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 2025

December 4, 2025

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)

December 4, 2025

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 2025*. This report is provided to you in the format according to our contract GS-00F-275CA, order number 47HAA021F0040, modification PO0008, dated January 15, 2025, 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 2025 Federal Information Security Modernization Act of 2014 (FISMA) report is one recommendation to address a specific General Services Administration (GSA) system-level finding within the information security program and practices. When developing plans of actions and milestones or corrective actions, GSA management should assess whether this finding is contained to its respective areas as described in this report or whether the recommendation 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 (703) 286-8160 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 2025

December 4, 2025

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, 2024, through May 31, 2025.[1] 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) 2025 included procedures at the entity and system levels for five GSA-owned information systems and five contractor-owned information systems. The FY 2025 Inspector General (IG) FISMA Reporting Metrics (FY 2025 IG FISMA Reporting Metrics) established in the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* document, dated April 3, 2025, served as the basis for our test procedures.[2]

To support the overall performance audit objective, we also performed external vulnerability scanning and penetration testing activities over a selected GSA-owned information system, and performed internal vulnerability scanning activities over three selected 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 25, 2025.

Additionally, we followed up on the status of nine prior years' findings. