U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

FEB 1 9 2017

MEMORANDUM FOR: TIMOTHY O. HORNE
ACTING ADMINISTRATOR (A)

FROM: CAROL F. OCHOA
INSPECTOR GENERAL (J)

SUBJECT: Transmittal of the Fiscal Year 2016 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 of GSA's compliance with the *Federal Information Security Modernization Act of 2014* (FISMA) for fiscal year 2016.

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. GSA contracted with KPMG, an independent public accounting firm, to assess its information security program in accordance with FISMA. The contract required that the evaluation be performed 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 dated December 16, 2016, 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 attached in its entirety.

The fiscal year 2017 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) 501-0374.

Attachments

**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 5306
Washington, DC 20405

February 1, 2017

Dear Ms. Presley-Doss,

We have submitted the following Federal Information Security Modernization Act (FISMA) reports for the General Services (GSA) Office of Inspector General (OIG) dated December 16, 2016:

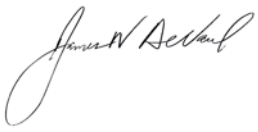
- *Fiscal Year 2016 Independent Evaluation of the U.S. General Services Administration's Compliance with the Federal Information Security Modernization Act of 2014 Report; and*
- *Fiscal Year 2016 U.S. General Services Administration's Federal Information Security Modernization Act of 2014 Management Systems Report.*

These reports were provided to you in this format pursuant to your written request as set forth in our Contract GS-23F-8127H, Order Number GSH1416AA0136, dated April 22, 2016 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 2016 FISMA Reports 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
Partner, Federal Advisory Services

# Fiscal Year 2016 Independent Evaluation of the U.S. General Services Administration's Compliance with the Federal Information Security Modernization Act of 2014 Report

December 16, 2016

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


BACKGROUND ..... 3
Federal Information Security Modernization Act ..... 3
OVERALL EVALUATION RESULTS ..... 4
FINDINGS ..... 5
1. Risk Management ..... 5
2. Contractor Systems ..... 10
3. Configuration Management ..... 11
4. Identity and Access Management ..... 17
5. Contingency Planning ..... 23
MANAGEMENT RESPONSE TO THE REPORT ..... 26


## Appendices


APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY ..... 28
APPENDIX II – STATUS OF PRIOR YEAR FINDINGS ..... 32
APPENDIX III – GLOSSARY ..... 37

**KPMG LLP**
1676 International Drive
McLean, VA 22102

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

**Re: Fiscal Year 2016 Independent Evaluation of the U.S. General Services Administration's Compliance with the Federal Information Security Modernization Act of 2014**

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 the GSA, to have an annual independent evaluation 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). 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 the Council of the Inspectors General on Integrity and Efficiency's 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 the GSA's information security program and practices for the period October 1, 2015 to September 30, 2016 for its information systems, including the 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 six selected GSA information systems, which included six minor applications and five GSA contractor information systems. Additional details regarding the scope of our independent evaluation are included in Appendix I, *Objective, Scope & Methodology*.

GSA's information security program and practices for its information systems have been established based on the applicable FISMA requirements, OMB policy and guidelines, and the National Institute of Standards and Technology (NIST) standards and guidelines. GSA is maintaining a security program for the eight FISMA metric domains.[1] However, while the security program has been implemented across GSA, we identified the following five of eight FISMA program areas that had 16 deficiencies:

1. Risk Management
2. Contractor Systems
3. Configuration Management

[1] The eight FISMA metric domains are risk management, contractor systems, configuration management, identity and access management, security and privacy training, information security continuous monitoring, incident response, and contingency planning.

4. Identity and access management
5. Contingency planning

We have made 26 recommendations related to these control deficiencies that, if effectively addressed by management, should strengthen the respective information systems and the GSA's information security program. In a written response, the GSA Chief Information Officer (CIO) agreed with our findings and recommendations (see *Management Response*).

This independent evaluation did not constitute an engagement in accordance with *Government Auditing Standards.* KPMG did not render an opinion on the 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 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.

Appendix I describes the FISMA evaluation's objective, scope, and methodology. Appendix II, *Status of Prior-Year Findings*, summarizes the GSA's progress in addressing prior-year recommendations. Appendix III contains a glossary of terms used in this report.

Sincerely,

KPMG LLP

December 16, 2016

## 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 the 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 the DHS in memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*, for the operational aspects of Federal cyber security, 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.

## OVERALL EVALUATION RESULTS

GSA's information security program and practices for its information systems have been established based on the applicable FISMA requirements, OMB policy and guidelines, and the NIST standards and guidelines. GSA is maintaining a security program for the five Cybersecurity Framework Security Functions which include eight FISMA metric domains. This outlined in the Fiscal Year (*FY) 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics v1.1.3, September 26, 2016* that were prepared by the DHS's Office of Cybersecurity and Communications Federal Network Resilience. The program areas are:

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

However, while the security program has been implemented across the GSA, we identified 16 deficiencies that we reported to GSA management in five of eight FISMA metric domains. We have made 26 recommendations related to these deficiencies that, if effectively addressed by management, should strengthen the respective information systems and the GSA's information security program. Based on the CyberScope scoring methodology for the FY 2016 evaluation period, four Cybersecurity Framework Functions: Identify, Protect, Detect, and Recover were rated not effective and Respond was rated as effective.[2]

The *Findings* section of this report presents the detailed findings and associated recommendations. In a written response to this report, the GSA CIO agreed with our findings and recommendations and provided corrective action plans (see *Management Response*). GSA's planned corrective actions are responsive to the intent of our recommendations.

Additionally, we evaluated the prior-year findings from the FY 2014 and 2015 FISMA Evaluations and noted that management had closed four of six findings and the remaining two are partially closed. See Appendix II, *Status of Prior-Year Findings*, for additional details.

[2] The scoring methodology is described in the *Fiscal Year 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics v1.1.3, September 26, 2016* and is determined by the entries in CyberScope.

## FINDINGS

### 1. Risk Management

#### System Security Plans

While performing our FISMA evaluation procedures we inspected GSA's policies and procedural guides for system security plans (SSP), we conducted inquiries with individuals to walk through the process and inspected documentation and determined that GSA has a SSP process, however we did determine that three of six systems and two of six minor applications SSP's were not documented in accordance with NIST Special Publication (SP) 800-53 Revision 4, which was published as final on April 30, 2013.

Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, page V, states:

> "**8. Implementations.**
> This standard specifies minimum security requirements for federal information and information systems in seventeen security-related areas. Federal agencies must meet the minimum security requirements as defined herein through the use of the security controls in accordance with NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, as amended.
>
> **9. Effective Date.**
>
> This standard is effective immediately. Federal agencies must be in compliance with this standard not later than one year from its effective date."

GSA Information Technology (IT) Security Policy, CIO 2100.1J, April 28, 2016, section 10. IT security controls on page 5, states:

> "All IT systems, including those operated by a contractor on behalf of the Government, must implement proper security controls according to the security categorization level in accordance with FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, the current version of NIST SP 800-53 R4, Security and Privacy Controls for Federal Information Systems and Organizations."

The GSA Chief Information Security Officer (CISO) informed us that due to cost and labor concerns, his office issued guidance which allowed system owners to update their SSP to be in accordance with NIST SP 800-53, Revision 4, during their next Authority to Operate (ATO) cycle or during the annual review, whichever comes first.

The untimely compliance with NIST SP 800-53, Revision 4, increases the security risk to the confidentiality, integrity and availability of data as Revision 4 updates the minimum baseline controls and enhancements for information systems.

We recommend that GSA perform the following actions:

1. For five information systems review and update the system security plans 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).

**Risk Assessments**

While performing our FISMA evaluation procedures we inspected GSA's risk assessment process policies and procedural guides, conducted inquiries with individuals to walk through the process and determined that the one of the six information systems and two of the six minor applications did not perform or have a current risk assessment.

GSA IT *Information Security Program Plan*, Version 1.0, May 1, 2015, section 3.4.1 Certification, Authorization, Security Assessment Policies and Procedures ([Security Assessment and Authorization] CA-1) on page 28, states:

> "Common Control Implementation:
>
> Security Assessment and Authorization Policy is included in CIO P 2100.1 - GSA IT Security Policy, Chapter 3. Policy on Management Controls. It states, "All GSA information systems must be assessed and authorized at least every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems"

GSA management stated that a comprehensive risk assessment has not been performed during the FY due to staffing issues and an oversight of entity policy.

Not having a fully comprehensive and documented risk assessment increases the risk of a threat or vulnerability to the data residing on the information system and diminishes the ability of GSA management to understand where to focus its efforts on maintaining a security plan.

We recommend that GSA perform the following action:

1. Complete the risk assessment for three information systems.

**Interconnection Security Agreement**

While performing our FISMA evaluation procedures we inspected GSA's system interconnection agreement process policies and procedural guides, conducted inquiries with individuals to walk through the process and determined that the Interconnection Security Agreement (ISA) for one of the six information systems was not reviewed by the Authorizing Official (AO) and the CISO.

GSA IT Security Policy, CIO 2100.1J, April 28, 2016, section h. System interconnections/information sharing on page 32, states:

> "(1) Written management authorization for system interconnection, based upon the acceptance of risk to the IT system, must be obtained from the AOs of both systems

> prior to connecting a system not under a single AO's control In Accordance With (IAW) NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems. Per NIST SP 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as Integrated Services Digital Network (ISDN), T1, T3, DS3, Virtual Private Network (VPN), etc.
>
> (2) If GSA systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system.
>
> (3) All interconnections between GSA and external entities including off-site contractors or Federal agency/departments must be approved by the AO and concurred by the GSA CISO, and reviewed on an annual basis, at a minimum."

GSA management was not aware the GSA IT Security Policy, CIO 2100.1J, April 28, 2016, required ISAs between GSA and external entities to be approved by the AO and concurred by the GSA CISO.

Failure to have the AO and GSA CISO approve, concur, and review ISAs between external entities, prevents GSA management and individuals responsible for information security to make sound decisions on whether the information system is complying with GSA security requirements and understanding the current risk associated with the information system.

We recommend that GSA perform the following action:

1. Review and approve the ISA in accordance with entity policy.

**Authority to Operate**

While performing our FISMA evaluation procedures we inspected GSA's security authorization process policies and procedural guides, conducted inquiries with individuals to walk through the process and determined one of the six information systems ATO was expired for a total of thirty-one (31) days 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.

GSA IT Security Policy, CIO 2100.1J, April 28, 2016, section 7, Authorizing Official (AO) on pages 11-12, states:

> "c. Information systems with an expiring ATO may perform a one-time extension of the current authorization for a period not to exceed one year (365 days) from the date of ATO expiry to allow development of near real-time continuous monitoring capabilities to support ongoing authorization.
> […]
> g. Ensure that new GSA information systems pursuing an agile development methodology and residing on infrastructures that have a GSA ATO concurred by the Office of the Chief Information Security Officer (OCISO) or a Federal Risk and Authorization Management Program (FedRAMP) ATO may request a limited ATO for the pilot period of the project not to exceed one year (365 days). The

> limited ATO will be based on a lightweight security assessment and authorization (A&A) process; however, the period of the limited ATO should be used to conduct a full A&A resulting in a new three-year ATO."

The information system is currently in a transitional period, which will allow for the consolidation of multiple similar components under the same scope. Due to the transition period, GSA management extended the ATO by one (1) year.

Without authorizations for system use, system owners and management may not be aware of the security risks posed by the use of their systems. As a result, there is the potential risk that systems are operating in a production environment without appropriate controls or management's understanding of the system risks. This could further lead to a compromise of the confidentiality, integrity, and availability of the data residing on the information system.

We recommend that GSA perform the following action:

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.

**Plans of Action and Milestones**

While performing our FISMA evaluation procedures we inspected GSA's POA&M process policies and procedural guides, conducted inquiries with individuals to walk through the process and determined the Quarter 1 and 2 POA&Ms were not reviewed in a timely manner for two of the six minor applications.

CIO-IT Security-09-44, IT Security Procedural Guide: *Plan of Action and Milestones (POA&M)*, Revision 3, June 29, 2016, section 7.1, POA&M Review and Report (Information System Security Officer (ISSO)) on page 15, states:

> "Policy and Compliance Division (ISP) will review POA&M submissions upon initial A&A of a GSA system (i.e., when an ATO Letter is received) and quarterly thereafter. ISP will provide comments in a POA&M Review Report which will be posted on the POA&M Management Site under the applicable system name and the current quarter/quarter for which the POA&M workbook was submitted. The ISSO/submitter will be notified when this occurs. Comments must be mitigated and/or addressed within 2 weeks of the report date."

