA management in 3 of 5 FISMA metric functions. We have made 13 recommendations related to these deficiencies that, if effectively addressed by management, should strengthen the respective information systems and GSA's information security program. However, the GSA security program was not effective because 1 cybersecurity function (Respond) was assessed at Managed and Measurable (Level 4) and the other 4 cybersecurity functions (Identify, Protect, Detect, and Recover) were assessed at Consistently Implemented (Level 3). We specifically noted the following deficiencies in 3 cybersecurity functions:

Cybersecurity Function: Identify

- Inventory definitions were not appropriately classified. (Risk Management)
- GSA did not have a formal review and acceptance process for contractor deliverables. (Risk Management)

Cybersecurity Function: Protect

- Two GSA information systems did not document the authorization and testing of application changes, operating system patches, and database patches. (Configuration Management)
- Five GSA information systems did not have a formal process for account authorization of privileged and non-privileged users. (Identity and Access Management)
- One GSA information system did not remove terminated privileged accounts in a timely manner. (Identity and Access Management)
- Two GSA information system's privileged operating system and database account reviews were not performed in accordance with GSA policy. (Identity and Access Management)
- Two GSA information system's session termination configuration settings were not configured in accordance with GSA policy. (Identity and Access Management)

Cybersecurity Function: Recover:

- A weekly full backup was not performed for 1 GSA information system. (Contingency Planning)

The *Findings* section of this report presents the detailed findings and associated recommendations. We will follow up on the status of the findings as part of the FY 2018 independent evaluation.

Additionally, we evaluated the open prior-year findings from the FY 2016 and FY 2015 FISMA evaluations and noted that management closed a total of 2 of 7 findings, 1 remains open, and 4 are partially closed. See Appendix II, *Status of Prior-Year Findings*, for additional details.

In a written response to this report, the GSA CIO concurred with our findings and recommendations (see *Management Response*).

FINDINGS

1. Identify Function – Risk Management

System Inventory

We inspected GSA FISMA reportable system inventory dated March 10, 2017 and August 3, 2017 and determined 8 of the 14 information systems were not appropriately classified as federal information systems based on GSA's definition.

GSA Information Technology (IT) Security Policy CIO 2100.1K, Section 7: Definitions, page 5, states:

> "f. Contractor System. An information system processing or containing GSA or federal data where the infrastructure and applications are wholly operated, administered, managed, and maintained by a contractor in non-GSA facilities.
> g. Federal information system. An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
> h. Agency system (i.e., Federal system). An information system processing or containing GSA or Federal data where the infrastructure and applications are NOT wholly operated, administered, managed, and maintained by a Contractor in non-GSA facilities."

NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, page G-5, states:

> "PM-5 INFORMATION SYSTEM INVENTORY
> Control: The organization develops and maintains an inventory of its information systems.
> Supplemental Guidance: This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements. For specific information system inventory reporting requirements, organizations consult OMB annual FISMA reporting guidance."

GSA updated the *GSA IT Security Policy CIO 2100.1K* to include the definitions to use when classifying information systems; however, when updating the FISMA inventory, human error caused the information systems to be classified as contractor and not federal. GSA is considering expanding the definitions of information systems to include cloud and hybrid to accurately reflect the current inventory of information systems. Failure to properly classify information systems will not provide a complete and accurate listing of the information system type that is used by GSA to support their mission. A complete and accurate inventory is a monitoring exercise that is necessary to ensure that appropriate monitoring and oversight of the contractor information systems is performed. GSA did correct the system classification for 5 of the 8 GSA information systems from contractor to federal.

We recommend that GSA perform the following actions:

1. Review the system inventory and reevaluate the system classifications based on GSA's definitions.
2. Consider expanding GSA definitions to include other types of systems such as cloud and hybrid.

Contractor Systems

We determined that GSA was receiving the required contractor deliverables for the 5 contractor information systems. However, we noted instances where the review and acceptance of the deliverables was not documented, did not follow a formal process when comments or concerns were presented to the contractor, and did not obtain sufficient assurance that GSA was monitoring the performance of the services provided by the contractor.

GSA IT Security Procedural Guide: Security Language for IT Acquisition Efforts, GSA-IT Security-09-48, Revision 3, February 2, 2017, page 10, Section 2.5 *Reporting and Continuous Monitoring*, states:

> "Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the contractors system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to GSA. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow GSA AOs [Authorizing Officials] to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur."

