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 2019

December 5, 2019

SENSITIVE INFORMATION REMOVED FOR PUBLIC RELEASE

U.S. General Services Administration
Office of Inspector General

JAN 1 7 2020

MEMORANDUM FOR: Emily W. Murphy
Administrator (A)

FROM: Carol F. Ochoa 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 2019, dated December 5, 2019

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 2019. 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, 2018, through September 30, 2019, 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 2020 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

KPMG LLP
8350 Broad Street Suite 900
McLean, VA 22102

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

December 12, 2019

Dear Ms. Presley-Doss,

As a deliverable for the FY 2019 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 2019*. 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.

We conducted our independent evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation and in accordance with Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA), that require us to report our findings and recommendations.

Detailed within the FY 2019 FISMA Report are recommendations to address specific GSA and system-level deficiencies within GSA's information security program and practices. When developing plans of actions and milestones (POA&Ms) or corrective actions, management should assess whether these deficiencies are contained to their respective areas as described in this report or whether the recommendations should be considered for other systems, security control areas, or processes within GSA's information system security program.

Please let me know if you have any questions.

Kind regards,

James W DeVaul

James DeVaul

Independent Evaluation on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2019

December 5, 2019

KPMG LLP
8350 Broad Street, Suite 900
McLean, VA 22102

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

Table of Contents

KPMG LLP
Suite 900
8350 Broad Street
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 2019

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) 2019 FISMA Reporting Metrics to collect these responses. FISMA requires the agency Inspector General (IG) or an independent external auditor to 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 we met professional standards and contractual requirements.

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, 2018 to September 30, 2019 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[1]. Additional details regarding the scope of our independent evaluation are included in Appendix I, *Objective, Scope, and Methodology*. Appendix II, *Status of Prior-Year Findings*, summarizes GSA's progress in addressing prior-year recommendations. Appendix III contains a *Glossary* of terms used in this report.

Consistent with applicable FISMA requirements, OMB policy and guidance, and National Institute of Standards and Technology (NIST) standards and guidelines, GSA established and maintained its information security program and practices for its information systems for the five cybersecurity functions[2] and eight FISMA metric domains[3]. Based on the responses we populated into CyberScope, we determined

[1] GSA information systems are operated internally by GSA whereas contractor systems are operated by a contractor on behalf of the agency.

[2] OMB, DHS, and CIGIE developed the FY 2019 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers (CIO) Council. In FY 2019, 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*.

[3] As described in the DHS' *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.3, April 9, 2019*, the eight FISMA metric domains are: risk management, configuration management, identity

that GSA's overall information security program was effective[4] because the majority of FISMA metric questions were Managed and Measurable (Level 4). The cybersecurity functions Identify, Protect, Detect, and Respond were determined to be Managed and Measurable (Level 4) and Recover was determined to be Consistently Implemented (Level 3).

Since FY 2015, we have identified control deficiencies in certain cybersecurity functions and FISMA metric domains. These control deficiencies continued for entity-wide and information systems' controls tested in FY 2019 as follows:

- Cybersecurity Function/Domain: Identify/Risk Management: lack of formalized review and acceptance of contractor system information demonstrating compliance with GSA security requirements; and

- Cybersecurity Function/Domain: Protect/Identity and Access Management: account management issues where user accounts were not removed timely after user separation from GSA.

While performing entity-wide and information systems' control testing for the FY 2019, we identified three control deficiencies in three of the five cybersecurity functions and three of the eight FISMA metric domains as follows:

Cybersecurity Function/Domain: Identify/Risk Management

- GSA did not have a formal review and acceptance process for deliverables designed to monitor security and compliance for both third-party systems selected.

Cybersecurity Function/Domain: Protect/Identity and Access Management

- One network user was not removed timely after separation.

Cybersecurity Function/Domain: Respond/Incident Response

- Two incidents were not reported timely to United States Computer Emergency Readiness Team (US-CERT).

We provided four 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 control deficiencies 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 11*).

and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

[4] The scoring methodology is described in the DHS' *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.3 April 9, 2019* that requires a Managed and Measurable rating (Level 4) to be considered effective as computed by the entries in CyberScope.

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 5, 2019

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 and 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 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 2019 Inspector General FISMA Reporting Metrics

For FY 2019, OMB, DHS, and CIGIE updated the IG FISMA reporting metrics to reflect changes to laws and guidance for the five cybersecurity functions and the eight FISMA metric domains. The IG FISMA questions are still organized around the five information security functions outlined in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) and the eight FISMA metric domains. **Table 1** shows the alignment of the Cybersecurity Framework to the FISMA Metric Domains.

