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

Independent Performance Audit on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report - Fiscal Year 2024

October 28, 2024

KPMG LLP
1801 K Street NW
Suite 12000
Washington, DC 20006

Donna Peterson-Jones
Supervisory Auditor/Contracting Officer's Representative
General Services Administration
Office of Inspector General
1800 F Street NW
Washington, DC 20405

CC: Sonya Panzo, Associate Deputy Assistant Inspector General for Auditing – Information Technology Audit Office (JA-T)

October 28, 2024

Dear Ms. Peterson-Jones,

KPMG is pleased to submit the public *Independent Performance Audit on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2024*. This report is provided to you in the format according to our contract GS-00F-275CA, order number 47HAA021F0040, modification PS0007, dated January 15, 2024, 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 Generally Accepted Government Auditing Standards and in accordance with Consulting Services Standards established by the American Institute of Certified Public Accountants, which require us to report our findings and recommendations.

Detailed within the fiscal year 2024 Federal Information Security Modernization Act of 2014 (FISMA) report are recommendations to address specific General Services Administration (GSA) entity-wide and system-level findings within the information security program and practices. When developing plans of actions and milestones or corrective actions, GSA management should assess whether these findings 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 the information system security program.

If you have any questions or concerns, please feel free to contact me at (202) 365-7214 or rdigrado@kpmg.com.

Kind regards,

Raphael S. DiGrado

Raphael DiGrado
Managing Director, Technology Assurance – Audit

INDEPENDENT PERFORMANCE AUDIT ON THE EFFECTIVENESS OF THE U.S. GENERAL SERVICES ADMINISTRATION'S INFORMATION SECURITY PROGRAM AND PRACTICES REPORT

FISCAL YEAR 2024

October 28, 2024

Executive Summary

Why We Performed This Audit

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the United States General Services Administration (GSA), to have an annual independent evaluation of their information security program and practices to determine the effectiveness of such program and practices. GSA contracted KPMG LLP ("KPMG" or "we") to conduct this audit, and the GSA Office of Inspector General monitored KPMG's work to ensure it met professional standards and contractual requirements.

We conducted a performance audit of GSA's information security program in accordance with Generally Accepted Government Auditing Standards (GAGAS) and with the Office of Management and Budget's (OMB's) most recent FISMA reporting guidance to determine the effectiveness of GSA's information security program and practices for its information systems for the period of October 1, 2023, through May 31, 2024. In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by the American Institute of Certified Public Accountants.

What We Found

Our testing for Fiscal Year (FY) 2024 included procedures at the entity and system levels for five GSA-owned information systems and five contractor-owned information systems. The FY 2024 Core and Supplemental Group 2 Inspector General (IG) Metrics (FY 2024 IG FISMA Reporting Metrics) established in the *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* dated February 10, 2023, served as the basis for our test procedures.[1]

Additionally, to support the overall performance audit objective, we also assessed management's actions for a selection of penetration test results and findings and performed internal vulnerability scanning activities over a select set of GSA-owned information systems in order to identify potential system flaws, misconfigurations, or vulnerabilities that could increase the risk of unauthorized access or elevation of privileges to GSA systems and data. This technical security testing was completed as of June 27, 2024.

Finally, we followed up on the status of four prior year findings. As a result of our procedures and based on the maturity levels calculated in CyberScope, we assessed GSA's information security program as "Effective" according to OMB guidance.[2] We made this determination based on assessing a majority of the FY 2024 IG FISMA Reporting Metrics as "Managed and Measurable" and "Optimized." Specifically, the Identify, Protect, Respond, and Recover cybersecurity functions were assessed as "Managed and Measurable," while the Detect cybersecurity function was assessed as "Optimized."

---

[1] https://www.cisa.gov/sites/default/files/2023-02/Final%20FY%202023%20-%202024%20IG%20FISMA%20Reporting%20Metrics%20v1.1_0.pdf

[2] The Department of Homeland Security uses CyberScope, a web-based application, to collect data that OMB uses to assess federal agencies' information technology (IT) security. Agencies are required to use CyberScope to submit reporting metrics, including the annual IG FISMA Metrics. IGs are also required to input an independent assessment of the overall effectiveness of their respective agency's information security program. Results for FY 2024 IG FISMA Reporting Metrics were required to be submitted in CyberScope no later than July 31, 2024.

Based on our testing, we determined that GSA implemented corrective actions to remediate two of the four prior year findings and that these findings were closed (see Appendix I). However, we determined that the other two prior year findings remained open, and also reported seven new findings (see Section IV) in the Protect cybersecurity function within the following areas:

Configuration Management

- Configuration Change Control – Lack of Approval for Operating System (OS) Patches Prior to Implementation to the Production Environment
- Flaw Remediation – Configuration, Patch, and Vulnerability Management Programs for three GSA-owned information systems Needs Improvement

Identity and Access Management

- Session Termination – Incompliant Session Termination Period Configuration Setting
- Separation of Duties – Self Approval during Application Account Reauthorization Process for one GSA-owned information system
- Account Management – Access Authorizations for New Database (DB) and OS User Access Not Documented for one GSA-owned information system

Security Training

- Specialized Training – Evidence for Specialized Training for GSA Personnel Not Consistently Completed and Tracked
- Security Training and Awareness – Weakness in Removal of Network Access for Users Not Completing Security Awareness Training

The nature of these findings impacted our assessment of certain FY 2024 IG FISMA Reporting Metrics within the Protect function, which subsequently impacted the calculated average rating of the function.

What We Recommend

We made eight recommendations related to five of the seven new findings that should strengthen GSA's information security program if effectively addressed by management.[3] GSA management should also consider whether these recommendations apply to other information systems maintained in the organization's FISMA system inventory and implement remedial action as needed.

We recommend that GSA management:

1. Enforce its defined procedures to obtain formal approval of all OS patches to three GSA-owned information systems prior to their implementation in the production environment and to retain associated supporting documentation.
2. Establish procedures and processes to enforce compliance with GSA's configuration and patching requirements on the websites for three GSA-owned information systems.
3. Properly update and remediate vulnerabilities and configuration weaknesses throughout the environments for three GSA-owned information systems in accordance with GSA and National Institute of Standards and Technology requirements.
4. Establish milestones to perform root cause analysis and remediation of reported vulnerabilities for three GSA-owned information systems, including the creation of Plans of Action and Milestones.

[3] Two of the seven Notices of Findings and Recommendations (NFRs) were issued without recommendations for the session termination and separation of duties NFRs because our testing determined that management implemented full corrective actions for the findings during the audit scope period. The NFRs were issued to report on the identified findings since they were present in the GSA IT environment during FY 2024 until remediation by management.

5. Enforce proper completion of DB and OS request forms for one GSA-owned information system to include obtaining authorizations from designated management prior to provisioning administrator access to its DB and OS, respectively.
6. Validate that access is appropriate for all DB and OS accounts on one GSA-owned information system.
7. Commit resources and implement a process to provide and formally track the completion of specialized training for GSA IT security personnel.
8. Implement an oversight process to disable access for all new users who do not complete their required Security Awareness training within the agency's defined timeframe and that is commensurate with GSA's risk appetite.

GSA management agreed with each of our findings and recommendations. The GSA Chief Information Officer's response is included in Section VI.

Contents

I. KPMG Letter

KPMG LLP
1801 K Street NW
Suite 12000
Washington, DC 20006

Administrator and Deputy Inspector General
United States General Services Administration
1800 F Street NW
Washington, DC 20405

Independent Performance Audit on the Effectiveness of the United States General Services Administration's Information Security Program and Practices Report – Fiscal Year (FY) 2024

This report presents the results of the independent performance audit of the United States General Services Administration's (GSA's) information security program and practices performed by KPMG LLP ("KPMG" or "we") for the period of October 1, 2023, through May 31, 2024. We conducted our performance audit fieldwork from March 19, 2024, through July 31, 2024. To support the overall performance audit objective, we also inspected and assessed management's actions for a selection of penetration test results and findings and performed internal vulnerability scanning activities over a select set of GSA-owned information systems in order to identify potential system flaws, misconfigurations, or vulnerabilities that could increase the risk of unauthorized access or elevation of privileges to GSA systems and data. The results of this technical testing are as of June 27, 2024.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

In addition to GAGAS, we conducted this performance audit in accordance with the Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA). This performance audit did not constitute an audit of financial statements or an attestation level report as defined under GAGAS and the AICPA standards for attestation engagements.