While GSA was receiving information from the contractors, *GSA IT Security Procedural Guide: Security Language for IT Acquisition Efforts* does not provide review and acceptance standards that should be followed. Failure to properly review and accept the deliverables may result in security weaknesses that are not appropriately tracked by GSA for remediation by the contractor.

We recommend that GSA perform the following actions:

1. Implement a formalized review and acceptance process of contractor deliverables that includes the information system security officer (ISSO) and information system security manager (ISSM) review of the information, and contracting officer's representative (COR) acceptance of the deliverable.
2. Provide training to applicable GSA employees on reviewing and accepting contractor deliverables stated in the *GSA IT Security Procedural Guide: Security Language for IT Acquisition Efforts, GSA-IT Security-09-48*.

2. Protect Function – Configuration Management

Change/Patch Management Approval

We identified the following exceptions:

- One GSA information system's authorization and testing evidence for the Quarter 1 Oracle database patch could not be provided; and
- One GSA information system's authorization and testing evidence for Quarter 1 and Quarter 3 application changes and the November 2016 Linux and Windows operating system patches could not be provided.

GSA IT Security Procedural Guide: Configuration Management (CM) CIO-IT Security-01-05, Revision 3 July 14, 2015, Section 4.3 CM-3 Configuration Change Control, page 21, states:

> "Manage configuration changes to the information system through a chartered Configuration Control Board (CCB) that approves proposed changes to the system. The CCB should monitor the following:
> [...]
> - Authorize, document, and control changes to the information system. Include emergency changes in the configuration change control process.
> - [...] Ensure that any testing performed does not adversely impact the information system (perform the test on a test platform, not a production platform)."

NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, page F-66, states:

> "CM-3 CONFIGURATION CHANGE CONTROL
> Control: The organization:
> [...]
> b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
> c. Documents configuration change decisions associated with the information system;
> d. Implements approved configuration-controlled changes to the information system;
> e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]"
>
> page F-67, states:
>
> "CM-3(2) CONFIGURATION CHANGE CONTROL - Test/Validate/Document Changes:
> The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system."

Due to an update in patch management tracking tools for 1 of the GSA information systems, the evidence for the testing of Quarter 1 2017 database patches were lost and could not be provided. For 1 other GSA information system, management was unable to provide documentation showing evidence that application and operating system patches were tested and approved prior to being implemented into production.

Without maintaining evidence of testing and authorizations, the risk increases that unauthorized changes/patches could be introduced to production impacting the confidentiality, integrity, and availability of the data residing on the information system.

We recommend that GSA perform the following actions:

1. Provide training on the change management requirements required by GSA policy to applicable GSA employees and contractors.
2. Document evidence of authorization of application changes, and operating system and database patches.

3. Protect Function – Identity and Access Management

Account Management

We identified the following exceptions:

a. Five GSA information systems, evidence of account authorization could not be provided for privileged and non-privileged user accounts
b. Terminated privileged accounts for the 1 GSA information system's operating system were not removed within 30 days of separation.
c. Two GSA information systems privileged account reviews for the operating system and database were not performed in accordance with GSA policy to verify that the individuals needed privileged access.

GSA IT Security Policy CIO 2100.1K, Section 22. Supervisors, page 31 states:

> "Supervisors are responsible for:
> a. Conducting annual review and validation of staff user accounts to ensure the continued need for access to a system;"

Section 2. Policies on Operating Controls, page 41 states:

> "(5) User authorizations must be verified annually for all information systems."

Section 2. Policies on Technical Controls, page 69 states:

> "(8) On a regular basis, data and system owners must inspect user access entitlements as needed to detect the following conditions that warrant termination, revocation, or suspension of account access:
> [...]
> 2. Upon issuance of the CISO monthly separation reports, Data and system owners must verify within 30 days that separated personnel no longer maintain access to GSA IT systems or resources."

