



---

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

---

**Independent Evaluation on the  
Effectiveness of the U.S. General  
Services Administration's  
Information Security Program and  
Practices Report - Fiscal Year 2018**

December 21, 2018

**SENSITIVE INFORMATION REMOVED FOR PUBLIC RELEASE**




U.S. GENERAL SERVICES ADMINISTRATION  
Office of Inspector General

---

JAN 18 2019

MEMORANDUM FOR: Emily W. Murphy  
Administrator (A)

FROM: Carol F. Ochoa   
Inspector General (J)

SUBJECT: Independent Evaluation on the Effectiveness of the U.S.  
General Services Administration's Information Security  
Program and Practices Report - Fiscal Year 2018, dated  
December 21, 2018

As required by the *Federal Information Security Modernization Act of 2014* (FISMA), attached is the annual independent evaluation report on the effectiveness of GSA's Information Security Program and Practices for Fiscal Year 2018. This restricted report contains specific systems' deficiencies and should be disseminated only to those individuals with a need to know.

FISMA requires Inspectors General or an independent external auditor, as determined by the Inspector General, to perform an annual independent evaluation of their agency's security program and practices. GSA contracted with KPMG LLP (KPMG), an independent public accounting firm, to conduct this annual evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE's) *Quality Standards for Inspection and Evaluation* and the Office of Management and Budget's (OMB's) FISMA reporting requirements. This independent evaluation did not constitute an engagement in accordance with the Government Accountability Office's *Government Auditing 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, 2017, through September 30, 2018, for its information systems, including GSA's compliance with FISMA and related information security policies, procedures, standards, and guidelines.

We monitored KPMG's work and reviewed their report and related documentation to ensure professional standards and contractual requirements were met. Our review was not intended to enable us to express, and we do not express, opinions on the effectiveness of GSA's information security controls or on whether GSA's security program complied with FISMA. 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, in all material respects, with CIGIE's *Quality Standards for Inspection and Evaluation* and OMB's FISMA reporting requirements.

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 2019 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

January 15, 2019

Dear Ms. Presley-Doss,

As a deliverable for the FY 2018 General Services Administration (GSA) Office of Inspector General (OIG) Federal Information Security Modernization Act (FISMA) evaluation, we have submitted the *Independent Evaluation on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2018*. This report was provided to you in this format pursuant to our contract GS-00F-275CA, task order number GSH1416AA0136 and is subject in all respects to the contract terms, including restrictions on disclosure of this deliverable to third parties.

Detailed within the FY 2018 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,

A handwritten signature in black ink, appearing to read 'James DeVaul'. The signature is written in a cursive, flowing style with a large, prominent loop at the end.

James DeVaul

# Independent Evaluation on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2018

December 21, 2018



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 INDEPENDENT EVALUATION REPORT .....	1
BACKGROUND .....	4
FEDERAL INFORMATION SECURITY MODERNIZATION ACT .....	4
FY 2018 INSPECTOR GENERAL FISMA REPORTING METRICS .....	5
OVERALL EVALUATION RESULTS.....	6
FINDINGS .....	8
1. IDENTIFY FUNCTION – RISK MANAGEMENT.....	8
2. PROTECT FUNCTION – CONFIGURATION MANAGEMENT .....	10
3. PROTECT FUNCTION – IDENTITY AND ACCESS MANAGEMENT.....	11
4. RECOVER FUNCTION – CONTINGENCY PLANNING .....	13
MANAGEMENT RESPONSE TO THE REPORT .....	15

**Appendices**

APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY .....	16
APPENDIX II – STATUS OF PRIOR-YEAR FINDINGS .....	20
APPENDIX III – GLOSSARY.....	25



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: Independent Evaluation on the Effectiveness of the U.S. General Services Administration’s Information Security Program and Practices Report – Fiscal Year 2018**

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 Fiscal Year (FY) 2018 FISMA Reporting Metrics to collect these responses. FISMA requires the agency Inspector General (IG) or an independent external auditor perform the independent evaluation as determined by the IG. GSA contracted 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 of October 1, 2017 to September 30, 2018 for its information systems, including GSA’s compliance with FISMA and related information security policies, procedures, standards, and guidelines. We based our work on a selection of GSA-wide security controls and a selection of system-specific security controls across six selected GSA information systems and two GSA contractor information systems. Additional details regarding the scope of our independent evaluation are included in Appendix I, *Objective, Scope & 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 five cybersecurity



functions<sup>1</sup> and eight FISMA metric domains.<sup>2</sup> In accordance with the results in CyberScope, GSA's information security program was not effective<sup>3</sup> because, while two cybersecurity functions (Identify and Respond) were assessed at Managed and Measurable (Level 4), the other three cybersecurity functions (Protect, Detect, and Recover) were assessed at Consistently Implemented (Level 3).