Consistent with the Federal Information Security Modernization Act of 2014 (FISMA) and Office of Management and Budget (OMB) requirements, the objective of this performance audit was to determine the effectiveness of GSA's information security program and practices for its information systems for the period of October 1, 2023, through May 31, 2024, in the five cybersecurity function areas outlined in the FY 2024 Core and Supplemental Group 2 Inspector General (IG) Metrics (FY 2024 IG FISMA Reporting Metrics) established in the *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* dated February 10, 2023, and to follow-up on the status of prior year findings. As a result of our procedures and based on the maturity levels calculated in CyberScope, we determined that GSA's information security program was "Effective" according to OMB guidance, as a majority of the FY 2024 IG FISMA Reporting Metrics were assessed as "Managed and Measurable" and "Optimized." Specifically, the Identify, Protect, Respond, and Recover cybersecurity functions were assessed as "Managed and Measurable," while the Detect cybersecurity function was assessed as "Optimized."

We caution that projecting the results of our audit to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

This report is intended solely for the use of GSA management, GSA Office of Inspector General, the Department of Homeland Security, and OMB and is not intended to be, and should not be, relied upon by anyone other than these specified parties.

KPMG LLP

October 28, 2024

II. Background, Objective, Scope, and Methodology

Background[4]

KPMG LLP ("KPMG" or "we") performed the Fiscal Year (FY) 2024 independent Federal Information Security Modernization Act of 2014 (FISMA) evaluation under contract with United States General Services Administration (GSA) as a performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) and Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA). The GSA Office of Inspector General (OIG) monitored our work to ensure we met professional standards and contractual requirements.

Agency Overview

GSA provides innovative solutions for federal agencies that include products, services, workspaces, and expertise to build a more high-performing, efficient, sustainable, and transparent government for the American people. The mission and strategic goals of GSA focus on four areas: real estate solutions, acquisition, digital government, and government operations. GSA helps federal agencies build and acquire office space and is referred to as the government's landlord. The organization also serves as a vehicle management and acquisition service, real estate and building management provider, information technology (IT) solutions provider, global supply chain manager, and a financial management provider. GSA's policies covering travel, property, and management practices promote effective and efficient government operations. GSA's main lines of business include the Federal Acquisition Service (FAS) and the Public Buildings Service (PBS). Various staff offices support GSA's operations in fields such as IT, legal, communications, and congressional affairs.

GSA is headquartered in Washington, D.C., and the organization employs nearly 12,000 employees nationwide across 11 regional offices. GSA has an annual contract volume of approximately $102 billion, manages over 231,000 leased vehicles, and assists tens of thousands of federal travelers through the GSA electronic travel system. Although GSA leverages billions of dollars in the marketplace, only one percent of GSA's total budget comes from direct congressional appropriations. The majority of GSA's operating costs must be recovered through the products and services it provides.

Program Overview

GSA IT, formerly known as the GSA Office of the Chief Information Officer, provides a range of services described throughout this section that enable GSA's overall mission. The GSA IT security program protects GSA systems and facilitates a successful telework program, and the GSA IT infrastructure is the backbone of GSA's business and management applications. GSA IT establishes policies and procedures that govern the use of IT across the organization and drives agency adherence consistent with government-wide guidelines published by the Office of Management and Budget (OMB). GSA IT's current strategic goals focus on customer experience, employee experience, and digital experience. Some of these goals specifically include increasing the velocity of technology transformation to deliver business value faster, advancing cybersecurity modernization, and maximizing data as a strategic asset. The GSA IT organizations are described below.

- *GSA's Chief Information Officer (CIO)*: The CIO oversees GSA IT and the entity-wide IT operations and budget to enable its alignment with strategic objectives and priorities. The CIO is responsible for oversight and governance of GSA's information security program and practices.
- *Office of the Deputy CIO:* The Deputy CIO serves as an advisor to the GSA CIO, Administrator, and other senior GSA officials on technology and data management initiatives and leads enterprise-wide

[4] The information in this section of the report is as of September 5, 2024.

modernization efforts. The Office of the Deputy CIO includes:

  - *Data to Decisions (D2D) Program:* The D2D program converts complex data into simple images and insights that are easy to understand and provides GSA users with a variety of dashboards to view, such as customer and employee survey dashboards. The D2D program also includes the Data Science Practitioner Group, which is comprised of employees from different GSA offices that work with data and provides a forum to discuss questions, share tips, and improve data practices.
  - *Office of Digital Infrastructure Technologies:* The Office of Digital Infrastructure Technologies operates GSA's IT infrastructure, software, and systems. Services provided by this office include IT help and on-site support, hardware and mobile device management, telework-related initiatives, IT Records Management, and the IT Continuity of Operations Program.
  - *Office of Acquisition IT Services:* The Office of Acquisition IT Services provides transformational system development, incremental system development, operational, and management services for FAS business applications and advises FAS leadership and program areas on IT tools that support or enhance FAS's business operations. The office is organizationally aligned with the FAS business areas to effectively deliver the IT services, systems, and functions they need. Additionally, this office provides cloud integration technology functions as a shared service for all of GSA IT.
  - *Office of Public Buildings IT Services:* The Office of Public Buildings IT Services provides enterprise solutions for GSA's real estate mission and buildings portfolio, delivers workspace IT programs, services, and solutions, and advises PBS business lines and customers on IT tools to support the government's business processes for workspaces leveraging innovative technology solutions.
  - *Office of Corporate IT Services:* The Office of Corporate IT Services provides enterprise solutions for GSA's IT systems portfolio, advises GSA's Service and Staff Offices on IT tools that support or enhance GSA's enterprise functions, and delivers IT platforms, services, and solutions for the GSA IT enterprise.

- *Office of Enterprise Data and Privacy Management:* The Office of Enterprise Data and Privacy Management seeks to continually improve data and information management, privacy, and accessibility, and focuses on managing federal materials which document the organization, functions, policies, decisions, procedures, operations, and other activities of GSA. The GSA Chief Data Officer oversees this office and its four divisions, which include: Enterprise Information & Data Management Division, Enterprise Data Governance and Privacy Division, Records and Information Management Division, and Section 508 & Accessibility Division.
- *Office of Digital Management:* The Office of Digital Management connects business and IT stakeholders and steers the planning, design, and measurement of IT solutions for GSA. This office focuses on strengthening business operations and strategy to help GSA's customers make decisions. This office includes three divisions: Policy & Investment Management Division, User Experience & Usability Division, and Portfolio Strategy & Analysis Division.
- *Office of the Chief Information Security Officer (OCISO):* The OCISO manages the GSA IT Security Office, which is responsible for the development and maintenance of the GSA IT security program. OCISO establishes and disseminates IT security policies, procedures, and guidelines which govern the use of IT across GSA. OCISO manages FISMA reporting processes and several of the control areas related to FISMA across the enterprise, such as identity and access management (IAM), flaw remediation, change management, incident response, and information security continuous monitoring.[5]

[5] IAM is interchangeable with identity, credential, and access management (ICAM).

OCISO includes five divisions:

- *Security Engineering Division* – The Security Engineering Division provides security consulting and engineering support for systems, emerging IT, and IT security initiatives. In addition, the Security Engineering Division runs GSA's Development, Security, and Operations Program to modernize security across the organization. The Security Engineering Division develops technical security standards and architectural security standards and provides software security testing in support of the GSA IT Standards process.
- *Identity, Credential, and Access Management (ICAM) Shared Service Division* – The ICAM Shared Service Division supports centralized IAM capabilities that improve coordination and governance across GSA IT and the development/delivery of enterprise certificate and key management capabilities. This division is also responsible for managing cyber supply chain risk management (SCRM) assurance for GSA IT and supports agencywide cyber SCRM activities.
- *Security Operations Division* – The Security Operations Division provides real-time operational security through security operations center and enterprise network security capabilities. This division supports IT division offices by providing vulnerability management and operational support security services at the enterprise level including managing firewalls, intrusion prevention systems, domain name systems, and security information and event management (SIEM) tools.
- *Policy and Compliance Division* – The OCISO Policy and Compliance Division provides management and maintenance of GSA Plans of Action and Milestones (POA&Ms) as well as the continuous monitoring program and security awareness and other role-based training programs. The Policy and Compliance Division also manages the processes for creating and maintaining GSA IT security policies and coordinates cybersecurity audits and the FISMA reporting processes. These efforts directly support the GSA information systems in use across the enterprise. This division periodically reports to the GSA Chief Information Security Officer (CISO) and system Authorizing Officials (AOs) to monitor the implementation of the GSA IT security program.
- *Information System Security Officer (ISSO) Support Division* – The ISSO Support Division provides support services to ISSOs and Information System Security Managers across all GSA systems and Service and Staff Offices. The ISSO Support Division facilitates the integration of IT security across other enterprise areas as well as compliance with security and privacy requirements. This division also assists the CISO and AOs during assessment and authorization processes for GSA systems.