Cybersecurity Framework Security Functions	FY 2019 IG FISMA Metric Domains
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 2019 IG FISMA Metric Domains.

OVERALL EVALUATION RESULTS

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, GSA established and maintained its information security program and practices for its information systems for the five cybersecurity functions and eight FISMA metric domains. Based on the responses we populated into CyberScope, we determined that GSA's overall information security program was effective because the majority of the FISMA metric questions were Managed and Measurable (Level 4). The cybersecurity functions Identify, Protect, Detect, and Respond were determined to be Managed and Measurable (Level 4) and Recover was determined to be Consistently Implemented (Level 3). The *Findings* section of this report presents the three deficiencies and four recommendations. We will review the status of these findings as part of the FY 2020 independent evaluation.

Additionally, we evaluated the prior-year findings from the FYs 2018, 2017, and 2016, FISMA evaluations and determined that GSA had closed 5 of 10 findings. 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 11*).

FINDINGS

1. Identify Function – Risk Management

Contractor Systems

We determined for both contractor information systems selected for testing that there was only partial or no evidence for certain required deliverables used to monitor contractors' compliance with GSA security requirements that the Contracting Officer's Representative (COR), Information System Security Officer (ISSO), and Information System Security Manager (ISSM) reviewed and accepted.

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, Section 2.5 Reporting and Continuous Monitoring, pages 11-15, 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 AOs [authorizing officials] to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.
>
> Deliverables to be provided to the GSA COR/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 A&A [Authorization and Accreditation] 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 Verification
> - Configuration Management Plan
> - Contingency Plan Test Report
> - Incident Response Test Report
> - Information System Interconnection Agreements
> - Rules of Behavior
> - Penetration Testing Report
> - Personnel Screening and Security"

While GSA received the information from the contractors, there was no formal review and acceptance of the deliverables. Failure to properly review and accept the deliverables might result in security weaknesses that are not tracked by GSA for remediation by the contractor.

RECOMMENDATION:

1. Implement a standard, formal contractor deliverable review and acceptance process by the COR that includes a review by the ISSO/ISSM.

2. Protect Function – Identity and Access Management

Account Management

We determined that 1 out of 613 separated GSA employees from October 1, 2018 through June 30, 2019 maintained an active network account past the allotted 30 days from separation. We also determined the account was not accessed after the individual's separation date on May 15, 2019.

GSA IT Security Policy CIO 2100.1L, Chapter 4: Policy for Protect Function, Section 1, Identity management, authentication and access control, page 37, states:

> "e. Disabling and removal of user accounts supporting account management processes, to include:
>
> (1) Supervisors being responsible for coordinating and arranging system access termination for all departing or resigning personnel, both Federal employees and contractors.
>
> (2) Account removal being initiated by a user's supervisor, COR, or through the review of information provided by the Office of Chief Information Security Officer (OCISO) (e.g., separation lists, role revisions). Data and system owners must verify within 30 days that separated personnel no longer maintain access to GSA IT systems or resources."

NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, page F-147, states:

> "PS-4 PERSONNEL TERMINATION
> Control: The organization, upon termination of individual employment:
> a. Disables information system access [Assignment: organization-defined time period] following the termination action; …"

The ServiceNow ticket was rejected because the supervisor did not approve the ticket within 30 days to process the account removal and the individual who opened the ServiceNow ticket was unaware that it was not processed until August 21, 2019. Without appropriate user access termination, 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.

RECOMMENDATION:

1. We recommend that GSA implement a monitoring control to review rejected ServiceNow tickets related to separated employees and contractors on a monthly basis.

3. Respond Function – Incident Response

Incident Response

Out of a population of 48 incidents reportable to US-CERT, we selected 11 incidents for testing and we determined that GSA IT did not report 2 out of the 11 incidents to US-CERT within the one hour timeframe.

GSA IT Security Procedural Guide: Incident Response (IR) CIO-IT Security-01-02 Revision 17, March 20, 2019, Section 2, Federal Incident Reporting Guidelines, page 10, states:

> "GSA will put forth a best effort to report all mandatory incidents within one-hour of notification to the GSA Incident Response Team and provide all available information. GSA will not delay reporting in order to provide further details (i.e. root cause, vulnerabilities exploited, or mitigation actions taken) as this may result in high risk to the system or enterprise. If the cause of the incident is later identified, the threat vector may be updated in a follow-up report."