Since FY 2015, we have identified issues associated with certain FISMA domains. These issues are still present for information systems tested in FY 2018:

- Cybersecurity Function: Identify – Risk Management: system security plans were not documented in-accordance with GSA requirements or were missing information;
- Cybersecurity Function: Identify – Risk Management: lack of formalized review and acceptance of contractor system information demonstrating compliance with GSA security requirements;
- Cybersecurity Function: Protect – Configuration Management: system personnel did not review vulnerability or baseline compliance scans;
- Cybersecurity Function: Protect – Identity and Access Management: account management issues where account re-certifications were not performed and user accounts were not removed timely after user separation from GSA; and
- Cybersecurity Function: Recover – Contingency Planning: backups were not performed in accordance with GSA and/or system policy.

We identified eight control deficiencies within three of the five cybersecurity functions and within four of the eight FISMA metric domains (identified in parentheses) as follows:

#### Cybersecurity Function: Identify

- An information system's system security plan (SSP) did not include the controls responsibility matrix (CRM) of inherited controls from the host system. (Risk Management)
- An information system's SSP did not reflect the control environment required by GSA policy. (Risk Management)
- GSA did not have a formal review and acceptance process for third party (contractor system) deliverables designed to monitor security and compliance. (Risk Management)

#### Cybersecurity Function: Protect

- An Information System Security Manager (ISSM) did not review compliance scanning results. (Configuration Management)
- Rules of behavior was not completed prior to gaining network access. (Identity and Access Management)
- A network user was not removed timely after separation. (Identity and Access Management)
- An information system did not have a formal account review/recertification process. (Identity and Access Management)

---

<sup>1</sup> OMB, DHS, and CIGIE developed the FY 2018 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers (CIO) Council. In FY 2018, the eight IG FISMA metric domains were aligned with the five cybersecurity functions of identify, protect, detect, respond, and recover, as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

<sup>2</sup> As described in the DHS' *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0. 1, May 24, 2018*, the eight FISMA metric domains are: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

<sup>3</sup> The scoring methodology is described in the DHS' *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0. 1, May 24, 2018*, which requires a Managed and Measurable rating (Level 4) to be considered effective as determined by the entries in CyberScope.





Cybersecurity Function: Recover

- Backups were not performed for parts of the production environment of an information system. (Contingency Planning)

We provided 13 recommendations related to these control deficiencies that, if effectively addressed by management, should strengthen the respective information systems and GSA's information security program. GSA should also implement a process that ensures similar conditions are addressed across all information systems. In a written response, the GSA Chief Information Officer (CIO) agreed with our findings and recommendations (see *Management Response*, page 15).

This independent evaluation did not constitute an engagement in accordance with *Generally Accepted Government Auditing Standards*. 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 risk that controls may become inadequate because of changes in technology or because compliance with controls may deteriorate.

Sincerely,

**KPMG LLP**

December 21, 2018

## **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 both the information and information systems supporting 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, related OMB policies, as well as 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 the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG.

**FY 2018 Inspector General FISMA Reporting Metrics**

For FY 2018, OMB, DHS, and CIGIE implemented a change to the IG FISMA reporting metrics by adding the metric Data Protection and Privacy to the Protect Function. The questions are still organized around the five information security functions outlined in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). **Table 1** shows the alignment of Cybersecurity Framework to the FISMA Metric Domains.

<b>Cybersecurity Framework Security Functions</b>	<b>FY 2018 IG FISMA Metric Domains</b>
Identify	Risk Management
Protect	Configuration Management Identity and Access Management Data Protection and Privacy 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 2018 IG FISMA Metric Domains.