GSA IT Security Procedural Guide: Access Control (AC) CIO-IT Security-01-07, Revision 4, May 8, 2017, Section 5.2 AC-2 Account Management, page 16, states:

> "Control: The organization:
> [...] e. Requires approvals by [System Owner and GSA Authorizing Official] for requests to create information system accounts;
> f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [GSA CIO-IT Security-01-01, Identification and Authentication, GSA CIO-IT Security-01-07, Access Control, and GSA-defined procedures or conditions (as applicable)];
> [...]
> i. Authorizes access to the information system based on:
> a. A valid access authorization;
> b. Intended system usage; and
> c. Other attributes as required by the organization or associated missions/business functions;
> j. Reviews accounts for compliance with account management requirements [annually];"

GSA IT Security Procedural Guide: Termination and Transfer CIO-IT Security-03-23, Revision 3, April 27, 2017, Section 8.1 PS-4 Personnel Termination, page 13, states:

> "Common Control Implementation: Disabling information system access is initiated and facilitated by the supervisor/CO/COR [Contracting Officer/ Contracting Officer Representative] of an individual. Retrieval of all information system-related property which includes HDPS-12 cards, authentication tokens (USB for privileged access), laptops, etc. is a common control provided by IO [IO is now part of Office of Deputy CIO (ID), specifically Office of Enterprise Infrastructure Operations (IDI)] and facilitated by the supervisor.
> [...]
> System Specific Expectations: The supervisor/CO/COR is responsible for notifying the appropriate ISSMs/ISSOs of a user's off-boarding so they can take appropriate action at a system/application level."

The privileged user was part of a large batch of approvals and, due to oversight, the form was not signed by the ISSO; however, the user's access was authorized. GSA management was not able to provide access authorization evidence for 2 GSA information system users, operating system administrators, and database administrators. For an information system, it does not have a formalized process for granting, reviewing, or terminating system accounts. GSA management for a system was not performing a sufficient review of access of privileged users.

Without proper account management processes, procedures, and configuration settings, potential for an unauthorized user to gain access to the system exists. This could result in unnecessary system downtime and destruction/exposure of critical data.

We recommend that GSA perform the following actions:

1. Implement a formal process for approving, reviewing, and removing privileged access.
2. Provide training to individuals and contractors that support GSA information systems on entity and system specific policies and for authorizing, granting, reviewing, and removing access.
3. Maintain evidence for approving, reviewing, and removing access for individuals with privileged and non-privileged access.

Session Termination

We determined that 2 of the 7 GSA information system's application, operating system, and/or database session termination configuration settings were configured to be less restrictive than the requirements in the GSA policy.

GSA IT Security Procedural Guide: Access Control (AC) CIO-IT Security-01-07, Revision 4, May 8, 2017, Section 5.11 AC-12 Session Termination, page 21, states:

> "Control: The information system automatically terminates a user session after [(a) A remote access connection after thirty (30) minutes of inactivity; (b) An Internet accessible application session after thirty (30) minutes of inactivity; or (c) A non-interactive user session after thirty (30) – sixty (60) minutes of inactivity. Static web sites and long running operations (e.g., batch jobs) are not subject to this time limit]. GSA Implementation Guidance: Control AC-12 is applicable at the FIPS [Federal Information Processing Standards] 199 Moderate and High levels."

GSA IT Security Policy CIO 2100.1K, Section a. Identification and authentication, pages 61 - 62, states:

> "(15) FIPS 199 Moderate and High impact systems shall automatically terminate:
> (a) A remote access connection after thirty (30) minutes of inactivity;
> (b) An Internet accessible application session after thirty (30) minutes of inactivity; or
> (c) A non-interactive user session after thirty (30) - sixty (60) minutes of inactivity. Static web sites and long running operations (e.g., batch jobs) are not subject to this time limit."

Due to a lack of awareness of entity-wide requirements by 2 of 7 GSA information system's management, session termination configuration settings were not appropriately implemented.

Without proper session termination configuration settings, the potential exists for an unauthorized user to gain access to the system. This could result in unnecessary system downtime and destruction/exposure of critical data.

We recommend that GSA perform the following action:
1. Configure the session termination settings in accordance with GSA policy.

4. Recover Function – Contingency Planning

System Backups

We determined that GSA requires Friday full backups to be performed, however, a Friday full weekly backup was not performed for 1 GSA information system for 1 of 5 selected weeks.

GSA IT Security Procedural Guide: Contingency Planning (CP) CIO-IT Security-06-29, Revision 3, March 9, 2016, Section 4.8 CP-9 Information System Backup, page 23, states:

> "Control: The organization:
> a. Conducts backups of user-level information contained in the information system [at least a GFS [Grandfather-father-son] Scheme with Daily Incremental and Friday Full];
> b. Conducts backups of system-level information contained in the information system [at least a GFS Scheme with Daily Incremental and Friday Full];
> c. Conducts backups of information system documentation including security-related documentation [at least a GFS Scheme with Daily Incremental and Friday Full];"

Without functioning backups and replication, this could result in unnecessary downtime and lack of data integrity in the event of a disaster.