- *Office of the Chief Technology Officer (CTO):* The Office of the CTO develops GSA's technology strategy, drives innovation, and works to improve user experiences. The vision of the Office of the CTO focuses on providing support across the organization to guide GSA IT towards adopting modern IT practices. This office includes three divisions: Digital Services Division, Solutions Strategy Division, and Service Delivery Division. The Office of the CTO also includes the following programs: Tech Radar, Tech Talks, IT Standards & Technology Approvals, and User Experience.

FISMA

On December 17, 2002, the President signed the Federal Information Security Management Act into law as part of the E-Government Act of 2002 (Public Law 107-347, Title III). The purpose of this act was to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets and provide a mechanism for improved oversight of federal agency information security programs. FISMA was amended on December 18, 2014 (Public Law 113-283). The amendment included the reestablishment of the oversight authority of the Director of the OMB with respect to agency information security policies and practices, and also set forth the authority for the Secretary of the Department of Homeland Security (DHS) to administer the

implementation of such policies and practices for information systems. FISMA requires that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including assessing the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

FISMA Inspector General Metrics and Reporting

OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), with review and feedback provided by several stakeholders including DHS and the Federal CIO and CISO Councils, released OMB Memorandum 24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, which established guidance for implementing the FY 2024 Core and Supplemental Group 2 Inspector General (IG) Metrics (FY 2024 IG FISMA Reporting Metrics).[6] The FY 2024 IG FISMA Reporting Metrics are aligned to the five information security functions outlined in the *National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), which include: Identify, Protect, Detect, Respond, and Recover. In addition, CIGIE maintained maturity models for nine FISMA metric domains: Risk Management (RM), Supply Chain Risk Management (SCRM), Configuration Management (CM), Identity and Access Management (IAM), Data Protection and Privacy (DPP), Security Training (ST), Information Security Continuous Monitoring (ISCM), Incident Response (IR), and Contingency Planning (CP).

Table 1 below illustrates the alignment of NIST Cybersecurity Framework functions to the FISMA metric domains within the FY 2024 IG FISMA Reporting Metrics.

Table 1: Alignment of NIST Cybersecurity Framework Functions to the FISMA Metric Domains

Cybersecurity Functions	FISMA Metric Domains
Identify	RM SCRM
Protect	CM IAM DPP ST
Detect	ISCM
Respond	IR
Recover	CP

Consistent with FY 2023, the FY 2024 IG FISMA Reporting Metrics were assessed using a maturity model with five levels: Ad Hoc (Level 1), Defined (Level 2), Consistently Implemented (Level 3), Managed and Measurable (Level 4), and Optimized (Level 5), as detailed in **Table 2** below.

[6] The FY 2024 IG FISMA Reporting Metrics were established in OMB's *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* dated February 10, 2023.

Table 2: IG Assessed Maturity Levels

Maturity Level	Description
Level 1: Ad Hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, and regularly updated based on a changing threat and technology landscape and business/mission needs.

The FY 2024 IG FISMA Reporting Metrics represent a continuation of the work started in FY 2022, when the IG metrics reporting process was transitioned to a multi-year cycle. The FY 2024 IG FISMA Reporting Metrics include Core Metrics and Supplemental Group 2 Metrics, as depicted in **Table 3** below.

Table 3: FY 2024 Metric Scoping

Core Metrics	Supplemental Group 2 Metrics
1. System Inventory 2. Hardware Management 3. Software Management 5. Information System Risk Governance 10. Enterprise View of Risk 14. External Products, Components, Systems, and Services 20. Secure Configuration Settings 21. Flaw Remediation 30. Non-Privileged User Multifactor Authentication (MFA) 31. Privileged User MFA 32. Least Privilege and Separation of Duties 36. Privacy Controls 37. Data Exfiltration 42. Knowledge, Skills, and Abilities 47. ISCM Strategy 49. Ongoing System Authorizations 54. Incident Detection and Analysis 55. Incident Handling 61. Business Impact Analyses 63. Contingency Testing/Exercises	4. Information System Priority 6. Information Security Architecture 15. Counterfeit Component Detection 17. CM Roles and Responsibilities 18. Enterprise-Wide CM Plan 23. Defining Change Control Activities 28. Personnel Screening 38. Data Breach Response Plan 39. Role-Based Privacy Training 44. Security Awareness Training 45. Specialized Security Training 50. ISCM Performance Measures 52. Incident Response Plan 53. IR Roles and Responsibilities 56. Sharing IR Information 62. Contingency Plans 64. System Backup and Storage

According to the FY 2024 IG FISMA Reporting Metrics, an information security program is considered effective if the overall calculated average for the program is at least Managed and Measurable (Level 4). For FY 2024 testing, a calculated average scoring model was used in which Core Metrics and Supplemental Group 2 Metrics were averaged independently to determine the maturity level for a domain and provide data points for the assessed program and function effectiveness. The calculated averages of both the Core Metrics and Supplemental Group 2 Metrics are used as data points to support the risk-based determination of overall program and function level effectiveness. Other data points considered include:

- Cybersecurity results, including system security control reviews, internal vulnerability scanning, and penetration testing conducted (by the agency) during the review period;
- The progress made by agencies in addressing outstanding IG recommendations; and
- Reported security incidents reported during the review period.

IGs should use CyberScope to calculate the maturity levels for each function and domain and then submit the results of the FY 2024 IG FISMA Reporting Metrics audit within the tool. CyberScope provides supplementary fields to allow for explanatory comments; IGs may use these fields to provide additional information supporting the FY 2024 IG FISMA Reporting Metrics audit results. The maturity levels calculated in CyberScope ultimately provide the determination for the overall effectiveness of the information security program.

Objective, Scope, and Methodology

Objective

Consistent with FISMA and OMB requirements, the objective of this performance audit was to determine the effectiveness of GSA's information security program and practices for its information systems for the period of October 1, 2023, through May 31, 2024. Specifically, we assessed GSA's performance in the five cybersecurity functions outlined in the FY 2024 IG FISMA Reporting Metrics. To support the overall performance audit objective, we also assessed management's actions for a selection of penetration test results and findings over one GSA-owned information system. In addition, we performed internal vulnerability scanning activities over three selected GSA-owned information systems. Our results for this testing are as of June 27, 2024. We conducted our fieldwork from March 19, 2024, through July 31, 2024. As part of our performance audit, we responded to the FY 2024 IG FISMA Reporting Metrics on the GSA OIG's behalf to assess maturity levels, and we also followed up on the status of prior year findings.

Scope

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation; FY 2024 IG FISMA Reporting Metrics; applicable NIST standards and guidelines, presidential directives, OMB memoranda referenced in the reporting metrics; and GSA information security policy directives. We assessed GSA's information security program as well as the implementation of program-level policies and procedures for each GSA information system selected for our testing.

We selected 10 information systems (5 GSA-owned systems and 5 contractor-owned systems) from a total population of 120 systems in the GSA FISMA system inventory as of February 13, 2024. We also performed follow-up testing over five additional GSA-owned information systems to determine whether GSA had addressed prior year findings related to those systems.

Methodology

We conducted this performance audit in accordance with GAGAS, which requires that we plan and conduct this performance audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by the AICPA. This performance audit did not constitute an audit of financial statements or an attestation level report as defined under GAGAS and the AICPA standards for attestation engagements.

We requested that GSA management provide a self-assessment of maturity levels for the FY 2024 IG FISMA Reporting Metrics to help us gain a better understanding of how the organization implemented relevant security controls and processes for the 37 metrics in scope. GSA management described policies, procedures, and control processes relevant to each metric in the self-assessment provided to us for inspection, which assisted us in requesting appropriate artifacts and meetings so that we could perform our audit procedures and conduct an independent assessment of the maturity levels.

Our procedures to assess the effectiveness of GSA's information security program and practices included the following:

- Inquiry of GSA System Owners, ISSOs, Information System Security Managers, system administrators, and other relevant control operators to walk through control processes applicable to each metric.
- Inspection of GSA information security policies, procedures, and guidelines established and disseminated by GSA IT.
- Inspection and observation of requested Provided by Client artifacts in order to determine whether GSA security control processes applicable to each metric were designed, implemented, and operating effectively across the enterprise and for the selected information systems during the audit scope period.

As discussed above, we also assessed management's actions for a selection of penetration test results and findings over one GSA-owned information system. In addition, we performed internal vulnerability scanning activities over three selected GSA-owned information systems. Our procedures for this testing included those listed above in addition to the review of web application penetration testing activities and other automated/manual testing techniques used to determine whether GSA's incident response and monitoring capabilities detected attempted suspicious activity. Our results for this testing are as of June 27, 2024.