Due to an oversight by GSA management, the Quarter 1 and Quarter 2 POA&Ms were not uploaded to the shared site for review by ISP.

Lack of review of POA&Ms increase the risk that GSA management does not identify IT security weaknesses that could compromise the confidentiality, integrity, and availability of data within the information system.

We recommend that GSA perform the following action:

1. Review system POA&Ms in accordance with GSA policy.

**System Inventory**

While performing our FISMA evaluation procedures we inspected GSA's system inventory policy and procedural guides, conducted inquiries with individuals to walk through the process and determined that one of the six information systems was misclassified as a GSA system and not as a contractor system.

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* on 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 did not follow their guidance on how they classify a contractor information system. GSA also stated they are waiting on clear guidance from OMB and DHS on a clear definition of contractor information systems.

Failure to properly classify systems might prevent them from the proper oversight and monitoring of the contractor systems being used by GSA to process data and prevent systems that should be GSA from having the appropriate security controls implemented.

We recommend that GSA perform the following actions:

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.

**2. Contractor Systems**

While performing our FISMA evaluation procedures we inspected GSA's contractor monitoring policies and procedural guides, conducted inquiries with individuals to walk through the process and determined that GSA has a contractor monitoring program and requires frequent document submissions and reviews to be performed, however we did identify that for five of the five contractor systems these deliverables were not always provided and/or GSA did not provide review or acceptance of these deliverables.

We also determined the contract for one of the five contractor information systems did not contain the required security and privacy requirements by the Federal Acquisition Regulation (FAR).

The CIO-IT Security-09-48, GSA IT Security Procedural Guide: *Security Language for IT Acquisition Efforts*, section 1.4, Reporting and Continuous Monitoring on page 10, 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 per the schedules below. 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 to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur."

Contracting Officer's Technical Representative (COTR), ISSO, and/or Information System Security Manager (ISSM) were not aware of the GSA IT Security Procedural Guide that required the review and acceptance of the deliverables.

GSA management informed us that management for one contractor information system was currently in contract negotiations and requested the documentation per the permission of the contracting officer.

Failure to have the contractor provide the required information as required by GSA's policy, prevents GSA AO and individuals responsible for information security to make sound decisions on whether the information system is complying with GSA security requirements and understanding the current risk associated with the information system.

We recommend that GSA perform the following actions:

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 (Service Organization Control [SOC] 1 and or 2 reports) that are provided by the contractor to include the follow up on any findings that are reported.

## 3. Configuration Management

### Configuration Management Baseline Scans

While performing our FISMA evaluation procedures we inspected GSA's configuration management baseline policies and procedural guides, conducted inquiries with individuals to walk through the process and determined that GSA has a configuration management baseline program, however we did identify that management did not document the review of baseline configuration scans for two of the six minor applications. In addition, management did not document or obtain waivers for configuration settings identified in the baseline configuration scans for two of the six information systems and two of the five minor applications.

Inspected the CIO-IT Security-01-05, GSA IT Security Procedural Guide: *Configuration Management (CM)*, Revision 3, July 14, 2015, and determined it documented the following in section 2.4.5 Step 5: Continuous Monitoring on page 10, states:

> "Increasingly, vendors are proactive in developing and releasing to the public fixes (or antidotes) to known vulnerabilities, and agencies must remain vigilant to ensure that they capture all relevant fixes as they are released, test their implementation for adverse effects, and implement them if deemed appropriate after testing is concluded."

GSA IT *Information Security Program Plan*, Version 1.0, May 1, 2015, section 3.5.2, Configuration Settings (CM-6) on page 33, states:

> "(c) GSA information systems, including vendor owned / operated systems are responsible for identifying and documenting any deviations from the configuration baselines utilized for system hardening. Any deviations should be documented in the system security plan and approved by the Authorizing Official."

Management informed us that a process has not been created yet for obtaining approved waivers for non-compliance items from security configuration scans. Management also was not aware of the requirements to review the security compliance scans or document deviations from the security compliance scans. One information system's environment is currently in a transitional period, which will allow for the consolidation of multiple similar components under the same scope. Due to the transitional period, these documents were unable to be provided.

Lack of documentation for management's review of baseline configuration scans and approved waivers increases the risk that system could be exposed to configuration weaknesses or vulnerabilities that could compromise the operational integrity of the system.

We recommend that GSA perform the following actions:

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.

3. Document the deviations with management approval, as required by GSA policy.

**Change/Patch Management Approval**

While performing our FISMA evaluation procedures we inspected GSA's change/patch (configuration) management policies and procedural guides, conducted inquiries with individuals to walk through the process and determined that GSA has a change/patch (configuration) management program, however we did identify that management did not document authorization for a selection of patches for the operating system (OS) supporting the one of the six information systems.

Inspected the CIO-IT Security-01-05, GSA IT Security Procedural Guide: *Configuration Management (CM),* Revision 3, July 14, 2015, and determined it documented the following in section 4.3, CM-3 Configuration Change Control on page 20, states:

> "Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. This control focuses on defining the configuration management process, controlling the information system configuration according to that process, and ensuring that no configuration changes are made without going through the approved configuration management process. Below are some general guidelines for implementing proper configuration control:
>
> - 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:
>   - Changes to the information system, including upgrades, modifications.
>   - Changes to the configuration settings for information technology product (e.g., operating systems, firewalls, routers).
>   - Emergency changes.
>   - Changes to remediate flaws.
> - Authorize, document, and control changes to the information system. Include emergency changes in the configuration change control process.
> - Conduct a security impact analysis to determine the ramifications of the proposed change. Consider changes only after analyzing the results of the security impact analysis.
> - Use the GSA change control forms (see Appendices) to document the proposed change, to submit the proposal to the CCB and to follow from initiation through approval or disapproval.
> - Documents all approved configuration-controlled changes in appropriate documentation. The current state of the system should be the 'as-built' configuration as reflected in the initial baseline with approved changes.
> - Audit activities associated with configuration changes to the information system. Review the approved configuration management process for key auditable activities and then review records of selected activities in the process; for example.
>   - Who approved the change request;
>   - Who implemented the change;
>   - Who completed the security impact assessment;
>   - Who tested the change; and
>   - How it was tested.

- Ensure that any testing performed does not adversely impact the information system (perform the test on a test platform, not a production platform)."

The one information system's environment is currently in a transitional period, which will allow for the consolidation of multiple similar components under the same scope. Due to the transitional period, these documents were unable to be provided.

Lack of documented review and approval for OS patches increases the risk that information system could be exposed to vulnerability weaknesses that could compromise the operational integrity of the system. This could further lead to a compromise of the confidentiality, integrity, and availability of the data residing on the information system.

We recommend that GSA perform the following action:

1. Document evidence of authorization of operating system patches.

**System Monitoring**

While performing our FISMA evaluation procedures we determined that monitoring over the operating system layer of the one of the six information systems, which included two minor applications was not being performed in accordance with GSA policy from October 1, 2015 to May 31, 2016.

IT Security Procedural Guide: *Configuration Management*, CIO-IT Security-01-05, Revision 3 on page 19, section CM-2, Baseline Configuration, states:

"The following bullets present implementation guidance for documenting the systems baseline:

- Determine the system's configuration based on GSA standards (e.g., baseline configuration, system image, standard build configuration). Reference the GSA Enterprise Architecture Committee (EARC) Approved IT Standards at http://ea.gsa.gov/index_bricks.html. The site identifies products or technical standards approved for current production deployment. The standards are consistent with GSA's enterprise architecture.
- Develop a system baseline configuration that is consistent with GSA's enterprise architecture. Include how the information system is linked to the GSA mission.
- Identify where the system falls within the enterprise architecture and describe its purpose, and its mission.
- Identify the components of the information system to be placed under configuration control. These components are called Configuration Items (CI). The CI inventory should include the following items:
  - Management documentation describing the processes used to develop (or manage the development of) the system, such as the Needs Statement and the Project.
  - Technical documentation or baselines describing the system (e.g., Functional Requirements Document).
  - A list of hardware and software components, including any code that was developed.
  - Data and database components (files and records that exist apart from software, which access the contents of a database).
  - Hard copies of documentation and commercial off-the-shelf (COTS) software.
  - The component's logical placement in the information system architecture.

- The specification to which the system is built.
- A system architecture drawing.

Maintaining the baseline configuration involves creating new baselines as the information system changes over time. When deviations are ultimately included in a new version of the baseline, they are no longer considered deviations, and compliance with the control is maintained. Deviations are differences between the current baseline configuration and the current operational configuration. The baseline configuration of the information system must be consistent with GSA's overall enterprise architecture."

*Information Security Program Plan*, Version 1.0, section 3.5.2, Configuration Settings (CM-6) on page 33, states:

"(c) GSA information systems, including vendor owned / operated systems are responsible for identifying and documenting any deviations from the configuration baselines utilized for system hardening. Any deviations should be documented in the system security plan and approved by the Authorizing Official."

IT Security Procedural Guide: *Access Control*, CIO-IT Security-01-07, Revision 3 on page 7, section 4.1, states:

"The general activities for authorizing personnel to access IT resources are:

- Categorize positions, roles, and responsibilities for GSA employees and for contractors.
- Screen personnel utilizing the GSA background investigations process.
- Obtain Authorization for requested access rights. Determine whether to grant access rights and which access rights should be granted based on the job function of the requestor, privacy concerns (AR-7) and a signed authorization request.
- Provide the GSA and any system specific Rules of Behavior. Receive the required acknowledgement(s) from the requestor.
- Manage access rights by establishing authorized access, documenting, monitoring, and removing access rights in a timely manner, including periodically recertifying the need for the approved access.
- Document the processes.
- Retain documentation according to GSA documentation retention policies."

GSA IT Security Policy, CIO 2100.1J, April 28, 2016, section t. Separation of Duties on pages 47-48, states:

"(2) Define and implement detailed separation of duties policies for IT systems based on the specific processes, roles, permissions, and responsibilities of personnel involved in departmental business operations.
[…]
(4) Document job descriptions and roles to accurately reflect the assigned duties, responsibilities, and separation of duties principles. By clearly documenting position responsibilities and functions, employees are positioned to better execute their duties [in accordance with] (IAW) policy.
[…]
(8) Information systems must enforce separation of duties through assigned access authorizations."

Section 8b on page 62, states:

"(b) Role conflicts. Any accesses or permissions that clearly violate established separation of duties policies must be coordinated with the designated Services, Staff Offices, or Regions (S/SO/R) ISSO to correct or resolve conflicting role assignments."

IT Security Procedural Guide: *Termination and Transfer*, CIO-IT Security-03-23, Revision 2, section 3.3 Supervisor Responsibilities on page 7, states:

"The supervisor must:

1) Notify the appropriate ISSM of the resources or accounts (to include communications) used as soon as the termination is known. The notification must list all resources and indicate requested actions, such as deny access to the resource then delete resources after 30 days.
[…]
2) Notify personnel responsible for any physical access to facilities to deny access.
[…]
4) Obtain sign-off by the designated ISSM and ISSO(s) that access privileges have been denied.
5) Follow up with the designated ISSM and ISSO(s), usually after 30 days, to verify that files and other data have been deleted."

Section 3.4 Best Practices for Supervisors, on page 10, states:

"5e) Establish a date for the automatic deletion of files held in user-specific directories/folders; this applies to not only GSA employees but also contractors, contractor facilities and other organizations using IT resources on behalf of GSA. […]Allow one day to lock the user out of the resource and 30 days to clear and remove data from the accounts. Supervisors will use the 30 days to decide what to do with the information, whether to retain it by moving it to another account or to delete it. At the end of 30 days, the account will be deleted and all remaining data associated with the account will be purged."

GSA IT Security Policy, CIO 2100.1J, April 28, 2016, Chapter 5 on page 58, states:

"(1) All internal GSA IT systems must display an approved warning banner to all users attempting to access GSA's computer systems. The warning banner must read as follows:

**********WARNING**********
This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

(2) For publicly accessible sites (i.e., open to the Internet) the sentence, "Therefore, no expectation of privacy is to be assumed" shall be removed. Detailed guidance regarding access controls is available in GSA-CIO-IT-Security-01-07: Access Control."

Due to the re-organization of the GSA IT Security team, monitoring over the operating system layer of for the information system was not being performed from October 1, 2015 to May 31, 2016. However, we were informed that monitoring of the operating system of this information system began being performed as of June 1, 2016, but no additional testing procedures were performed to determine the monitoring of risks was occurring.

Without proper monitoring of security controls at all levels supporting a system, potential security risks could be present that could lead to a compromise of the confidentiality, integrity, and availability of the data residing on the information system.