## **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 five cybersecurity functions and eight FISMA metric domains.

While a security program has been implemented across GSA, we identified eight control deficiencies in three of five FISMA metric functions that we reported to GSA management. We provided 13 recommendations related to these control deficiencies that, if effectively addressed by management, should strengthen the respective information systems and GSA's information security program.

Furthermore, in accordance with the results in CyberScope, GSA's information security program was not effective because, while two cybersecurity functions (Identify and Respond) were assessed at Managed and Measurable (Level 4), the other three cybersecurity functions (Protect, Detect, and Recover) were assessed at Consistently Implemented (Level 3).

Since FY 2015, we have identified issues associated with certain FISMA domains. These issues are still present for information systems tested in FY 2018:

- Cybersecurity Function: Identify – Risk Management: system security plans were not documented in accordance with GSA requirements or were missing information;
- Cybersecurity Function: Identify – Risk Management: lack of formalized review and acceptance of contractor system information demonstrating compliance with GSA security requirements;
- Cybersecurity Function: Protect – Configuration Management: system personnel did not review vulnerability or baseline compliance scans;
- Cybersecurity Function: Protect – Identity and Access Management: account management issues where account re-certifications were not performed and user accounts were not removed timely after user separation from GSA; and
- Cybersecurity Function: Recover – Contingency Planning: backups were not performed in accordance with GSA and/or system policy.

We identified eight control deficiencies within three of the five cybersecurity functions and within four of the eight FISMA metric domains (identified in parentheses) as follows:

### Cybersecurity Function: Identify

- An information system's SSP did not include the CRM of inherited controls from the host system. (Risk Management)
- An information system's SSP did not reflect the control environment required by GSA policy. (Risk Management)
- GSA did not have a formal review and acceptance process for third party (contractor system) deliverables designed to monitor security and compliance. (Risk Management)

### Cybersecurity Function: Protect

- An ISSM did not review compliance scanning results. (Configuration Management)
- A GSA system user did not certify their acceptance of the Agency's rules of behavior prior to gaining network access. (Identity and Access Management)
- A network user was not removed in a timely manner after separation. (Identity and Access Management)

- An information system did not have a formal account review/recertification process. (Identity and Access Management)

Cybersecurity Function: Recover

- Backups were not performed for two production servers of an information system. (Contingency Planning)

The *Findings* section of this report presents the detailed findings and associated recommendations grouped by the FISMA metric domain. We will review the status of these findings as part of the FY 2019 independent evaluation.

Additionally, we evaluated the open prior-year findings from the FY 2017 and FY 2016 FISMA evaluations and noted management closed a total of four out of nine findings with the remaining five partially closed. See Appendix II, *Status of Prior-Year Findings*, for additional details.

In a written response to this report, the GSA CIO agreed with our findings and recommendations (see *Management Response*, page 15).

## FINDINGS

### 1. Identify Function – Risk Management

#### System Security Plan

We determined an information system's SSP did not include the CRM that identifies the fully inherited controls from the host information system or PL8 (information security architecture), a critical control required by GSA. We also determined that another information system's SSP did not reflect the current hosting environment. Specifically, the baseline compliance and vulnerability scans and system backups were not documented in accordance with GSA policy.

NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, pages F-139 – F-140, states:

“PL-2 System Security Plan

Control: The organization:

- a. Develops a security plan for the information system that:
  - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions  
[...]
- d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments”

Due to lack of management oversight, the CRM checklist identifying the critical controls inherited from the host system was not referenced in the information system's SSP. The system owners failed to review and update the SSP to reflect the system environment and how the controls are currently operating.

Without an accurate SSP encompassing critical and required controls inherited from the host information system, the potential exists for the system owner to overlook risks that may not be covered by the host information system, which may compromise the integrity of the system. Without an updated SSP, the potential exists for discrepancies between how controls are implemented and operate. This could result in controls that are not operating as required by GSA policy and increase the risk to the confidentiality, availability, and integrity of data.

We recommend GSA perform the following actions:

1. Update the SSP to include the CRM and reflect the NIST SP 800-53 Revision 4 security controls are fully inherited from the host information system.
2. Review and update the SSP to reflect the current hosting environment.