For one of the incidents, the responsible party properly submitted the incident to the OIG but did not click 'submit' to US-CERT when they completed reviewing the incident. The other incident was not submitted timely to US-CERT due to a new analyst who was not familiar with the process due to lack of experience and training. Failure to properly report an incident to US-CERT in a timely manner could result in the actions to detect and protect against malicious code or other critical GSA information and systems being delayed, allowing those systems and information to be compromised.

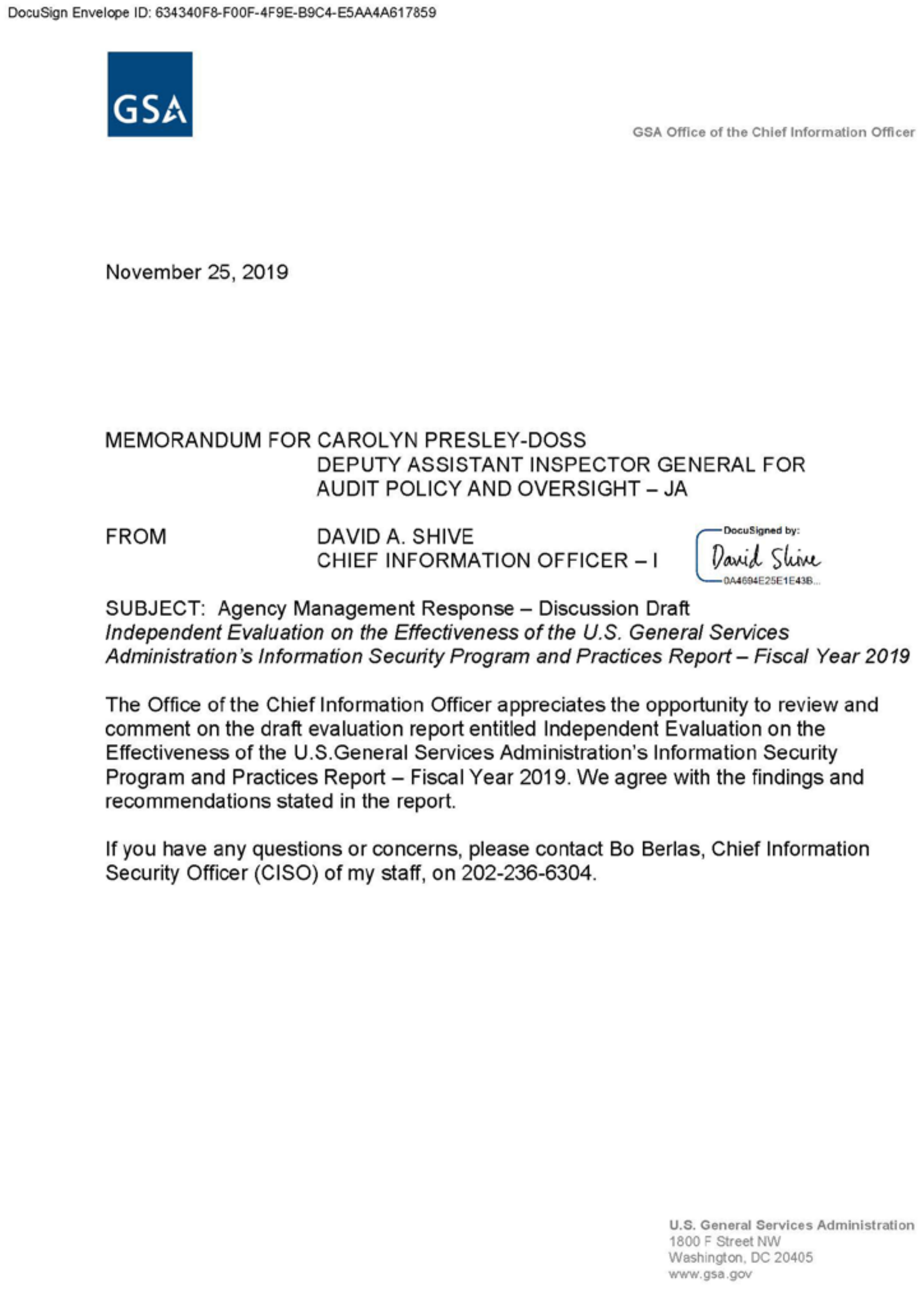
RECOMMENDATIONS:

We recommend GSA:

1. Implement a monitoring control to ensure incidents are reported timely to US-CERT.
2. Provide training to new analysts on the GSA incident reporting process, including how to submit incidents to US-CERT.