We recommend that GSA perform the following action:

1. Monitor, authorize, and review the operating system configuration, new and separated users, and separation duties.

## 4. Identity and Access Management

### Account Management

While performing our FISMA evaluation procedures we inspected GSA's account management policies and procedural guides and conducted inquiries with individuals to walk through the account management program. We identified the following exceptions:

a. User accounts were not deactivated after 90 days of inactivity for the two of the six information systems.
b. Evidence of authorization could not be provided for a privileged user of one of the six information systems.
c. Terminated application user maintained access to the system past the allotted 30 days from separation for one of the six minor applications.

GSA IT Security Policy, CIO 2100.1J, April 28, 2016, section a. Identification and Authentication on page 56, states:

> "FIPS 199 Moderate and High impact systems shall automatically disable inactive accounts after ninety (90) days."

The CIO-IT Security-01-07, IT Security Procedural Guide: *Access Control*, Revision 3, April 1, 2015, section 4.1, Personnel Authorization Best Practices on page 7, states:

> "The general activities for authorizing personnel to access IT resources are:
> - Categorize positions, roles, and responsibilities for GSA employees and for contractors.
> - Screen personnel utilizing the GSA background investigations process.
> - Obtain Authorization for requested access rights. Determine whether to grant access rights and which access rights should be granted based on the job function of the requestor, privacy concerns (AR-7) and a signed authorization request.
> - Provide the GSA and any system specific Rules of Behavior. Receive the required acknowledgement(s) from the requestor.
> - Manage access rights by establishing authorized access, documenting, monitoring, and removing access rights in a timely manner, including periodically recertifying the need for the approved access.
> - Document the processes.
> - Retain documentation according to GSA documentation retention policies."

The CIO-IT Security-03-23, IT Security Procedural Guide: *Termination and Transfer*, Revision 2, January 29, 2008, section Supervisor Responsibilities on page 7, states:

> "The supervisor must:
> 1) Notify the appropriate ISSM of the resources or accounts (to include communications) used as soon as the termination is known. The notification must list all resources and indicate requested actions, such as deny access to the resource then delete resources after 30 days.
> […]
> 2) Notify personnel responsible for any physical access to facilities to deny access.
> […]

4) Obtain sign-off by the designated ISSM and ISSO(s) that access privileges have been denied.
5) Follow up with the designated ISSM and ISSO(s), usually after 30 days, to verify that files and other data have been deleted."

GSA management stated that the two information systems cannot be configured to deactivate user accounts when users have not accessed their account after 90 days of inactivity.

GSA management stated that due to an oversight, the access form for one privileged user could not be located. The user was a transfer and completed the required entity trainings, but the access form could not be located.

Due to a lack of oversight, GSA management did not remove the terminated users account within a timely manner.

Without proper control of authorized and terminated access, 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 actions:

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.

**Audit Log Monitoring**

While performing our FISMA evaluation procedures we inspected GSA's audit log monitoring policies and procedural guides and conducted inquiries with individuals to walk through the audit log monitoring program. However we did identify that audit logs are being reviewed on an ad-hoc basis for two of the six information systems and one of the six minor applications.

The CIO-IT Security-01-08, GSA IT Procedural Guide: *Audit and Accountability (AU)*, Revision 4, section 3.6, AU-6 Audit Review, Analysis, and Reporting on page 11, states:

> "Aggregated and correlated logs and events within the enterprise Security Information and Event Management (SIEM) tool are reviewed by GSA OCISO ISO division for indications of compromise on business days. As necessary, this analysis also supports investigations and response to suspicious activities, enhancement AU-6 (2), conducted by the GSA Incident Response Team, IAW the IT Security Procedural Guide: Incident Response (IR) CIO-IT Security-01-02.
>
> For enhancement AU-6 (1), for internal systems, through a combination of auditable events from a variety of devices around the agency, GSA's Enterprise SIEM tool uses correlation rules to detect and respond to indicators of compromise.
>
> For enhancement AU-6 (3), the enterprise SIEM tool correlates audit records across different security components and logging sources to gain organization-wide situational awareness.
>
> For enhancement AU-6 (5) and (6), as requested the GSA OCISO ISO division will coordinate with the GSA Incident Response Team to integrate analysis from other sources while suspicious activities are investigated.
> […]
> The system owner maintains the responsibility of reviewing information system logs on their systems for unusual activity on a weekly basis, and should keep a log that such a review has taken place."

GSA management stated that one information system and minor application audit logs are being reviewed on an ad hoc basis, but due to an oversight of GSA policy, audit logs were not reviewed in a timely manner.

One information system's environment is currently in a transitional period, which will allow for the consolidation of multiple similar components under the same scope. Due to the transitional period, these documents were unable to be provided.

Failure to perform reviews of the audit log could allow unusual activity to go unnoticed or undetected without proper intervention.

We recommend that GSA perform the following actions:

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.

**Passwords**

While performing our FISMA evaluation procedures we inspected GSA's password policies and procedural guides and conducted inquiries with individuals to walk through their password configuration settings, however we did identify the following exceptions:

a. Session lock was not configured appropriately for two of the six information systems and two of the six minor applications.
b. Session termination was not configured appropriately for two of the six information systems and two of the six minor applications.
c. Maximum password age was not configured appropriately for the one minor application's database.
d. Maximum password age could not be provided for the one of the six information systems.
e. Password complexity was not configured appropriately for the one of the six information systems.

GSA IT Security Policy, CIO 2100.1J, April 28, 2016, Chapter 5: Policy on Technical Controls on page 54-56, states:

> "(1) Authentication schemes for Moderate and High Impact systems must utilize multifactor authentication using two or more types of identity credentials (e.g. passwords, Security Assertion Markup Language (SAML) 2.0 biometrics, tokens, smart cards, one time passwords) as approved by the Authorizing Official and in accordance with the security requirements in the subparagraphs of this paragraph.
>
> (2) An authentication scheme using passwords as a credential must implement the following security requirements
>
> (a) Passwords must contain a minimum of eight (8) characters which include a combination of letters, numbers, and special characters. Accounts used to access United States Government Configuration Baseline (USGCB) compliant workstations must contain a minimum of sixteen (16) characters but do not have to contain a combination of letters, numbers, and special characters.
>
> (b) Information systems must be designed to require passwords to be changed every 90 days.
>
> (c) Information systems must automatically lockout users after not more than ten (10) failed access attempts during a 30 minute time period. Accounts must remain locked for a minimum of 30 minutes for the next login prompt.
>
> (d) Passwords for all mobile devices such as GSA approved smart phones, iPads, and tablets must be a minimum of 6 characters. The six character password requirement also applies to personal mobile devices accessing GSA data or systems.
>
> (e) Passwords must not be stored in forms (i.e. Windows dialog boxes, web forms, etc.).
>
> (f) All default passwords on network devices, databases, operating systems, must be changed.