#### Contractor Systems

We determined GSA does not have a formal process for reviewing and accepting required deliverables used for monitoring contractor's compliance with GSA security requirements for one of two information systems.

The GSA Information Technology (IT) Security Procedural Guide: *Security and Privacy Requirements for IT Acquisition Efforts CIO-IT Security-09-48 Revision 4*, January 25, 2018, on page 11, 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 external 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 [Authorizing Officials] AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

Deliverables to be provided to the GSA [Contractor Officer’s Representative] COR/[Information System Security Officer] ISSO/ISSM Quarterly

- Vulnerability Scanning
- Plan of Action and Milestones (POA&M) Update

Deliverables to be provided to the GSA COR/ISSO/ISSM Annually

- Updated [Authorization and Accreditation] (A&A) documentation including the System Security Plan and Contingency Plan
- User Certification/Authorization Review Documents
- Separation of Duties Matrix
- Information Security Awareness and Training Records
- Annual FISMA Assessment
- System(s) Baseline Configuration Standard Document
- System Configuration Settings
- Configuration Management Plan
- Contingency Plan Test Report
- Incident Response Test Report
- Results of Physical Security User Certification/Authorization Review
- Results of Review of Physical Access Records
- Information System Interconnection Agreements
- Rules of Behavior
- Personnel Screening and Security”

While GSA received the information from the contractors, there was no formal review or acceptance of the deliverables by management in order to determine contractor compliance with GSA security policies. Failure to properly review and accept the deliverables could result in GSA failing to identify and track potential security weaknesses that need to be remediated by the contractor.

We recommend GSA perform the following actions:

1. Implement a formalized review and acceptance process of contractor deliverables that requires both the ISSM/ISSO and the COR review the information provided by the contractor, and sign-off on the review and acceptance in a timely manner.
2. Provide training to applicable GSA employees reviewing and accepting contractor deliverables stated in the CIO-IT Security-09-48, IT Security Procedural Guide: *Security and Privacy Requirements for IT Acquisition Efforts*.

## 2. Protect Function – Configuration Management

### Compliance and Vulnerability Scans

For a selection of five biweekly scans, we determined that one of the scans was not reviewed by management.

GSA IT Security Procedural Guide: *Vulnerability Management Process CIO-IT Security-17-80*, Section 5.3 Configuration Baseline Reports, page 6, states:

“To support GSA requirements for compliance with configuration baselines (a POA&M is required unless 75% of systems within the FISMA boundary are compliant with 75% of the baseline configuration settings), the SecOps Scanning Team prepares biweekly reports for approved configuration baselines. The results are distributed for review to ISSOs and ISSMs in system-specific zip files.”

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, page F-64, states:

“CM-2 Baseline Configuration

Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.”

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, page F-153, states:

“RA-5 Vulnerability Scanning

Control: The organization:

- a. Scans for vulnerabilities in the information system and hosted applications [Assignment: *organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;  
[...]
- c. Analyzes vulnerability scan reports and results from security control assessments;”

During January 2018, a new ISSO for the system transitioned into the role. During the transition, the ISSO’s responsibility for reviewing the scan results and communicating them to the information system team was not performed. This lack of review of security compliance scans increases the amount of risk the system could be exposed to, including configuration weaknesses or vulnerabilities that could compromise the operational integrity of the system.

We recommend GSA perform the following action:

1. Assign a backup employee for reviewing compliance/vulnerability scan results in order to perform this function in the absence of the ISSO.



### 3. Protect Function – Identity and Access Management

#### Account Management

We identified the following exceptions:

- a. The rules of behavior (ROB) was not completed for 1 out of 45 new users selected for testing. The user was granted network access on April 20, 2018 and the ROB was not signed until July 2, 2018.
- b. For one out of 634 separated users, GSA did not remove access to the user’s network account timely (within 30 days of user separation).
- c. One information system does not have a formal or periodic process to perform account recertification.

*GSA IT Security Policy CIO 2100.1K*, Chapter 3: Policy on Management Controls, Section h. Rules of the system, pages 37-38, states:

- “(1) Authorized users must be provided written Rules of Behavior IAW [In Accordance With] GSA Order CIO 2104.1 before being allowed access into any GSA, non-public information system.
- (2) The user must acknowledge receipt of these rules through a positive action.”