We recommend that GSA perform the following actions:
1. Develop and implement a formalized mitigation strategy for failed system backups.
2. Maintain evidence of proper completion of backups performed.
3. Provide training on the backup management requirements.

MANAGEMENT RESPONSE TO THE REPORT

The following is the GSA CIO's response, dated November 14, 2017, to the FY 2017 FISMA Evaluation Report.

GSA

GSA Office of the Chief Information Officer

November 14, 2017

MEMORANDUM FOR CAROLYN PRESLEY-DOSS
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
AUDIT POLICY AND OVERSIGHT – JA

FROM DAVID A. SHIVE
CHIEF INFORMATION OFFICER – I

SUBJECT: Agency Management Response – Draft Evaluation Report *KPMG's Fiscal Year 2017 Independent Evaluation of the U.S. General Services Administration's Compliance with the Federal Information Security Modernization Act of 2014*

The Office of the Chief Information Officer appreciates the opportunity to review and comment on the draft evaluation report entitled *Draft Evaluation Report: KPMG's Fiscal Year 2017 Independent Evaluation of the U.S. General Services Administration's Compliance with the Federal Information Security Modernization Act of 2014*.

We have reviewed the draft evaluation report and we agree with the findings and recommendations stated in the report.

If you have any questions or concerns, please contact Kurt Garbars, Chief Information Security Officer (CISO) of my staff, on 202-208-7485.

U.S. General Services Administration
1800 F Street NW
Washington, DC 20405
www.gsa.gov

APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY

The overall objective for this FISMA evaluation was to conduct an independent evaluation of the information security program and practices of GSA to assess the effectiveness of such programs and practices for the year ending September 30, 2017. The specific objectives of this evaluation were to:

- Perform the annual independent FISMA evaluation of GSA's information security programs and practices;
- Respond to the DHS FY 2017 Inspector General FISMA Reporting Metrics; and
- Follow up on the status of prior-year FISMA findings.

We conducted our independent evaluation in accordance with the CIGIE's Quality Standards for Inspection and Evaluation and applicable AICPA standards. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation, Presidential directives, and the DHS *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0,* dated April 17, 2017. We reviewed GSA's information security program for a program-level perspective and then examined how each of the information systems selected for our testing selection implemented these policies and procedures.

We made a selection of 7 GSA information systems and 5 GSA contractor information systems from a total population of 114 major applications and general support systems (GSS) as of August 3, 2017[4].

To assess the effectiveness of the information security program and practices of GSA, our scope included the following:

- Inquired of information system owners, ISSOs, ISSMs, system administrators and other relevant individuals to walk through each control process.
- An inspection of the information security practices and policies established by the Office of GSA IT.
- An inspection of the information security practices, policies, and procedures in use across GSA.
- An inspection of artifacts to determine the implementation and operating effectiveness of security controls.

We performed our fieldwork at GSA's headquarters offices in Washington, District of Columbia (D.C.) during the period of April 4, 2017 through September 8, 2017. During our evaluation, we met with GSA management to provide a status of the engagement and discuss our preliminary conclusions.

Criteria

We focused our FISMA evaluation approach on federal information security guidance developed by NIST and OMB. NIST Special Publications provide guidelines that are considered essential to the development and implementation of agencies' security programs. The following is a listing of the criteria used in the performance of the FY 2017 FISMA evaluation:

[4] We received an inventory on March 10, 2017 that had 112 GSA information systems. The changes in system inventory between March 2017 and August 2017 was due to new systems and the retirement of systems.

NIST, FIPS and/or Special Publications[5]

- *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*
- *NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model*
- *NIST Special Publication 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems*
- *NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments*
- *NIST Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems*
- *NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- *NIST Special Publication 800-46 Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*
- *NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program*
- *NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations*
- *NIST Special Publication 800-53A Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*
- *NIST Special Publication 800-60 Revision 1, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*
- *NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide*
- *NIST Special Publication 800-63-3, Digital Identity Guidelines*
- *NIST Special Publication 800-70 Revision 3, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*

OMB Policy Directives

- *OMB Circular A-130, Managing Information as a Strategic Resource*
- *M-17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*
- *M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*
- *OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*

United States Department of Homeland Security

- *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics V1.0 April 17, 2017*

[5] Per OMB FISMA reporting instructions, while agencies are required to follow NIST standards and guidance in accordance with OMB policy, there is flexibility within NIST's guidance documents (specifically in the 800 series) in how agencies apply the guidance. However, NIST FIPS are mandatory. Unless specified by additional implementing policy by OMB, guidance documents published by NIST generally allow agencies latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable and compliant with the guidance.