> (g) Other than default or one time use passwords, passwords must never be sent via e-mail, regular mail, or interoffice mail.
>
> (h) User IDs and passwords must never be distributed together (i.e. same e-mail, regular mail, interoffice mail, etc.).
>
> (i) Users must be authenticated before resetting or distributing a password.
>
> (4) Systems with an authentication assurance level of 2 or above, used by federal employees or contractors must accept federal Personal Identity Verification (PIV) cards and verify them in accordance with guidance in OMB M-11-33.
>
> (5) All users issued Government Furnished Equipment are required to log into the workstation using a GSA issued PIV credential.
> […]
> (13) All GSA workstation and mobile devices shall initiate a session lock after 15 minutes of inactivity. The session lock shall remain in effect until the user reestablishes access using appropriate identification and authentication.
> […]
> (16) FIPS 199 Moderate and High impact systems shall automatically terminate a remote access connection and Internet accessible application session after thirty (30) minutes of inactivity. The time will be thirty (30) – sixty (60) minutes for non-interactive users. Static web sites, long running batch jobs and other operations are not subject to this time limit."

GSA management stated that due to an oversight of the GSA IT Security Policy, CIO 2100.1J, April 28, 2016, the information systems were configured inappropriately for maximum password age, password complexity, session lock, and session termination.

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

We recommend that GSA perform the following action:

1. Configure all user accounts in accordance with GSA policy password configuration requirements.

**Warning Banners**

While performing our FISMA evaluation procedures we inspected GSA's warning banner policy, and determined three of the six information systems and two of the six minor applications did not contain the appropriate warning banner.

GSA IT Security Policy, CIO 2100.1J, April 28, 2016, Chapter 6 on page 58, states:

> "d. (1) All internal GSA IT systems must display an approved warning banner to all users attempting to access GSA's computer systems. The warning banner must read as follows:

> **********WARNING**********
> This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution."

GSA management stated that due to an oversight of the GSA IT Security Policy, CIO 2100.1J, April 28, 2016, the warning banner for five information systems did not contain the appropriate wording.

Without appropriate disclosure advising all users of the proper use and consequences of misuse of information resources, GSA may be placing itself in a position of legal liability. In response to the finding, GSA management has updated the warning banners for the information systems to be in compliance with the GSA IT Security Policy, CIO 2100.1J, April 28, 2016.

We recommend that GSA perform the following action:

1. Configure and update the warning banners to conform to GSA requirements.

## 5. Contingency Planning

### Contingency Planning Testing and Business Impact Analysis

While performing our FISMA evaluation procedures we inspected GSA's contingency planning testing and business impact analysis (BIA) policies and procedural guides, conducted inquiries with individuals to walk through the process and determined that GSA has a contingency planning testing and BIA program, however we did identify the following exceptions:

- BIA was not incorporated in the contingency plans for one information systems and two minor applications;
- The contingency plan for one minor application had not been tested during the fiscal year; and
- Backups for two minor applications were not configured and performed.

The CIO-IT Security-06-29, GSA IT Security Procedural Guide: *Contingency Planning (CP)*, Revision 3, March 9, 2016, section 1.3, Contingency Planning Roles and Responsibilities on page 3, states:

> "System Owners (e.g. System Program Managers/Project Managers). The Contingency Planning responsibilities of the System Owner include the following: […]Developing, implementing and maintaining an approved IT Contingency Plan which includes an acceptable Business Impact Analysis (BIA)."

Section 2.2, Step 2 – Conduct the Business Impact Analysis on page 6, states:

> "The BIA should be performed during the Initiation phase of the System Development Lifecycle (SDLC). As the system design evolves and components change, the BIA may need to be conducted again during the Development/Acquisition phase of the SDLC. All information systems are required to conduct a BIA as part of the overall contingency planning process. The BIA development process as detailed by NIST SP 800-34, typically consists of the following steps:
>
> - Determine mission/business functions and recovery criticality.
> - Identify resource requirements.
> - Identify recovery priorities for system resources."

Section 2.6, Step 6 – Ensure Plan Testing and Exercise on page 9, states:

> "Regardless of the test type selected, all Contingency Plan Tests should address the following key areas (as applicable):
>
> - Notification procedures;
> - System recovery on an alternate platform from backup media;
> - Internal and external connectivity;
> - System performance using alternate equipment;
> - Restoration of normal operations; and
> - Other plan testing (where coordination is identified, i.e., Continuity of Operations (COOP), Business Continuity Plan (BCP)).
>
> There are two basic formats for contingency plan tests, including:
>
> - Classroom or Tabletop Exercise – Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to

discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

- Functional Exercise (Limited Scope or Integrated Testing) – Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner."

Section 4.3, CP-4 Contingency Plan Testing and Exercises on page 17, states:

> "As per CP-4, Enhancement (1), GSA FIPS 199 Moderate and High impact systems must coordinate their contingency plan testing with organizational elements responsible for related plans such as Disaster Recovery, Continuity of Operations (COOP) and/or Incident Response plans."

GSA management stated they did not have adequate time and/or resources to perform the required annual testing of contingency plan and Disaster Recovery Plan (DRP) and BIA.

One information system's environment is currently in a transitional period, which will allow for the consolidation of multiple similar components under the same scope. Due to the transitional period, these documents were unable to be provided.

There is a risk that critical steps to recover the application, resources requirements, and recovery priorities are not identified and incorporated into the contingency plan when the BIA has not been completed and this could impact the recovery of the application. Since testing the contingency plan was not completed on a regular basis, management may not be aware of risks that could impact the successful restoration of the system, along with increasing the risk of a compromise of the confidentiality, integrity, and availability of the data residing on the information system in the event of a disaster.

We recommend that GSA perform the following actions:

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.