*GSA IT Procedural Guide: Information Security Program Plan (ISPP) CIO-IT Security-18-90*, Section 3.12.2 Rules of Behavior (PL-4), pages 60-61, states:

“The organization:

- a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
- b. Receives a signed acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; ...”

*GSA IT Security Policy CIO 2100.1K*, Chapter 5: Policy on Technical Controls, Section I. Account Management, page 69, states:

- “(2) Upon issuance of the CISO monthly separation reports, data and system owners must verify within thirty (30) days that separated personnel no longer maintain access to GSA IT systems or resources.”

*GSA IT Security Policy CIO 2100.1K*, Chapter 5: Policy on Technical Controls, Section b. Logical access controls, page 62, states:

- “(3) Information system accounts must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Reviews and validations of system users’ and staff users’ accounts shall be completed annually to ensure the continued need for system access.”

*GSA IT Security Policy CIO 2100.1K*, Chapter 5: Policy on Technical Controls, Section I. Account management, pages 68-69, states:

“(7) User account privileges must be reviewed across the appropriate Service and Staff Office application portfolio to assess incompatible and non-compliant role assignments (e.g. review of user access assignments across multiple significant systems that share data or pass transactions to identify conflicts with separation of duties policy).”

*GSA system application, System Security Plan, Section 13.1.2 AC-2: Account Management, pages 54-56, states:*

“The organization:

j. Reviews accounts for compliance with account management requirements annually  
[...]

Tenant Responsibility:

GSA tenant is responsible for implementing appropriate Account Management processes, Administration for privileged and non-privileged accounts, monitoring for all accounts IAW GSA policy for Database Scheme and Web Application components as well as for those services/components not selected from the Service Catalog.”

Due to a management oversight in the provisioning of the user’s network access, the ROB was not completed before network account access was granted. Authorized users that do not read and sign the ROB could have access to the system and not be aware of their user requirements.

Also, management failed to disable a user’s network account in a timely manner. When users separate from GSA and their user account is not removed, unauthorized users could use the account to gain access to the GSA network.

System management failed to create a formalized process to recertify user accounts. Lack of a formal account recertification process could allow non-authorized users access to the information system. These gaps could negatively impact the confidentiality, availability, and integrity of GSA data.

We recommend GSA perform the following actions:

1. Compare the Rules of Behavior Tracker to the New Hire Listing on a monthly basis to verify new hires have completed the Rules of Behavior.
2. Compare the separations report to the Active Directory user listing on a monthly basis to ensure separated users are removed from the Active Directory.
3. Develop and implement a formalized process to approve and review privileged user accounts for an information system.
4. Maintain evidence for the approval, review, and removal of privileged user accounts.
5. Provide training on the account management requirements for an information system.

#### 4. Recover Function – Contingency Planning

##### System Backups

We determined daily and weekly backups for two production servers on the information system were not performed for a period of time.

GSA IT Procedural Guide: *Contingency Planning (CP) CIO-IT Security-06-29, Revision 4*, Section 4.8 CP-9 Information System Backup, pages 24-25, states:

“Control: The organization:

- a. Conducts backups of user-level information contained in the information system [using at least a Grandfather-Father-Son scheme with daily incremental and weekly full];
- b. Conducts backups of system-level information contained in the information system [using at least a Grandfather-Father-Son scheme with daily incremental and weekly full];
- c. Conducts backups of information system documentation including security-related documentation [using at least a Grandfather-Father-Son scheme with daily incremental and weekly full]”

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, CP-9 Information System Backup, page F-86, states:

“Control: The organization:

- a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
- b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
- c. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and
- d. Protects the confidentiality, integrity, and availability of backup information at storage locations.”

Due to the lack of adherence to GSA-wide policies, GSA IT personnel did not complete the daily backup of an information system. Furthermore, two servers did not receive backup requests until June 10, 2018.

Without conducting proper system backups, management cannot ensure all system information is safely stored and secured. This increases the risk for loss of information and inaccurate data: therefore, increasing the risk that the integrity and availability of the data residing within those servers is compromised and lost. Without current backups, management may experience increased downtime as it works to recover the application data.