We conducted our fieldwork from March 19, 2024, through July 31, 2024. All testing was conducted remotely through virtual walkthroughs and observations with GSA management. We also periodically met with GSA management and the GSA OIG virtually to discuss our audit progress and identified findings.

Criteria

We focused our FISMA performance audit approach on federal information security guidance developed by NIST and OMB. NIST Special Publications (SPs) establish guidelines for the development and implementation of federal security programs. We also utilized GSA's information security policy directives, which outline the organization's requirements related to information security. We included the specific criteria applicable to each finding identified in FY 2024 in the "Audit Findings and Recommendations" section of this report.

III. Overall Results

GSA established and maintained its information security program and practices for its information systems across the five cybersecurity functions and nine FISMA metric domains consistent with applicable FISMA requirements, OMB guidance, and NIST standards. Based on the ratings for each metric and associated averages calculated in CyberScope, we determined that GSA's information security program was effective. **Table 4** below depicts assessed maturity levels for each cybersecurity function.

Table 4: Maturity Levels for Cybersecurity Functions

Cybersecurity Function / Metric Domains	Assessed Maturity Level
Identify (RM and SCRM)	Managed and Measurable (Level 4)
Protect (CM, IAM, DPP, and ST)	Managed and Measurable (Level 4)
Detect (ISCM)	Optimized (Level 5)
Respond (IR)	Managed and Measurable (Level 4)
Recover (CP)	Managed and Measurable (Level 4)

Although we assessed GSA's information security program as effective, we reported seven findings within the Protect cybersecurity function. The nature of these findings impacted our assessment of certain FY 2024 IG FISMA Reporting Metrics within the Protect function, which subsequently impacted the calculated average rating of the function. **Table 5** below depicts the finding areas by function for the seven reported findings.

Table 5: Summary of Finding Areas by Cybersecurity Functions

Function	Finding Area
Protect – CM	Configuration Change Control
Protect – CM	Flaw Remediation
Protect – IAM	Session Termination
Protect – IAM	Separation of Duties
Protect – IAM	Account Management
Protect – ST	Specialized Training
Protect – ST	Security Training and Awareness

Identify

The objective of the Identify function in the NIST Cybersecurity Framework is to understand and manage cybersecurity risks to systems, people, assets, data, and capabilities within an organization. Understanding cybersecurity risks enables an agency to focus and prioritize efforts consistent with its risk management strategy and business needs. This function is carried out through proper RM and SCRM processes.

Risk Management (RM)

FISMA requires federal agencies to establish an information security program that protects the systems, data, and assets commensurate with their risk environment. RM is the process of identifying, assessing, and controlling threats to an organization's operating environment. These threats or risks could stem from various sources, including budget uncertainty, natural disasters, and cybersecurity threats. A sound risk

management plan and program that addresses the various risks can aid an agency in establishing an information security program.

Based on the results of our audit procedures, we determined that GSA management implemented policies and procedures to maintain a complete and accurate inventory of its major information systems by using a Governance, Risk, and Compliance (GRC) platform to store and manage system security information (e.g., accreditation status, system type, and ownership). GSA also implemented a suite of security tools to maintain an inventory of hardware devices connected to the GSA network and to track software assets and their associated licenses.

GSA management developed and implemented processes for assessing and authorizing information systems, performing risk assessments, developing and implementing secure architecture, and tracking and monitoring POA&Ms. These processes allow GSA stakeholders to identify, manage, and track cybersecurity risks that the OCISO incorporates into GSA's overall risk register. GSA management also utilized dashboards to analyze data from implemented security tools related to risks and vulnerabilities that impacted GSA information systems.

However, we did note that two prior year findings related to GSA's POA&M management remained open during FY 2024. Specifically, we noted that certain entity-wide and system-level POA&Ms were not updated timely in accordance with the defined process. We also noted that a system-level POA&M had not been developed for a control implementation gap that was identified in the system security plan (SSP) for one GSA-owned information system as required.

Supply Chain Risk Management (SCRM)

SCRM requires agencies to develop policies, procedures, and programs to manage supply chain risks associated with system development, acquisition, maintenance, and disposal. This includes monitoring third-party vendors and service providers and helping to ensure appropriate contractual requirements are included for acquisitions.

Based on the results of our performance audit procedures, we determined that GSA management created an SCRM Executive Board responsible for enterprise-wide governance and established SCRM policies and procedures. GSA management also implemented tools to monitor critical supplier risks and SCRM events. GSA management also developed detailed guides for monitoring contractor-owned information systems. This included the use of GSA's GRC platform to monitor and review information security monitoring deliverables. We did not report any findings related to GSA's SCRM program and associated security controls.

Protect

The objective of the Protect function in the NIST Cybersecurity Framework is to develop and implement appropriate safeguards to enable the delivery of critical services of organizations. The Protect function supports organizations' ability to limit, contain, or prevent the impact of a cybersecurity event. This function is carried out through proper CM, IAM, DPP, and ST processes.

Configuration Management (CM)

FISMA requires agencies to develop an information security program that includes policies and procedures to help ensure compliance with minimally acceptable system security configuration requirements. CM refers to processes used to control changes/patches to information systems (i.e., change management and patch management) to establish and maintain the integrity of the systems and their underlying data.

Based on the results of our audit procedures, we determined that GSA management developed and implemented a CM plan and holds stakeholders accountable for carrying out CM roles and responsibilities. Changes to GSA information systems, including program changes, configuration changes, patches, and emergency changes, are required to be documented, tested, and approved prior to implementation in the production environment in accordance with defined configuration control processes. GSA management also established processes to monitor the IT environment for unauthorized system changes and for compliance with baseline configurations and secure configuration settings. Compliance is monitored across the enterprise through tools at least biweekly, and the results are reported to relevant stakeholders.

Additionally, we determined that GSA management established processes related to flaw remediation, including asset discovery and vulnerability scanning across the enterprise. Vulnerability scan results are reviewed by management at defined frequencies, and vulnerabilities must be remediated within established timeframes or tracked in POA&Ms through resolution.

However, we reported two findings related to GSA's patch management and flaw remediation processes for certain selected GSA-owned information systems. Specifically, we noted that approvals for operating system (OS) patches were not documented prior to implementation in the production environment for two GSA-owned information systems. Further, we noted that GSA did not timely remediate or create POA&Ms for moderate and low vulnerabilities identified for three GSA-owned information systems in accordance with GSA policy. These findings impacted our assessed maturity ratings for the associated metrics, and, therefore, impacted our overall assessment of GSA's CM program.

Identity and Access Management (IAM)

IAM requirements dictate that agencies implement capabilities to help ensure that information system users can only access data required for their job functions (i.e., "need-to-know"), in accordance with the principles of separation of duties and least privilege. Aspects of the IAM program include screening personnel, issuing and maintaining user credentials, and managing logical and physical access rights.

Based on the results of our audit procedures, we determined that GSA management defined and tracked performance measures related to the effectiveness of the IAM program. Additionally, we determined that GSA management utilized tools to implement the IAM program. These tools were used to enforce multi-factor authentication, manage user accounts and monitor their behavior, and retain access authorization documentation. GSA processes related to access agreements, privileged and non-privileged user multi-factor authentication, and remote access operated effectively during the period.

However, we reported three findings related to GSA's account management processes for certain selected GSA-owned information systems. Specifically, we observed that the session termination setting for one GSA-owned information system did not comply with GSA policy. As a result, the duration of open privileged account sessions was not adequately restricted. We also noted that two users with access to one GSA-owned information system reviewed their own access during the annual access review and reauthorization process, which was not in keeping with the principles of separation of duties and least privilege. Further, we noted that authorization was not documented for five database (DB) users and one OS user granted access to one GSA-owned information system during the performance audit period. These findings impacted our assessed maturity ratings for the associated metrics, and, therefore, impacted our overall assessment of GSA's IAM program.

Data Protection and Privacy (DPP)

DPP refers to a collection of activities focused on preserving the confidentiality, integrity, and availability of information systems and their underlying data through proper access restrictions and protections against

unauthorized disclosure of information. Effectively managing risks associated with the creation, collection, use, maintenance, dissemination, disclosure, and disposal of personally identifiable information (PII) depends on the safeguards in place for the information systems that process, store, and transmit this information. OMB Circular A-130, *Managing Information as a Strategic Resource,* requires federal agencies to develop, implement, and maintain enterprise-wide privacy programs that align with the NIST Risk Management Framework to protect PII and other sensitive data. The head of each federal agency is ultimately responsible for managing PII and ensuring that privacy is protected for their agency. Executive Order 13719, *Establishment of the Federal Privacy Council,* requires agency heads to designate a Senior Agency Official for Privacy who has agency-wide responsibility and accountability for the agency's privacy program.