**System Backups**

While performing our FISMA evaluation procedures we inspected GSA's backup policies and procedural guides, and conducted inquiries with individuals to walk through the process. We determined that GSA requires backups to be performed, but we identified that backups were not configured or performed for two minor applications.

The CIO-IT Security-06-29, GSA IT Security Procedural Guide: *Contingency Planning*, Revision 3, March 9, 2016, section 4.8, CP-9 Information System Backup on pages 23-24, states:

> "Backups are performed primarily for recovery purposes and therefore serve one of the key elements of contingency planning. As such, it is equally important that the security and the integrity of the backup data be maintained at the alternate storage location. Chapter 5, pages 45-47 of NIST SP 800-34 provides detailed guidance on selecting and implementing an effective backup strategy as well as implementing the appropriate data security in order to maintain the integrity of system data and software.
>
> GSA policy requires a Grandfather-Father-Son backup scheme (GFS Scheme) with daily incremental and Friday full backups to be performed for each of the information types identified in the control objectives. The protection of backup data at the alternate storage location must be implemented in accordance with the NIST SP 800-53, Rev 4, requirements per FIPS 199 impact level. Typical protective mechanisms include the use of digital signatures and cryptographic hashes.
>
> As per CP-9, Enhancement (1), GSA FIPS 199 Moderate and High impact systems must test their backup information at least annually."

GSA management stated a new tool was being implemented to perform information system backups which prevented backups from being performed.

Without functioning backups and replication, the minor applications could experience unnecessary downtime and lack of data integrity in the event of a disaster.

We recommend that GSA perform the following action:

1. Configure the new tool, Catalogic Software Management, to back up information systems on a frequency consistent with GSA policy.

## MANAGEMENT RESPONSE TO THE REPORT

The following is the GSA CIO's response, dated December 5, 2016, to the FY 2016 FISMA Evaluation Report.

GSA

GSA Office of the Chief Information Officer

December 5, 2016

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 Reports KPMG's Fiscal Year 2016 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 reports entitled *Draft Evaluation Reports: KPMG's Fiscal Year 2016 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 objectives 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, 2016. The specific objectives of this evaluation was to:

- Perform the annual independent FISMA evaluation of the GSA's information security programs and practices.
- Respond to the DHS FISMA questions on behalf of the GSA OIG.
- Follow up on the status of prior-year FISMA findings.

We conducted our independent evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation and applicable AICPA standards.

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation, Presidential directives, and the DHS *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics V1.1.3*, dated September 26, 2016. We reviewed the GSA 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 also tested a selection of six GSA information systems, which included six minor applications and five GSA contractor information systems from a total population of 117 major applications and general support systems as of May 18, 2016. We tested the information systems to assess whether GSA was effective in implementing the GSA's security program and meeting the FIPS 200 minimum-security standards to protect information and information systems.

We mapped the requirements of FY2016 DHS/OMB IG questions to the NIST SP 800-53, Revision 4 security controls. The controls selected provide continuous, automated monitoring of the most at risk portions of GSA's information technology infrastructure and address the metric domain requirement. Having these controls in place will allow GSA to focus on its primary mission.

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

- Conducting inquires 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 the GSA's headquarters offices in Washington, D.C. during the period of April 28, 2016 through September 2, 2016. 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 2016 FISMA evaluation:

**NIST, FIPS and/or Special Publications**[3]

- *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 1, Guide to Enterprise Telework and Remote Access 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 800-63-2, Electronic Authentication Guideline*
- *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, Management of Federal Information Resources*
- *M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*
- *M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*
- *OMB Memorandum 15-01, Fiscal Year 2014 – 2015 Guidance on Improving Federal Information Security and Privacy Management Practices*
- *M-14-04, Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
- *M-14-03, Enhancing the Security of Federal Information and Information Systems*
- *M-12-20, FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
- *M-12-05, Update on Contingency Planning*
- *OMB Memorandum 07-18, Ensuring New Acquisitions Include Common Security Configurations*

[3] 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.

- *OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- *OMB Memorandum 07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*
- *OMB Memorandum 06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments*
- *OMB Memorandum 06-16, Protection of Sensitive Agency Information*
- *OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*
- *OMB Memorandum 04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act (as amended)*

**United States Department of Homeland Security**

- *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics V1.1.3 September 26, 2016*

**GSA Policy and Procedural Guides**

- *IT Security Procedural Guide: Termination and Transfer CIO-IT Security-03-23, Revision 3, June 30, 2015*
- *IT Security Procedural Guide: Access Control CIO-IT Security-01-07, Revision 3, April 1 2015*
- *IT Security Procedural Guide: Audit and Accountability (AU) CIO-IT Security-01-08, Revision 4, July 18, 2016*
- *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, Version 1.0, May 1, 2015*
- *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 3, June 29, 2016*
- *IT Security Procedural Guide: CIO-IT Security-09-48 Security Language for IT Acquisition Efforts, Revision 2, November 7, 2014*
- *GSA IT Security Policy, CIO 2100.1J, April 28, 2016*
- *IT Security Procedural Guide: Incident Response (IR), CIO-IT Security-01-02, Revision 12, March 15, 2016*
- *IT Security Procedural Guide: Identification and Authentication, CIO-IT Security-01-01, Revision 4, May 30, 2015*
- *IT Security Procedural Guide: IT Security Training and Awareness Program CIO-IT Security 05-29, Revision 4, November 3, 2015*
- *IT Security Procedural Guide: Information Security Continuous Monitoring Strategy, CIO-IT Security-12-66, June 24, 2015*
- *IT Security Procedural Guide: Managing Enterprise Risk Security Assessment and Authorization, Planning, and Risk Assessment (CA, PL, & RA) CIO-IT Security-06-30, Revision 9, May 19, 2016*
- *GSA IT Risk Management Strategy, Version 1.0, June 15, 2015*
- *GSA Order CIO 2100.3C Mandatory IT Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities, June 23, 2016*

- *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, June 21, 2016*
- *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 1, March 15, 2016*