We recommend GSA perform the following actions:

1. Enforce NIST, GSA-wide, and system-specific backup policies and procedures to ensure the control is operating effectively.

2. Provide periodic training of NIST, GSA-wide, and system-specific backup policies and procedures.
3. Develop routine system checks and preventative monitoring to ensure systems are properly being backed up on a daily basis.

## MANAGEMENT RESPONSE TO THE REPORT

The following is the GSA CIO's response, dated December 13, 2018, to the FY 2018 FISMA Evaluation Report.



GSA Office of the Chief Information Officer

December 13, 2018

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

FROM DAVID A. SHIVE e-Signed by David Shive  
on 2018-12-14  
CHIEF INFORMATION OFFICER – I

SUBJECT: Agency Management Response – Draft Evaluation Report  
*Independent Evaluation on the Effectiveness of the U.S. General Services  
Administration's Information Security Program and Practices Report - Fiscal Year 2018*

The Office of the Chief Information Officer appreciates the opportunity to review and comment on the draft evaluation report entitled *Independent Evaluation on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2018*. We agree with the findings and recommendations stated in the report.

If you have any questions or concerns, please contact Pranjali Desai, Acting Chief Information Security Officer (CISO) of my staff, on 202-208-0719.

U.S. General Services Administration  
1800 F Street NW  
Washington, DC 20405  
[www.gsa.gov](http://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, 2018. 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 2018 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 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 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 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0.1*, dated May 24, 2018. 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 implemented these policies and procedures.

We made a selection of six GSA information systems and two GSA contractor information systems from a total population of 113 major applications and general support systems as of March 19, 2018.

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 office in Washington, District of Columbia (D.C.) during the period of April 10, 2018 through September 30, 2018. During the course of 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 2018 FISMA evaluation:

**NIST, Federal Information Processing Standard (FIPS), and/or SPs<sup>4</sup>**

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST Cybersecurity Framework Version 1.1, *Framework for Improving Critical Infrastructure Cybersecurity*
- NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*
- NIST SP 800-44 Version 2, *Guidelines on Securing Public Web Servers*
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-60 Volume 1, Revision 1: *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*
- NIST SP 800-63-3, *Digital Identity Guidelines*
- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
- NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*
- NIST SP 800-184, *Guide for Cybersecurity Event Recovery*
- NIST Supplemental Guidance on Ongoing Authorization, *Transitioning to Near Real-Time Risk Management*

**OMB Policy Directives**

- Federal Enterprise Architecture (FEA) Framework, Version 2
- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*
- OMB Circular A-130, *Managing Information as a Strategic Resource*
- OMB Memorandum 08-05, *Implementation of Trusted Internet Connections (TIC)*
- OMB Memorandum 14-03, *Enhancing the Security of Federal Information and Information Systems*

---

<sup>4</sup> 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 16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*
- OMB Memorandum 17-09, *Management of Federal High Value Assets*
- OMB Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*
- OMB Memorandum 17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
- OMB Memorandum 18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security Privacy Management Requirements*

#### **United States Department of Homeland Security**

- DHS Binding Operational Directive 15-01, *Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems*
- DHS Binding Operational Directive 17-01, *Removal of Kaspersky-Branded Products*
- FCD-1, *Federal Continuity Directive 1*
- FY 2018 Chief Information Officer (CIO) Federal Information Security Modernization Act Metrics
- FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0.1, May 24, 2018
- United States Computer Emergency Readiness Team (US-CERT) Federal Incident Notification Guidelines
- US-CERT Federal Incident Reporting Guidelines
- Homeland Security Presidential Directive (HSPD) 12, *Policy for a common Identification Standard for Federal Employees and Contractors*
- Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