Based on the results of our audit procedures, we determined that GSA management implemented a privacy program and related security controls, such as those related to encryption and media sanitization, to protect PII and other sensitive data. GSA management utilized tools to implement security and privacy controls and monitor the network for data leaks.

GSA management also performed data exfiltration exercises to assess the effectiveness of enhanced network defenses and data breach response procedures. Further, GSA management implemented a role-based privacy training program that incorporated feedback and lessons learned from key stakeholders to improve the program's effectiveness. We did not report any findings related to GSA's DPP program and associated security controls.

Security Training (ST)

ST is a cornerstone of a strong information security program, as it helps prepare both privileged and non-privileged information systems users to limit exposure of GSA systems and data to unnecessary risk while performing their job duties.

Based on the results of our audit procedures, we determined that GSA management implemented an effective security awareness training program, which included simulated phishing exercises to assess information system users' ability to identify and prevent attempts to obtain sensitive information through social engineering attacks. Performance measures to assess the effectiveness of the program, such as metrics related to training completion and successful simulated phishing attempts, were established and tracked across the enterprise. GSA management also performed detailed workforce assessments and addressed gaps in the knowledge, skills, and/or abilities of program staff through talent acquisition and training. During our performance audit fieldwork, we found that GSA employees had a training level that effectively reduced the number of security incidents caused by personnel throughout the tested period.

However, we reported two findings related to GSA's entity-wide security training program. Specifically, we noted that GSA did not provide specialized role-based security training to individuals with significant security responsibilities during the audit scope period. Further, we noted that two selected GSA system users did not complete security awareness training within the required timeframe, and the users' network access was not disabled after the deadline as required by GSA policy. These findings impacted our assessed maturity ratings for the associated metrics, and therefore impacted our overall assessment of GSA's ST program.

Detect – Information Security Continuous Monitoring (ISCM)

The objective of the Detect function in the NIST Cybersecurity Framework focuses on the timely discovery of cybersecurity events. This function is critical to a robust information security program as the effects of

cybersecurity events can be mitigated more quickly if they are identified in a timely manner. The NIST Cybersecurity Framework states that ISCM processes should be used to detect anomalies and continuously monitor information systems across the enterprise to identify events. The Detect function is carried out through ISCM tools and processes intended to promote timely identification of cybersecurity events.

To further enhance federal agencies' ISCM capabilities, Congress established the Continuous Diagnostics and Mitigation (CDM) Program in 2012. The CDM Program supports agency efforts to identify and prioritize cybersecurity risks on an ongoing basis based on potential impact.

Based on the results of our audit procedures, we determined that GSA management implemented an enterprise-wide SIEM platform as well as ISCM and CDM dashboards to collect and analyze data related to the agency's security posture on a near real-time basis. GSA management also established effective security Assessment and Authorization processes to authorize information systems and periodically assess the implementation of required security controls. Additionally, GSA management implemented an enterprise-wide ongoing authorization program to maintain a continuous Authorization to Operate status for the GSA systems enrolled in the program. We did not report any findings related to GSA's ISCM program and associated security controls.

Respond – Incident Response (IR)

The objective of the Respond function in the NIST Cybersecurity Framework is to develop and implement actions to be taken when a cybersecurity event has been detected. Such actions include the establishment of proper IR plans and procedures to be executed during and after incidents, analysis to determine the impact of incidents and mitigation to contain (i.e., prevent expansion) and resolve incidents, managing communications with relevant stakeholders during and after incidents, and incorporating lessons learned into the incident response program. FISMA requires agencies to document and implement an enterprise-wide IR program.

Based on the results of our audit procedures, we determined that GSA management implemented an effective IR program through the execution of IR plans and procedures and the use of advanced IR tools, including the enterprise-wide SIEM platform. These tools provided GSA management with a centralized view of incident response activities on a near real-time basis and facilitated risk-based prioritization decisions as well as the timely containment and resolution of incidents. These tools also offered reporting capabilities to streamline communication of IR activities to relevant stakeholders in accordance with the channels defined in IR plans and procedures.

GSA management utilized its threat vector taxonomy to classify incidents and report associated IR metrics to the United States Computer Emergency Readiness Team in accordance with DHS guidelines. Additionally, GSA management used insights provided by IR tools to prevent or limit the impact on other systems, where applicable. We did not report any findings related to GSA's IR program and associated security controls.

Recover – Contingency Planning (CP)

The objective of the Recover function in the NIST Cybersecurity Framework is to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident or other disaster. Activities that are part of this function, such as developing and testing contingency plans, support timely recovery to normal operations and reduce the impact from an incident or disaster.

Based on the results of our audit procedures, we determined that GSA management established processes to define mission essential functions across the enterprise and to develop, maintain, update, and test contingency plans and associated documentation, including business impact analyses and disaster recovery plans. GSA management also established processes to report recovery activities to relevant stakeholders and to incorporate lessons learned into the CP program. We did not report any findings related to GSA's CP program and associated security controls.

IV. Audit Findings and Recommendations

Protect – CM – Configuration Change Control

GSA IT's controls to formally approve OS patches prior to implementation into the production environment did not operate effectively on a consistent basis. Specifically, we noted the following:

- Of the five patches to one GSA-owned information system selected for testing and the five OS patches to another GSA-owned information system selected for testing, all patches were implemented in the production environment without required and documented approvals.
- One of the four OS patches to one GSA-owned information system selected for testing was implemented in the production environment without required and documented approvals.

The following criteria support the noted condition:

GSA *IT [Digital Innovation for GSA Infrastructure Technologies] Change Management (ChM) Plan,* dated February 26, 2023, Section 5.1.1.1 ([Engineering Review Board] Review Criteria and Disposition) states:

> **5.1.1.1 Change Request Review Criteria**
> [Engineering Review Board] voting members will perform a high-level review to verify compliance with these change request criteria:
>
> - Change requests are accurately documented.
> - The designated risk, impact, and priority fields align with the scope and complexity of the change request.
> - A valid business justification for performing the change is presented (e.g., proposed changes are in support of approved projects or are needed to resolve documented incidents or problems that have been identified in the environment).
> - Change requests adhere to standard schedules when applicable or are appropriately scheduled with stakeholders.
> - Change Owners have reviewed changes with appropriate stakeholders (e.g., technical points of contact, application/system owners, etc.) and conducted a thorough technical review (by and for) areas impacted by the change has been conducted.
> - Appropriate communication for stakeholders and end users has been planned and prepared in coordination, when appropriate, with the Communications Team.
> - Proposed changes have been tested in a non-production environment if possible.
> - Updated management documents (e.g., Business Process Document) have been included.
> - Back-out plans are well documented for each change that will ensure restoration of the previous level of service should a change not complete as intended or provide the desired outcome.
> - Service validation steps are documented to ensure that the successful or unsuccessful implementation of a change has not adversely impacted other services and that the implemented change is operating as intended.
> - Identification of supporting resources is understood, agreed upon, and planned for to ensure the successful implementation of a change.
> - Correlation to precipitating drivers is identified (e.g., [Change Style Indicator], Problem Ticket, Risk item).

The Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government*, GAO-14-704G, dated September 2014, states:

> Design of Appropriate Types of Control Activities, 10.03,
> […]

Appropriate documentation of transactions and internal control. Management clearly documents internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination.
[…]
Documentation and records are properly managed and maintained.

GSA *IT Security Procedural Guide: Configuration Management (CM) CIO-IT Security-01-05*, Revision (Rev.) 5, dated March 1, 2022, Section 4.3 (CM-3 Configuration Change Control) states:

Control:

a. Determine and document the types of changes to the system that are configuration-controlled;
b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
c. Document configuration change decisions associated with the system;
d. Implement approved configuration-controlled changes to the system;
e. Retain records of configuration-controlled changes to the system for [five years for configuration-controlled items, or longer if deemed necessary by GSA [System Owner] or Contractor and approved by the GSA CISO and AO];
f. Monitor and review activities associated with configuration-controlled changes to the system; and
g. Coordinate and provide oversight for configuration change control activities through [a defined CM approval process (example: a charted Configuration Change Board)] that convenes [on a defined basis in support of the system's CM requirements to approve changes such as:
    - Upgrades and modifications to the information system or its components
    - Changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers)
    - Emergency changes required to address an immediate issue
    - Changes to remediate flaws].