MANAGEMENT RESPONSE TO THE REPORT

The following is the GSA CIO's response, dated Month November 25, 2019, to the FY 2019 FISMA Evaluation Report.



DocuSign Envelope ID: 634340F8-F00F-4F9E-B9C4-E5AA4A617859

GSA

GSA Office of the Chief Information Officer

November 25, 2019

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

FROM
DAVID A. SHIVE
CHIEF INFORMATION OFFICER – I

DocuSigned by:
David Shive
0A4694E25E1E43B...

SUBJECT: Agency Management Response – Discussion Draft
Independent Evaluation on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2019

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 2019. We agree with the findings and recommendations stated in the report.

If you have any questions or concerns, please contact Bo Berlas, Chief Information Security Officer (CISO) of my staff, on 202-236-6304.

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

APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY

The overall objective for this FISMA evaluation was to conduct an independent evaluation of the information security program and practices of GSA to assess the effectiveness of such programs and practices for the period of October 1, 2018 to September 30, 2019. 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 2019 Inspector General FISMA Reporting Metrics; and
- Follow up on the status of prior-year FISMA findings.

We conducted our independent evaluation in accordance with the CIGIE's Quality Standards for Inspection and Evaluation and applicable AICPA standards. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe 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 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.3*, dated April 9, 2019. 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 eight information systems (six GSA information systems and two contractor information systems) from a total population of 98 major applications and general support systems as of March 1, 2019. We also performed follow-up testing on eight GSA information systems and seven GSA contractor information systems to determine if GSA had closed the prior-year findings.

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

- Inquiry 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; and
- 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 16, 2019 through September 30, 2019. During our evaluation, we met regularly 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 SPs 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 2019 FISMA evaluation:

NIST, Federal Information Processing Standard (FIPS), and/or SPs[5]

- 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)*

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

- OMB Memorandum 14-03, *Enhancing the Security of Federal Information and Information Systems*
- 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 19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security Privacy Management Requirements*
- OMB Memorandum 19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*

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*
- DHS Binding Operational Directive 18-02, *Securing High Value Assets*
- FCD-1, *Federal Continuity Directive 1*
- FY 2019 Chief Information Officer (CIO) Federal Information Security Modernization Act Metrics
- FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.3, April 9, 2019
- 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 2100.1L*, July 15, 2019
- 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 14*, February 1, 2019
- 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*, Revision 2, April 16, 2019
- 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 6, March 20, 2019
- IT Security Procedural Guide: *Termination and Transfer CIO-IT Security-03-23,* Revision 4, June 4, 2019
- 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 17, March 20, 2019
- GSA Order CIO 2100.3C, *Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities*, June 23, 2016
- GSA Order ADM 2470.2, *Occupant Emergency Plan (GSA Headquarters Building)*, November 17, 2017
- GSA Order CIO 1878.3, *Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices*, January 23, 2019
- IT Security Procedural Guide: *Vulnerability Management Process CIO-IT Security-17-80,* Initial Version, February 6, 2017
- *GSA IT General Rules of Behavior CIO 2104.1B CHGE 1*, April 2, 2019
- GSA Order CIO P 1878.1, *GSA Privacy Act Program*, September 2, 2014
- GSA Order CIO P 2180.1, *GSA Rules of Behavior for Handling Personally Identifiable Information (PII)*, October 29, 2014

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 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 and current year testing identified no findings, 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. Based on our testing we determined of the 10 prior-year findings, 5 were open and 5 were closed.

Prior Year Findings – Evaluation

Prior Year Findings – 2016 Evaluation

Finding Number	**Prior-Year Condition**	**Recommendation(s)**	**Status**
2. Contractor Systems	We determined that required reviews by the COR, ISSM, and ISSO for two contractor systems of the contractor deliverables were not provided.	2. Document the review of third party reports (SOC) [System and Organization Controls Report] 1 and or 2 reports that are provided by the contractor to include the follow up on any findings that are reported.	2. Closed
4. Identity and Access Management – Account Management	We identified a terminated application user maintained access to the system past the allotted 30 days from separation.	3. Remove terminated users from systems within the required timeframe.	3. Open – Based on our current year testing, we determined two separated application user accounts maintained access to the system past the allotted 30 days from separation.