#### **GSA Policy and Procedural Guides**

- *GSA IT Security Policy CIO 2100.K*, June 30, 2017
- IT Security Procedural Guide: *Risk Management Strategy CIO-IT Security-18-91 Revision 2*, March 14, 2018
- IT Security Procedural Guide: *Managing Enterprise Risk CIO-IT Security-06-30, Revision 12*, January 17, 2018
- IT Security Procedural Guide: *Information Security Program Plan, CIO-IT Security-18-90, Revision 2*, March 14, 2018
- IT Security Procedural Guide: *Federal Information Security Modernization Act (FISMA) Implementation CIO-IT Security-04-26*, April 27, 2017
- GSA Order CIO P 2181.1 *Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing*, October 20, 2008
- IT Security Procedural Guide: *Plan of Action and Milestones (POA&M) CIO-IT Security-09-44, Revision 5*, January 19, 2018
- GSA Order ADM 2400.1A *Insider Threat Program*, May 18, 2016
- IT Security Procedural Guide: *Security and Privacy Requirements for IT Acquisition Efforts CIO-IT Security-09-48, Revision 4*, January 25, 2018
- IT Security Procedural Guide: *Configuration Management (CM) CIO-IT Security-01-05, Revision 4*, January 17, 2018
- IT Security Procedural Guide: *Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Implementation CIO-IT Security-14-69, Revision 3*, April 30, 2018



- IT Security Procedural Guide: *Identification and Authentication (IA)* CIO-IT Security-01-01, Revision 5, May 8, 2017
- IT Security Procedural Guide: *Termination and Transfer* CIO-IT Security-03-23, Revision 3, April 27, 2017
- IT Security Procedural Guide: *Access Control (AC)* CIO-IT Security-01-07, Revision 4, May 8, 2017
- IT Security Procedural Guide: *Audit and Accountability (AU)* CIO-IT Security-01-08, Revision 5, November 3, 2017
- IT Security Procedural Guide: *Security Awareness and Role Based Training Program* CIO-IT Security-05-29, Revision 5, October 25, 2016
- IT Security Procedural Guide: *Contingency Planning (CP)* CIO-IT Security-06-29, Revision 4, April 12, 2018
- IT Security Procedural Guide: *Information Security Continuous Monitoring Strategy*, CIO-IT Security-12-66, Revision 2, October 10, 2017
- IT Security Procedural Guide: *Incident Response (IR)* CIO-IT Security-01-02, Revision 16, March 22, 2018
- GSA Order CIO 2100.3C, *Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities*, June 23, 2016

**Other Directives, Policies, and Legislation**

- National Insider Threat Policy
- Federal Cybersecurity Workforce Assessment Act of 2015
- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance
- National Archives and Records Administration's (NARA) guidance on information systems security records
- Playbook: *Enterprise Risk Management for the U.S. Federal Government*
- Federal Acquisition Regulation (FAR) Case 2007-004, *Common Security Configurations*
- Presidential Policy Direction (PPD) 41, *United States Cyber Incident Coordination*
- U.S. Government Accountability Office (GAO) – Standards for Internal Control in the Federal Government

**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 implemented, we closed the findings. If recommendations were partially implemented, not implemented at all, or we identified findings during our testing, we determined the finding to be open.

**Prior Year Findings – 2016 Evaluation**

<b>Finding #</b>	<b>Prior-Year Condition</b>	<b>Recommendation(s)</b>	<b>Status</b>
<b>1. Risk Management - System Security Plans</b>	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 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.	1. Closed
<b>1. Risk Management - Risk Assessments</b>	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. Closed
<b>1. Risk Management - System Inventory</b>	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.	1. Closed
<b>2. Contractor Systems</b>	We determined that required reviews by the COTR, 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: <i>Security Language for IT Acquisition Efforts</i> .  2. Document the review of third party reports (SOC [System and	1. Closed  2. Open

Finding #	Prior-Year Condition	Recommendation(s)	Status
		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.	
<b>3. Configuration Management - Change/Patch Management Approval</b>	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. Closed
<b>4. Identity and Access Management - Account Management</b>	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.	2. Maintain authorizations for granting access to individuals for privileged access.  3. Remove terminated users from systems within the required timeframes.	2. Closed  3. Open
<b>5. Contingency Planning - Contingency Planning Testing and Business Impact Analysis</b>	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. Closed  2. Closed

Finding #	Prior-Year Condition	Recommendation(s)	Status
	<ul style="list-style-type: none"> <li>Backups for 2 of 12 GSA information systems were not configured and performed.</li> </ul>		