This condition occurred because approvals for OS patches to two GSA-owned information systems were verbally communicated during the testing and development phases. The patches to another GSA-owned information system were being retroactively tracked after the new approval process was implemented. Furthermore, several required approvals for one GSA-owned information system were provided through an approved messaging application and, due to GSA policy, were not retained.

Without implementing effective configuration management controls, the risk increases that unauthorized patches could be implemented into the production environment, which could introduce system issues or malicious code into the OS environments without detection. This also increases the risk that the confidentiality, integrity, and availability of the data residing on the information system could be compromised.

RECOMMENDATION:

We recommend that GSA management enforce its defined procedures to obtain formal approval of all OS patches to three GSA-owned information systems prior to their implementation in the production environment and to retain associated supporting documentation.

Protect – CM – Flaw Remediation

GSA management's control for tracking and remediating website-based vulnerabilities for configuration and patch management requirements within three GSA-owned information systems were not consistently implemented. Specifically, GSA management has not timely remediated vulnerabilities identified during website scans or created POA&Ms to track remediation activities. Specifically, we noted a total of 106 (9 medium and 97 low risk) vulnerabilities:

- 45 for one GSA-owned information system (6 medium, and 39 low risk),
- 40 for one GSA-owned information system (3 medium, and 37 low risk), and
- 21 for one GSA-owned information system (21 low risk).

The following criteria support the noted condition:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Rev. 5, Release 5.1.1, dated November 2023, states:

RA-5 Vulnerability Monitoring and Scanning
Control:

a. Monitor and scan for vulnerabilities in the 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 are identified and reported;
b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;
c. Analyze vulnerability scan reports and results from vulnerability monitoring;
d. Remediate legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk;
e. Share information obtained from the vulnerability monitoring process and control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other systems (i.e., systemic weaknesses or deficiencies).

SI-2 Flaw Remediation
Control:

a. Identify, report, and correct system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Install security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and
d. Incorporate flaw remediation into the organizational configuration management process […].

GSA IT Security Procedural Guide: Vulnerability Management Process CIO-IT Security-17-80, Rev. 4, dated March 13, 2023, Section 3.1 (Implementation of NIST Controls) states:

> GSA systems must implement NIST controls RA-5, Vulnerability Monitoring and Scanning, and SI-2(3), Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions, in accordance with the frequencies and timelines established in the control statements and parameters as indicated below (only the parts of RA-5 and SI-2(3) that address frequencies or timelines are listed).

RA-5:

a. Monitor and scan for vulnerabilities in the system and hosted applications [weekly authenticated scans for OS – including DBs, monthly unauthenticated scans for web application, annual authenticated scans for web applications] and when new vulnerabilities potentially affecting the system are identified and reported; […]
d. Remediate legitimate vulnerabilities [
    1. [Binding Operational Directive] Timelines
        a. Within 14 days for vulnerabilities added to [Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA)] [Known Exploited Vulnerabilities (KEV)] Catalog with a [Common Vulnerabilities and Exposures (CVE)] date post FY21.
        b. Per the CISA KEV catalog date or GSA Standard timelines below, whichever is earlier, for vulnerabilities in the CISA KEV catalog with a CVE date in FY21 or earlier.
        c. Within 15 days for Critical (Very High) vulnerabilities for Internet-accessible systems or services.
    2. GSA Standard Timelines
        a. Within 30 days for Critical (Very High) and High vulnerabilities.
        b. Within 90 days for Moderate vulnerabilities.
        c. Within 120 days for Low vulnerabilities for Internet-accessible systems/services.] in accordance with an organizational assessment of risk.

SI-2(3):

b. Establish the following benchmarks for taking corrective actions: [
    1. [Binding Operational Directive] Timelines
        a. Within 14 days for vulnerabilities added to CISA's KEV Catalog with a CVE date post FY21.
        b. Per the CISA KEV catalog date or GSA Standard timelines below, whichever is earlier, for vulnerabilities in the CISA KEV catalog with a CVE date in FY21 or earlier.
        c. Within 15 days for Critical (Very High) vulnerabilities for Internet-accessible systems or services.
    2. GSA Standard Timelines
        a. Within 30 days for Critical (Very High) and High vulnerabilities.
        b. Within 90 days for Moderate vulnerabilities.
        c. Within 120 days for Low vulnerabilities for Internet-accessible systems/services.].

This condition occurred because GSA management did not remediate or track previously identified website application vulnerabilities due to their severity and engineering cycles. Thus, the vulnerabilities identified receive lower priority compared to critical and high findings.

As security updates are released to mitigate the risk of vulnerabilities affecting web applications, a lack of timely implementation of these security patches and updates increases the risk of potentially compromising the confidentiality, integrity, and availability of the data residing on the three GSA-owned information systems. Without a consistent process for remediating vulnerabilities in the environments for these three GSA-owned information systems, there is an increased risk that web application flaws could expose the web applications to attacks, unauthorized modification, or data being compromised. Further, not prioritizing the resolution of known findings may result in the findings continuing in future years.

RECOMMENDATIONS:

We recommend that GSA management:

1. Establish procedures and processes to enforce compliance with GSA's configuration and patching requirements on the websites for three GSA-owned information systems.
2. Properly update and remediate vulnerabilities and configuration weaknesses throughout the environments for three GSA-owned information systems in accordance with GSA and NIST requirements.
3. Establish milestones to perform root cause analysis and remediation of reported vulnerabilities for three GSA-owned information systems, including the creation of POA&Ms.

Protect – IAM – Session Termination

GSA management did not consistently implement the session termination control across GSA IT in accordance with GSA's IT security policy and procedures. Specifically, the session termination setting for one GSA-owned information system was configured to 120 minutes, whereas the GSA IT security policy requirement is 30 minutes.

The following criteria support the noted condition:

GSA Order CIO 2100.1P, *GSA Information Technology (IT) Security Policy*, dated January 31, 2024, Chapter 4 (Policy for Protect Function), states:

> [Federal Information Processing Standard (FIPS)] 199 Moderate and High systems must terminate user sessions regardless of user activity:
> 1. After 30 minutes of inactivity.
> 2. Thirty days for systems at [Authenticator Assurance Level (AAL)] 1.
> 3. Twelve hours for systems at AAL2 and AAL3.

GSA *IT Security Procedural Guide: Access Control (AC) CIO-IT Security-01-07*, Rev. 6, dated May 14, 2024, Section 3.11 (AC-12 Session Termination) states:

> Control: Automatically terminate a user session after [
> 1. 30 minutes of inactivity
> 2. The following timeframes, regardless of user activity:
>   a. Thirty (30) days for systems at AAL1.
>   b. Twelve (12) hours for systems at AAL2 and AAL3. […]].

GSA *IT Security Procedural Guide: Vulnerability Management Process CIO-IT Security-17-80*, Rev. 4, dated March 13, 2023, Section 5.4.2 ([Configuration Settings Management (CSM)] Compliance Reporting) states:

> A FISMA system's compliance with CSM requirements is regularly reported to executives. A FISMA system will be reported as non-compliant with CSM requirements if any GSA Operating System benchmark within the FISMA System is reporting under 85% compliance.

This condition occurred because the management team for the GSA-owned information system was not aware of the 30-minute session termination requirement and had improperly configured the setting to 120 minutes. Also, per GSA policy, the GSA IT baseline configuration compliance scans pass with a score of 85 percent or higher. As a result, the compliance scan indicated that the GSA-owned information system passed even though it had an improper configuration setting for session terminations.

Invalid or inappropriate session terminations may result in less secure web application sessions with more exposure and risk to external threats and vulnerabilities, which could adversely impact GSA systems and data.

RECOMMENDATION:

GSA management remediated the identified condition as of April 30, 2024; therefore, this finding was issued without an associated recommendation.

Protect – IAM – Separation of Duties

For the FY 2024 annual application user's reauthorization for one GSA-owned information system, two of 180 users reviewed and approved their own access, which is not in accordance with separation of duties principles.

The following criteria support the noted condition:

GSA Order CIO 2100.1P, *GSA Information Technology (IT) Security Policy,* dated January 31, 2024, Chapter 2 (Security Roles and Responsibilities) states:

n. Providing guidance or input for periodic assessments of [Service and Staff Offices] including Regional Offices security measures and goals to assure implementation of GSA policy and procedures.

GSA *IT Security Procedural Guide: Access Control (AC) CIO-IT Security-01-07*, Rev. 6, dated May 14, 2024, Section 3.6 (AC-06 Least Privilege) states:

(07) Least Privilege | Review of User Privileges. FIPS 199 Moderate and High systems

a. Review [annually as part of the annual account review (per AC-02j)] the privileges assigned to [all roles and users] to validate the need for such privileges; and
b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Rev. 5, Release 5.1.1, dated November 2023, states:

AC-5 Separation of Duties
Control:

a. Identify and document [*Assignment: organization-defined duties of individuals requiring separation*]; and
b. Define system access authorizations to support separation of duties.