GSA Policy and Procedural Guides

- *IT Security Procedural Guide: Termination and Transfer CIO-IT Security-03-23, Revision 3, April 27, 2017*
- *IT Security Procedural Guide: Access Control CIO-IT Security-01-07, Revision 4, May 8, 2017*
- *IT Security Procedural Guide: Audit and Accountability (AU) CIO-IT Security-01-08, Revision 4, March 23, 2017*
- *IT Security Procedural Guide: Configuration Management (CM) CIO-IT Security-01-05, Revision 3, July 14, 2015*
- *IT Security Procedural Guide: Information Security Program Plan, Revision 1, May 2, 2017*
- *IT Security Procedural Guide: Contingency Planning (CP) CIO-IT Security-06-29, Revision 3, March 9, 2016*
- *IT Security Procedural Guide: Plan of Action and Milestones (POA&M) CIO-IT Security-09-44, Revision 4, February 24, 2017*
- *GSA IT Security Policy CIO 2100.1K, June 30, 2017*
- *IT Security Procedural Guide: Incident Response (IR) CIO-IT Security-01-02, Revision 14, April 3, 2017*
- *IT Security Procedural Guide: Identification and Authentication (IA) CIO-IT Security-01-01, Revision 5, May 5, 2017*
- *IT Security Procedural Guide: Information Security Continuous Monitoring Strategy CIO-IT Security-12-66, Revision 1, May 11, 2017*
- *IT Security Procedural Guide: Managing Enterprise Risk CIO-IT Security-06-30, Revision 10, April 10, 2017*
- *GSA IT Risk Management Strategy, Revision 1, May 12, 2017*
- *GSA Order ADM 2400.1A Insider Threat Program, May 18, 2016*
- *IT Procedural Guide: Federal Information Security Modernization Act [FISMA] Implementation CIO-IT Security-04-26, Revision 1, April 26, 2017*
- *GSA Order CIO P 2181.1 Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing, October 20, 2008*
- *IT Security Procedural Guide: Security Awareness and Role Based Training Program CIO-IT Security-05-29, Revision 5, July 18, 2016*
- *IT Security Procedural Guide: Secure Sockets Layer [SSL]/Transport Layer Security [TLS] Implementation Guide CIO-IT Security-14-69, Revision 2, October 17, 2016*
- *IT Security Procedural Guide: Security Language for IT Acquisition Efforts GSA-IT Security-09-48, Revision 3, February 2, 2017*

APPENDIX II – STATUS OF PRIOR-YEAR FINDINGS

As part of this year's FISMA Evaluation, we followed up on the status of open prior year findings. We inquired of GSA personnel and inspected evidence related to current year test work to determine the status of the findings. If recommendations were determined to be implemented, we closed the findings. If recommendations were determined to be only partially implemented or not implemented at all, we determined the finding to be open.

Prior Year Findings – 2015 Evaluation

Finding #	Prior-Year Condition	Recommendation(s)	Status
1. Configuration Management	While performing our FISMA evaluation procedures we inspected GSA's configuration and vulnerability policy and procedural guides, conducted inquiries with individuals to walk through the process and determined that GSA has a configuration and vulnerability management program; however, we did identify the following exceptions: a. Evidence of review for WebInspect scans could not be provided for the two months selected for three of the five systems selected for testing. b. Evidence of critical and high information system's operating system and database vulnerabilities were not being remediated within 30 days for four of five of the systems selected for testing, but the vulnerabilities are tracked in GSA's scanning tool. c. Evidence of review of vulnerability scans by the TechOps Information System Security Officer (ISSO) could not be provided for four of five of the systems selected for testing.	2. Maintain evidence that ISSOs or other designated individuals review the operating system and database compliance, WebInspect and the vulnerability scan reports.	2. Closed