**Prior Year Findings – 2017 Evaluation**

Finding #	Prior-Year Condition	Recommendation(s)	Status
<p><b>1. Identify Function – Risk Management</b></p> <p><b>System Inventory</b></p>	<p>We inspected GSA FISMA reportable system inventory dated March 10, 2017 and August 3, 2017 and determined eight information systems were not appropriately classified as federal information systems based on GSA’s definition.</p>	<p>1. Review the system inventory and reevaluate the system classifications based on GSA’s definitions.</p> <p>2. Consider expanding GSA definitions to include other types of systems such as cloud and hybrid.</p>	<p>1. Closed</p> <p>2. Closed</p>
<p><b>1. Identify Function – Risk Management</b></p> <p><b>Contractor Systems</b></p>	<p>We determined that GSA was receiving the required contractor deliverables for five contractor 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.</p>	<p>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.</p> <p>2. Provide training to applicable GSA employees on reviewing and accepting contractor deliverables stated in the <i>GSA IT Security Procedural Guide: Security Language</i></p>	<p>1. Open</p> <p>2. Closed</p>

Finding #	Prior-Year Condition	Recommendation(s)	Status
		<i>for IT Acquisition Efforts, GSA-IT Security-09-48.</i>	
<p><b>2.Protect Function – Configuration Management</b></p> <p><b>Change/Patch Management Approval</b></p>	<p>We identified the following exceptions:</p> <ul style="list-style-type: none"> <li>• One information system’s authorization and testing evidence for the Quarter 1 Oracle database patch could not be provided; and</li> <li>• One 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.</li> </ul>	<ol style="list-style-type: none"> <li>1. Provide training on the change management requirements required by GSA policy to applicable GSA employees and contractors.</li> <li>2. Document evidence of authorization of application changes, and operating system and database patches.</li> </ol>	<p>1. Closed</p> <p>2. Open</p>
<p><b>3.Protect Function – Identity and Access Management</b></p> <p><b>Account Management</b></p>	<p>We identified the following exceptions:</p> <ol style="list-style-type: none"> <li>a. Evidence of account authorization could not be provided for privileged and non-privileged user accounts for five information systems.</li> <li>b. Terminated privileged accounts for an information system operating system were not removed within 30 days of separation.</li> <li>c. Privileged account reviews for the operating system and database were not performed in accordance with GSA policy to verify that the individuals needed privileged</li> </ol>	<ol style="list-style-type: none"> <li>1. Implement a formal process for approving, reviewing, and removing privileged access.</li> <li>2. Provide training to individuals and contractors that support information systems on entity and system specific policies and for authorizing, granting, reviewing, and removing access.</li> <li>3. Maintain evidence for approving, reviewing, and removing access for individuals with privileged and non-privileged access.</li> </ol>	<p>1. Open</p> <p>2. Closed</p> <p>3. Closed</p>

Finding #	Prior-Year Condition	Recommendation(s)	Status
	access for two information systems.		
<b>3. Protect Function – Identity and Access Management</b>  <b>Session Termination</b>	We determined two information systems (application, operating system, and/or database) session termination configuration settings were configured to be less restrictive than the requirements in the GSA policy.	1. Configure the session termination settings in accordance with GSA policy.	1. Open
<b>4. Recover Function – Contingency Planning</b>  <b>System Backups</b>	We determined that GSA requires Friday full backups to be performed, however, a Friday full weekly backup was not performed for an information system for 1 of 5 selected weeks.	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 for the application.	1. Closed  2. Closed  3. Closed

**APPENDIX III – GLOSSARY**

<b>ACRONYM</b>	<b>DEFINITION</b>
A&A	Authorization and Accreditation
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
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
CP	Contingency Planning
CSIP	Cybersecurity Strategy and Implementation Plan
D.C.	District of Columbia
DHS	Department of Homeland Security
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
GSA	U.S. General Services Administration
HSPD	Homeland Security Presidential Directive
IA	Identity and Access Management
IG	Inspector General
IR	Incident Response
ISCM	Information Security Continuous Monitoring
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
KPMG	KPMG LLP
LATO	Limited Authority to Operate
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget

<b>ACRONYM</b>	<b>DEFINITION</b>
OS	Operating System
POA&M	Plan of Action and Milestones
SOC	System and Organization Controls
SP	Special Publication
SSL	Secure Sockets Layer
SSP	System Security Plan
TLS	Transport Layer Security