Prior Year Findings – 2017 Evaluation

Finding Number	Prior-Year Condition	Recommendation(s)	Status
1. Identify Function – Risk Management **Contractor Systems**	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.	1. Implement a formalized review and acceptance process of contractor deliverables that includes the ISSO and ISSM review of the information, and COR acceptance of the deliverable.	1. Open – Based on our current testing one out of five systems did not document the formal review and acceptance of the deliverables.
2. Protect Function – Configuration Management **Change/Patch Management Approval**	We identified a system 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.	2. Document evidence of authorization of application changes, and operating system and database patches. Updated recommendation: Document evidence of testing and authorization of operating system patches.	2. Open – Based on our current testing of ten selected operating system patches we determined that evidence supporting the testing and authorization was not provided.
3. Protect Function – Identity and Access Management **Account Management**	We identified privileged account reviews for the operating system and database for a system were not performed in accordance with GSA policy to verify that the individuals needed privileged access.	1. Implement a formal process for approving, reviewing, and removing privileged access for the system.	1. Open – Based on our current testing we determined that the system owner did not document a formal process for removing privileged access from the system.

Finding Number	Prior-Year Condition	Recommendation(s)	Status
3. Protect Function – Identity and Access Management **Session Termination**	We determined a system's application, operating system, and database session termination configuration settings were configured to be less restrictive than the requirements in the GSA policy. Specifically, we determined the following session termination settings were configured: • Application: 60 minutes; • Operating system (Windows and Linux): session termination configuration settings not configured; and • Database: session termination configuration settings were not provided.	1. Configure the session termination settings for system in accordance with GSA policy.	1. Closed

Prior Year Findings – 2018 Evaluation

Finding Number	Prior-Year Condition	Recommendation(s)	Status
1. Identify Function – Risk Management **System Security Plan**	We determined a system's system security plan (SSP) did not include the Controls Responsibility Matrix (CRM) that identifies the fully inherited controls from the platform or PL-8 (information security architecture), a critical control required by GSA. We also determined another 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.	We recommend GSA perform the following actions: 1. Update the SSP for the system to include the CRM and reflect the NIST SP 800-53 Revision 4 security controls are fully inherited from the platform. 2. Review and update the system's SSP to reflect the current hosting environment.	1. Closed 2. Closed
1. Identify Function – Risk Management **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.	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*.	1. Closed 2. Closed

Finding Number	**Prior-Year Condition**	**Recommendation(s)**	**Status**
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.	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.	1. Closed
3. Protect Function – Identity and Access Management **Account Management**	We identified the following exceptions: a. The rules of behavior 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 Rules of Behavior 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). A system did not have a formal or periodic process to perform account recertification.	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 that new hires have completed the Rules of Behavior. 2. Compare the HR Links 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 a system. 4. Maintain evidence for the approval, review, and removal of privileged user accounts. 5. Provide training on the account management requirements for a system.	1. Closed 2. Open – See Finding 2 in the current year section of the report. 3. Closed 4. Closed 5. Closed

Finding Number	Prior-Year Condition	Recommendation(s)	Status
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.	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.	1. Closed 2. Closed 3. Closed

APPENDIX III – GLOSSARY

ACRONYM	DEFINITION
A&A	Authorization and Accreditation
AC	Access Control
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
AU	Audit and Accountability
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
COR	Contracting Officer's Representative
CM	Configuration Management
CP	Contingency Planning
CRM	Controls Responsibility Matrix
CSIP	Cybersecurity Strategy and Implementation Plan
D.C.	District of Columbia
DHS	Department of Homeland Security
FEA	Federal Enterprise Architecture
FICAM	Federated Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAO	U.S. Government Accountability Office
GSA	U.S. General Services Administration
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
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
NARA	National Archives and Records Administration
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OCISO	Office of Chief Information Security Officer
OIG	Office of Inspector General

ACRONYM	**DEFINITION**
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
PPD	Presidential Policy Direction
SOC	System and Organization Controls
SP	Special Publication
SSL	Secure Sockets Layer
SSP	System Security Plan
The Act	Title III of the E-Government Act of 2002
TIC	Trusted Internet Connections
TLS	Transport Layer Security
US-CERT	United States Computer Emergency Readiness Team