Finding #	Prior-Year Condition	Recommendation(s)	Status
3. Risk Management Entity-Wide Policy and System Security Plans	While performing our FISMA evaluation procedures we inspected various entity-level policies and procedural guides and system security plans (SSP), conducted inquiries with individuals to walk through the process and determined that GSA has implemented these policies and procedural guides, however we did identify the following exceptions: b. System security plans for four of the five systems tested were based on NIST SP 800-53, Revision 3, but they should have followed Revision 4. c. The Limited Authority to Operate (LATO) for one of five systems expired and the system operated for 23 days until Authority To Operate (ATO) was granted.	3. For all other information systems that do not have system security plans that do not include all relevant controls from NIST SP 800-53, Revision 4 formally document this on respective system's and entity wide plan of action and milestones. 4. Provide periodic training over the review and completion of the GSA Authorization package, to include all documents within the enclosure of the package.	3. Closed 4. Closed

Prior Year Findings – 2016 Evaluation

Finding #	Prior-Year Condition	Recommendation(s)	Status
1. Risk Management - System Security Plans	We determined that the SSP's for 5 of 12 (6 major and 6 minor) GSA information systems were not documented in accordance with NIST Special Publication (SP) 800-53 Revision 4 which was published as final on April 30, 2013.	1. For the 5 information systems review and update the SSP's to include all relevant controls from NIST SP 800-53, Revision 4. 2. For all other information systems that have SSP's that do not include all relevant controls from NIST SP 800-53, Revision 4 formally document this on respective system's and entity wide plan of action and milestones (POA&M).	1. Open 2. Closed
1. Risk Management - Risk Assessments	We determined that 3 of 12 GSA information systems did not perform or have a current risk assessment.	1. Complete the risk assessment for the 3 information systems.	1. Open
1. Risk Management - Interconnection Security Agreement	We determined that the Interconnection Security Agreement (ISA) for 1 of 12 GSA information systems and a third party was not reviewed by the Authorizing Official (AO) and the Chief Information Security Officer (CISO).	1. Review and approve the ISA in accordance with entity policy.	1. Closed
1. Risk Management - Authority to Operate	We determined that the ATO was expired for a total of thirty-one (31) days for 1 of 12 GSA information systems until the ATO extension letter was signed. The gaps of time, within our examination period, between the original ATO package date and the extension letter were January 17, 2016 – February 17, 2016.	1. Provide training over the review and completion of the information system ATO per GSA policy, to include all documents within the enclosure of the package.	1. Closed

Finding #	Prior-Year Condition	Recommendation(s)	Status
1. Risk Management - Plans of Action and Milestones	We determined that the Quarter 1 and 2 POA&Ms were not reviewed in a timely manner for 2 of 12 GSA information systems.	1. Review system POA&Ms in accordance with GSA policy.	1. Closed
1. Risk Management - System Inventory	We determined that 1 of 12 GSA information systems was misclassified as a GSA system and not as a contractor system.	1. Review the system inventory and reevaluate the system classifications based on the definition GSA has created for contractor systems. 2. Reclassify the information system as a contractor system.	1. Open 2. Closed
2. Contractor Systems	We determined that required reviews by the COTR [contracting officer's technical representative], ISSM, and ISSO of the contractor deliverables for 5 of 5 contractor information systems were not provided.	1. Provide periodic training over reviewing and accepting contractor deliverables stated in the CIO-IT Security-09-48, IT Security Procedural Guide: *Security Language for IT Acquisition Efforts*. 2. Document the review of third party reports (SOC [System and Organization Controls Report] 1 and or 2 reports) that are provided by the contractor to include the follow up on any findings that are reported.	1. Open 2. Open
3. Configuration Management – Configuration Management Baseline Scans	We determined that GSA has a configuration management baseline program, however management did not document the review of baseline configuration scans for 2 of 12 GSA information systems. In addition, management did not document or obtain waivers for configuration settings identified in the baseline configuration	1. Provide training or reminders on the GSA policy for documenting and reviewing baseline configuration deviations and scans. 2. Document management's review the baseline configuration scans.	1. Closed 2. Closed 3. Closed