## *APPENDIX II – STATUS OF PRIOR-YEAR FINDINGS*

In FY 2014, another firm conducted the FISMA Evaluation and KPMG conducted the FY 2015 FISMA Evaluation. As part of this year's FISMA Evaluation, we followed up on the status of the 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 – 2014 Evaluation**

| Finding # | Prior-Year Condition | Recommendation(s) | Status |
|---|---|---|---|
| **2.2 – Configuration-Related Vulnerabilities** | While performing our FISMA evaluation procedures, we determined that GSA has not documented the timely remediation of configuration-related vulnerabilities, including scan findings, as part of the POA&M process, as specified in the organization's policies and procedures. In accordance with GSA guidelines, "GSA requires the mitigation of all HIGH RISK vulnerabilities within 30 days (of identifying vulnerabilities) per the Government Performance and Results Act measures." However, GSA does not have organization-wide policies and procedures for determining whether the organization remediates high risk vulnerabilities within a timely manner. | 2. Develop procedures to determine whether configuration-related vulnerabilities are remediated within a timely manner of the weaknesses discovery. | 2. Closed |

**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:<br><br>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.<br><br>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.<br><br>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. | 1. Remediate high and critical vulnerabilities in-accordance within 30 days as required by GSA policy.<br><br>2. Maintain evidence that ISSOs or other designated individuals review the operating system and database compliance, WebInspect and the vulnerability scan reports. | 1. Closed<br><br>2. Open |

| Finding # | Prior-Year Condition | Recommendation(s) | Status |
|---|---|---|---|
| **2. Contingency Planning** | While performing our FISMA evaluation procedures we inspected GSA's contingency planning and backup policy and procedural guides, we conducted inquiries with individuals to walk through the process and determined that GSA has a contingency planning program and requires backups to be performed, however we did identify the following exceptions:<br>a. Supply chain threats were not addressed for all five systems selected.<br>b. There was no evidence that the Business Impact Analysis results were incorporated for three of the five systems selected for testing.<br>c. The contingency plan was tested for only three of the five systems selected for testing.<br>d. There was no evidence of having an alternate processing agreement for four of five systems selected for testing.<br>e. Backups were not performed for two of the five systems selected for testing. | 1. Update the contingency plans to include the missing NIST-required sections.<br>2. Schedule and perform an annual test of contingency plans to determine if it is effective and incorporate lessons learned from the test.<br>3. Work with all responsible parties and have an alternate processing site agreement in place and update the contingency plan and system security plan.<br>4. Identify the cause for backups not being performed and implement a backup schedule in accordance with GSA policy. | 1. Closed<br>2. Closed<br>3. Closed<br>4. 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, 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:<br><br>a. We inspected 19 IT Security Policy/Procedural Guides and determined the following four have not been reviewed or updated annually:<br>• IT Security Procedural Guide: Configuration Management (CM) CIO-IT Security-01-05<br>• IT Security Procedural Guide: Contingency Planning (CP) CIO-IT Security-06-29<br>• IT Security Procedural Guide: Managing Enterprise Risk, CIO-IT Security-06-30<br>• IT Security Procedural Guide: Windows 7 Hardening CIO-IT Security-11-61<br><br>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. | 1. For the four information systems, review and update the system security plans to include all relevant controls from NIST SP 800-53, Revision 4.<br><br>2. Continue to review and update the IT Security Procedural Guides to reflect the NIST SP 800-53, Revision 4 security controls.<br><br>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.<br><br>4. Provide periodic training over the review and completion of the GSA Authorization package, to include all documents within the enclosure of the package. | 1. Closed<br><br>2. Closed<br><br>3. Open<br><br>4. Open |

| Finding # | Prior-Year Condition | Recommendation(s) | Status |
|---|---|---|---|
| | 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. | | |
| **4. Security Training** | While performing our FISMA evaluation procedures we inspected GSA's security training policies and procedural guides and conducted inquiries with individuals to walk through the security training program. We selected 15 individuals to review their training records and determined that evidence for four individuals could not be provided for role-based training. | 1. Develop tracking procedures that cohesively tracks the class participation and successful completion of their classes. | 1. Closed |
| **5. Plan of Action and Milestones** | While performing our FISMA evaluation procedures we inspected GSA's POA&M policy and procedural guides and conducted inquiries with individuals to walk through the POA&M process. We then inspected the POA&Ms and determined that costs associated with weaknesses were not being recorded or tracked for two of the five systems. | 1. Tie the agency's budget submission using the systems unique project identifier. This links the security costs for a system with the security performance of a system.<br><br>2. Identify, estimate, and record the cost to mitigate weaknesses on the POA&M. | 1. Closed<br><br>2. Closed |

## APPENDIX III – GLOSSARY

| ACRONYM | DEFINITION |
|---|---|
| A&A | Assessment and Authorization |
| AICPA | American Institute of Certified Public Accountants |
| AO | Authorizing Officials |
| ATO | Authority To Operate |
| AU | Audit and Accountability |
| BCP | Business Continuity Plan |
| BIA | Business Impact Analysis |
| CA | Security Assessment and Authorization |
| CCB | Configuration Control Board |
| CI | Configuration Items |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| CM | Configuration Management |
| COOP | Continuity of Operations |
| COTR | Contracting Officer's Technical Representative |
| COTS | Commercial Off-The-Shelf |
| CP | Contingency Planning |
| CSIP | Cybersecurity Strategy and Implementation Plan |
| DHS | Department of Homeland Security |
| DRP | Disaster Recovery Plan |
| EARC | Enterprise Architecture Committee |
| FAR | Federal Acquisition Regulation |
| FedRAMP | Federal Risk and Authorization Management Program |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Modernization Act |
| FY | Fiscal Year |
| GSA | U.S. General Services Administration |
| HSPD | Homeland Security Presidential Directive |
| IAW | In Accordance With |
| IG | Inspector General |
| IR | Incident Response |
| ISA | Interconnection Security Agreement |
| ISDN | Integrated Services Digital Network |
| ISP | Policy and Compliance Division |
| ISSM | Information System Security Manager |

| ACRONYM | DEFINITION |
|---|---|
| ISSO | Information System Security Officer |
| IT | Information Technology |
| LATO | Limited Authority to Operate |
| NIST | National Institute of Standards and Technology |
| OCISO | Office of the Chief Information Security Officer |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| OS | Operating System |
| PIV | Personal Identity Verification |
| POA&M | Plan of Action and Milestones |
| SAML | Security Assertion Markup Language |
| SDLC | System Development Lifecycle |
| SIEM | Security Information and Event Management |
| SOC | Service Organization Control |
| S/SO/R | Services, Staff Offices, or Regions |
| SP | Special Publication |
| SSL | Secure Sockets Layer |
| SSP | System Security Plan |
| TLS | Transport Layer Security |
| USGCB | United States Government Configuration Baseline |
| VPN | Virtual Private Network |