This condition occurred because the management team for the GSA-owned information system did not consider the risk of having two users, who were responsible for the application access review process, to reauthorize their own access.

Ineffective user access reviews increase the risk that inappropriate activities or inappropriate access to the system may occur without management's awareness. This may increase the risk of unauthorized modification, destruction, or exposure of critical data for the GSA-owned information system.

RECOMMENDATION:

GSA management remediated the identified condition as of April 30, 2024; therefore, this finding was issued without an associated recommendation.

Protect – IAM – Account Management

GSA management did not document its access authorization for five of five sampled new DB users and one of two sampled new OS users with access to the DB and OS supporting one GSA-owned information system, which did not adhere to GSA IT Security Procedural Guide: Access Control (AC). Specifically, an access request ticket for one DB sample user could not be located, two DB users did not have access request tickets tracked, and five DB users and one OS user did not have an approval date tracked in their access request tickets.

The following criteria support the noted condition:

GSA *IT Security Procedural Guide: Access Control (AC) CIO-IT Security-01-07*, Rev. 6, dated May 14, 2024, Section 3.2 (AC-02 Account Management) states:

> Control:
> […]
> d. Specify:
> 1. Authorized users of the system;
> 2. Group and role membership; and
> 3. Access authorizations (i.e., privileges) and [the following attributes as defined in the user role(s) matrix in GSA [System Security and Privacy Plan] Template Section 9: Types of Users – Internal or External; Privileged, Non-Privileged, or No Logical Access; Sensitivity Level; Authorized Privileges; Functions Performed; MFA Authentication Method] for each account;
> e. Require approvals by [designated account managers as specified in AC-02.b] for requests to create accounts; and
> f. Create enable, modify, disable, and remove accounts in accordance with [CIO-IT Security-01-01, Identification and Authentication, CIO-IT Security-01-07, Access Control, and GSA-defined procedures or conditions (as applicable)] […].

The GAO *Standards for Internal Control in the Federal Government*, GAO-14-704G, dated September 2014, states,

> Design of Appropriate Types of Control Activities, 10.03,
> […]
> Appropriate documentation of transactions and internal control. Management clearly documents internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination.
> […]
> Documentation and records are properly managed and maintained.

This condition occurred because GSA management did not consider properly documenting its access authorization process for users. GSA management informed us that approvals for new users were provided verbally through meetings or via Google Chat and therefore no documentation was created.

Not obtaining appropriate approval for new access increases the risk that unauthorized access could be permitted, which increases the opportunity for the confidentiality, integrity, and availability of the data residing on the GSA-owned information system to be compromised.

RECOMMENDATIONS:

We recommend that GSA management:

1. Enforce proper completion of DB and OS request forms for one GSA-owned information system to include obtaining authorizations from designated management prior to provisioning administrator access to its DB and OS, respectively; and
2. Validate that access is appropriate for all DB and OS accounts on one GSA-owned information system.

Protect – ST – Specialized Training

GSA management's control to provide and track required specialized training for GSA IT security personnel was not consistently implemented. Specifically, GSA management could not provide supporting documentation evidencing completion of specialized training for all GSA Information Security personnel. As a result, we were unable to assess whether GSA removed the respective system access of GSA IT security personnel who did not complete required specialized training in accordance with GSA IT security policy. Further, management did not disable network access to users who were required to complete specialized training but did not, in accordance with GSA policy.

The following criteria support the noted condition:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Rev. 5, Release 5.1.1, dated November 2023, states:

> **AT-3 Role-Based Training**
> Control:
> a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [*Assignment: organization-defined roles and responsibilities*]:
> 1. Before authorizing access to the system, information, or performing assigned duties, and [*Assignment: organization-defined frequency*] thereafter; and
> 2. When required by system changes.
>
> **AT-4 Training Records**
> Control:
> a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and
> b. Retain individual training records for [*Assignment: organization-defined time period*].

5 Code of Federal Regulation 930.301, *Information Systems Security Awareness Training Program*, last amended July 2024, states:

> Each Executive Agency must develop a plan for Federal information systems security awareness and training and:
> a. Identify employees with significant information security responsibilities and provide role-specific training in accordance with NIST standards and guidance available on the NIST Web site, http://csrc.nist.gov/publications/nistpubs/, as follows:
>
> […]
>
> 4. CIOs, IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.
> 5. IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.

GSA Order CIO 2100.1P, *GSA Information Technology (IT) Security Policy,* dated January 31, 2024, Chapter 2 (Security Roles and Responsibilities) states:

> The GSA [Senior Agency Official for Privacy] directs the planning and implementation of the GSA Privacy Program to ensure agency personnel, including contractors, receive appropriate privacy awareness training based on their roles and access to privacy data.
>
> The GSA CISO directs the planning and implementation of the GSA IT Security Awareness Training Program to ensure agency personnel, including contractors, receive appropriate security awareness training based on their roles and access to information and information systems.
>
> The [Supervisor] conducts annual reviews of staff training records to ensure annual IT Security and Privacy Awareness Training, and application specific training has been completed for all users. The records shall be forwarded to ISSOs/System Owners as part of the annual recertification efforts.

Chapter 4 (Policy for Protect Function) states:

a. All GSA employees and contractors, as appropriate given their role and security responsibilities, must adhere to training requirements in GSA CIO-IT Security-05-29: Security and Privacy Awareness and Role Based Training Program.
b. Failure to comply with annual awareness and specialized IT security training requirements will result in termination of access to the GSA enterprise and applications. AOs can terminate system accounts.
c. All personnel must complete initial Controlled Unclassified Information (CUI) awareness training within 60 days of employment, plus refresher training at least every two years thereafter.
d. GSA employees and contractors on the Incident Response Team identified in GSA CIO-IT Security-01-02 must be trained on their roles and responsibilities within 60 days of assignment and annually thereafter.
e. Personnel with contingency planning responsibilities must be trained in their contingency roles and responsibilities with respect to the information system annually.

GSA *IT Security Procedural Guide: Security and Privacy Awareness and Role Based Training Program CIO-IT Security-05-29,* Rev. 8, dated May 23, 2023, Section 3.1.3 (Compliance with Mandatory Training Requirements) states:

> Demonstrating mastery of the topics listed in Appendix A: is required to maintain network access. Failure to complete the required training or "test-out" from the required training will result in loss of network access.
>
> This enforcement action also applies to new users; failure to satisfy the mandatory training requirement will result in loss of access to the GSA Enterprise network.

Section 4.2 (Role-Based Training) states:

> The OCISO and Chief Privacy Officer provide specialized role-based training on a regular basis. This training is open to all GSA personnel with the responsibility to manage, operate, or authorize operations for a GSA system. Topics are selected based on emerging technologies, IT security policies and procedures, input from team member surveys, and documentation changes that impact the group. These training sessions can be used to satisfy role-based training requirements.

This condition occurred because privileged user training was reprioritized given competing priorities.

The absence of supporting documentation for specialized training of GSA IT security personnel creates a risk of non-compliance with federal standards and GSA policy, potentially resulting in unqualified personnel handling sensitive data. This could further lead to inadequate security measures, increasing the likelihood of data breaches, and potentially damaging the GSA's reputation and operational efficiency.

RECOMMENDATION:

We recommend that GSA management commit resources and implement a process to provide and formally track the completion of specialized training for GSA IT security personnel.

Protect – ST – Security Training and Awareness

GSA IT management's control to complete the required Security Awareness training for all new GSA personnel was not consistently implemented. Specifically, for two of 25 sampled users, GSA IT management did not disable network access for new users who did not complete the training by the required due date. Further, both individuals completed the trainings between 9 and 22 days after the required due dates.

The following criteria support the noted condition:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Rev. 5, Release 5.1.1, dated November 2023, states:

> **AT-2 Literacy Training and Awareness**
> Control:
> a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
> 1. As part of initial training for new users and [*Assignment: organization-defined frequency*] thereafter; and
> 2. When required by system changes or following [*Assignment: organization-defined events*] […].

GSA Order CIO 2100.1P, *GSA Information Technology (IT) Security Policy,* dated January 31, 2024, Section 4.2 (Awareness and Training) states:

a. All GSA employees and contractors, as appropriate given their role and security responsibilities, must adhere to training requirements in GSA CIO-IT Security-05-29: Security and Privacy Awareness and Role Based Training Program.
b. Failure to comply with annual awareness and specialized IT security training requirements will result in termination of access to the GSA enterprise and applications. AOs can terminate system accounts.
c. All personnel must complete initial CUI awareness training within 60 days of employment, plus refresher training at least every two years thereafter.