Finding #	Prior-Year Condition	Recommendation(s)	Status
	scans for 4 of 12 GSA information systems.	3. Document the deviations with management approval, as required by GSA policy.	
3. Configuration Management - Change/Patch Management Approval	We determined that management did not document the authorization for a selection patches for the operating system (OS) supporting 1 of 12 GSA information systems.	1. Document evidence of authorization of operating system patches.	1.Open
3. Configuration Management - System Monitoring	We determined that monitoring over the operating system layer of 1 of 12 GSA information systems was not being performed in accordance with GSA policy from October 1, 2015 to May 31, 2016.	1. Monitor, authorize, and review the operating system configuration, new and separated users, and separation duties.	1.Closed
4. Identity and Access Management - Account Management	We identified the following exceptions: a. User accounts were not deactivated after 90 days of inactivity for 2 of 12 GSA information systems. b. Evidence of authorization could not be provided for a 1 of 12 GSA information system's operating system administrator's account. c. Terminated application user maintained access to the system past the allotted 30 days from separation for 1 of 12 GSA information systems.	1. Provide training around entity policies for authorizing, granting, and terminating access to information systems. 2. Maintain authorizations for granting access to individuals for privileged access. 3. Remove terminated users from systems within the required timeframes. 4. Review last logon dates on a defined basis and lock accounts that exceed the 90 days of inactivity.	1.Closed 2.Open 3.Open 4.Closed

Finding #	Prior-Year Condition	Recommendation(s)	Status
4. Identity and Access Management - Audit Log Monitoring	We determined that audit logs are being reviewed on an ad-hoc basis for 3 of 12 GSA information systems.	1. Provide training or reminders on the GSA policy for documenting the weekly review of audit logs. 2. Document and maintain evidence of review for audit logs.	1. Closed 2. Closed
4. Identity and Access Management - Passwords	We identified the following exceptions: a. Session lock was not configured appropriately for 4 of 12 GSA information systems. b. Session termination was not configured appropriately for 4 of 12 GSA information systems. c. Maximum password age was not configured appropriately for 1 of 12 d. Maximum password age could not be provided for 1 of 12 GSA information systems. e. Password complexity was not configured appropriately for 1 of 12 GSA information systems.	1. Configure all user accounts in accordance with GSA policy password configuration requirements.	1. Closed
4. Identity and Access Management - Warning Banners	We determined that 5 of 12 GSA information systems did not contain the appropriate warning banner.	1. Configure and update the warning banners to conform to GSA requirements.	1. Closed
5. Contingency Planning - Contingency Planning Testing and Business Impact Analysis	We identified the following exceptions: • BIA (Business Impact Analysis) was not incorporated in the contingency plans for 3 of 12 GSA information systems. • The contingency plan for 1 of 12 GSA information system had not been tested during the fiscal year; and	1. Complete the BIA and update the contingency plans. 2. Schedule and perform an annual test of the contingency plan to determine if it is effective and incorporates lessons learned from the test.	1. Open 2. Open

Finding #	Prior-Year Condition	Recommendation(s)	Status
	• Backups for 2 of 12 GSA information systems were not configured and performed.		
5. Contingency Planning - System Backups	We identified that backups were not configured or performed for 2 of 12 GSA information systems.	1. Configure the new tool, Catalogic Software Management, to back up information systems on a frequency consistent with GSA policy.	1. Closed

APPENDIX III – GLOSSARY

ACRONYM	DEFINITION
AC	Access Control
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Officials
ATO	Authority to Operate
AU	Audit and Accountability
BIA	Business Impact Analysis
BYOD	Bring Your Own Device
CCB	Configuration Control Board
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CO	Contracting Officer
COR	Contracting Officer's Representative
COTR	Contracting Officer's Technical Representative
CP	Contingency Planning
CSIP	Cybersecurity Strategy and Implementation Plan
D.C.	District of Columbia
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
GAGAS	Generally Accepted Government Auditing Standards
GFS	Grandfather-father-son
GSA	U.S. General Services Administration
GSS	General Support Systems
HSPD	Homeland Security Presidential Directive
IA	Identity and Access Management
IG	Inspector General
IO	IO is now part of Office of Deputy CIO (ID), specifically Office of Enterprise Infrastructure Operations (IDI)
IR	Incident Response
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
KPMG	KPMG LLP

ACRONYM	DEFINITION
LATO	Limited Authority to Operate
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OS	Operating System
POA&M	Plan of Action and Milestones
RM	Risk Management
SOC	System and Organization Controls
SP	Special Publication
SSL	Secure Sockets Layer
SSP	System Security Plan
ST	Security Training
TLS	Transport Layer Security