GSA *IT Security Procedural Guide: Security and Privacy Awareness and Role Based Training Program CIO-IT Security-05-29*, Rev. 8, dated May 23, 2023, Section 3.1.3 (Compliance with Mandatory Training Requirements) states:

> Demonstrating mastery of the topics listed in Appendix A: is required to maintain network access. Failure to complete the required training or "test-out" from the required training will result in loss of network access.
>
> This enforcement action also applies to new users; failure to satisfy the mandatory training requirement will result in loss of access to the GSA Enterprise network.

This condition occurred because the two new users should have been disabled for incompletion of the Security Awareness training but were not disabled due to the retirement of the process practitioner. Additionally, per GSA IT management's risk assessment, management identified the gap as a low-risk area compared to other competing priorities.

By not disabling access for users who do not complete their required Security Awareness training may increase the risk that unauthorized access could be permitted, potentially resulting in unqualified personnel

handling sensitive data. This could further lead to inadequate security measures, increasing the likelihood of data breaches, and potentially damaging the GSA's reputation and operational efficiency.

RECOMMENDATION:

We recommend that GSA management implement an oversight process to disable access for all new users who do not complete their required Security Awareness training within the agency's defined timeframe and that is commensurate with GSA's risk appetite.

V. Conclusions

GSA management established and maintained its information security program and practices for its information systems for the five cybersecurity functions and nine FISMA metric domains during FY 2024. We assessed GSA's information security program as "Effective" within CyberScope; this determination was made because the majority of the FY 2024 IG FISMA Reporting Metrics and the associated calculated averages for the metric domains and cybersecurity functions were assessed as "Managed and Measurable" or "Optimized." Specifically, the Identify, Protect, Respond, and Recover cybersecurity functions were assessed as "Managed and Measurable," while the Detect cybersecurity function was assessed as "Optimized." We also performed follow-up testing to determine the status of four prior year findings and reported that two of the four findings were closed (see Appendix I). However, we determined that the other two prior year findings remained open, and also reported seven new findings that impacted the Protect cybersecurity functions and the CM, IAM, and ST FISMA metric domains. The nature of these findings impacted our assessment of certain FY 2024 IG FISMA Reporting Metrics within the Protect function, which subsequently impacted the calculated average rating of the function.

We made eight recommendations related to five of the seven new findings that should strengthen GSA's information security program if effectively addressed by management. GSA management should also consider whether these recommendations apply to other information systems maintained in the organization's FISMA system inventory and implement remedial action as needed. In a written response, GSA management agreed with our findings and recommendations for strengthening their information security program (see Section VI).

VI. Agency Comments – Management Response to the Report

GSA

GSA Office of the Chief Information Officer

10/17/2024

MEMORANDUM FOR SONYA PANZO
ASSOCIATE DEPUTY ASSISTANT INSPECTOR GENERAL FOR AUDITS - INFORMATION TECHNOLOGY AUDIT OFFICE (JA-T)

FROM DAVID A. SHIVE
CHIEF INFORMATION OFFICER – (I)

SUBJECT: Agency Management Response – Draft Report: Independent Performance Audit on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report - Fiscal Year 2024

The Office of the Chief Information Officer appreciates the opportunity to review and comment on the draft evaluation report entitled Independent Performance Audit on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2024. 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.

DocuSigned by:
David Shive
A3AE4284A2754F9...

10/21/2024

Appendix I –
Status of Prior Year Findings

As part of the FY 2024 FISMA performance audit, we performed procedures to determine whether management closed prior year findings. Findings were closed if management provided sufficient documentation to evidence that the associated recommendations were fully implemented. Findings with recommendations that were determined to be partially implemented or not implemented remained open. As outlined in the table below, we determined that two of four prior year findings were closed.

Prior Year Findings - 2022 Audit[7]

Finding Number	Prior Year Condition	Recommendation(s)	Status
3. Protect – IAM **Audit Log Monitoring** **Access Review and Recertification**	Weaknesses were noted with audit logging and access administration controls for one GSA-owned information system. Specifically, we noted: 1. Management did not develop and implement a manual or automated process to document the periodic review of privileged system user account activities. 2. System application users were required to recertify their access; however, an independent recertification by the GSA Program Management Office was not performed.	We recommend that GSA: 1. Amend the SSP audit log review frequency to adhere to GSA IT Security Procedural Guide: *AU* or obtain an Acceptance of Risk or formal risk acceptance for system controls that do not comply with GSA IT policies and directives. 2. Develop and implement a process to document evidence of the periodic review of privileged user account activities. 3. Ensure all system users are independently recertified no less than annually, in accordance with GSA policy.	Closed (in FY 2023) Closed (in FY 2023) Closed (in FY 2024)
10. Protect – IAM **Access Authorization**	GSA management did not document its authorization of access for two of two new OS administrators and two of two new application administrators supporting one GSA-owned information system, which did not adhere to the SSP and *GSA IT Security Policy* CIO 2100.1M.	We recommend that GSA: 1. Enforce proper completion of application administrator and OS administrator request forms to include obtaining authorizations from designated management prior to provisioning administrator access to the system's application and OS, respectively. 2. Validate that access is appropriate for all system application and OS administrator accounts.	Closed (in FY 2023) Closed (in FY 2024)

[7] These findings were first reported in FY 2022, but certain recommendations were determined to be open during the FY 2023 FISMA performance audit. As a result, we performed follow-up testing for these findings in FY 2024.

Prior Year Findings - 2023 Audit

Finding Number	Prior Year Condition	Recommendation(s)	Status
1. Identify – RM **POA&Ms**	Weaknesses were identified in the process for updating entity-wide and system-level POA&Ms on a quarterly basis in accordance with GSA policy and procedures. Specifically, we identified the following weaknesses: • Two entity-wide POA&Ms with a status of "Delayed" had not been updated since August 2022 to indicate a rationale for the delays, milestone changes, or new scheduled completion dates in the listing. • For one GSA-owned information system, five system-level POA&Ms with a status of "Delayed" had not been updated at the time of our testing to indicate a rationale for the delays, milestone changes, or new scheduled completion dates in the listing. Additionally, scheduled completion dates or statuses were not documented for three system-level POA&Ms for the system. • For one GSA-owned system component, three system-level POA&Ms with a status of "Delayed" had not been updated at the time of our testing to indicate a rationale for the delays, milestone changes, or new scheduled completion dates in the listing.	We recommend that GSA management document updates within the entity-wide and system-level POA&M listing in a timely manner, to include rationale for delays, milestone changes, or new scheduled completion dates for delayed POA&Ms.	Open
2. Identify – RM **Protect – IAM** **POA&Ms** **Session Termination**	GSA management did not document a system-level POA&M for a control implementation gap identified in the SSP for NIST SP 800-53 Rev. 5 Access Control (AC) control AC-12 (*Session Termination*) for one GSA-owned information system. Specifically, the SSP noted that control AC-12 related to session termination was partially implemented and was planned to be fully implemented. However, a POA&M was not	We recommend that GSA management document POA&Ms for any required security controls noted as partially implemented and/or planned within system security plans.	Open

Finding Number	Prior Year Condition	Recommendation(s)	Status
	documented to track the risk related to a required security control not being implemented for the system in accordance with GSA policy and procedures.		

Appendix II – Glossary

Acronym	Definition
AAL	Authenticator Assurance Level
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CM	Configuration Management
CP	Contingency Planning
CSM	Configuration Settings Management
CTO	Chief Technology Officer
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
D2D	Data to Decisions
DB	Database
DHS	Department of Homeland Security
DPP	Data Protection and Privacy
FAS	Federal Acquisition Services
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
FY 2024 IG FISMA Reporting Metrics	FY 2024 Core and Supplemental Group 2 IG Metrics
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
GRC	Governance, Risk, and Compliance
GSA	General Services Administration
IAM	Identity and Access Management
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IR	Incident Response
ISCM	Information Security Continuous Monitoring
ISSO	Information System Security Officer
IT	Information Technology
KEV	Known Exploited Vulnerabilities
KPMG	KPMG LLP
MFA	Multifactor Authentication
NFR	Notice of Finding and Recommendation
NIST	National Institute of Standards and Technology
OCISO	Office of the Chief Information Security Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OS	Operating System
PBS	Public Buildings Services

Acronym	Definition
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
Rev.	Revision
RM	Risk Management
SCRM	Supply Chain Risk Management
SIEM	Security Information and Event Management
SP	Special Publication
SSP	System Security Plan
ST	Security Training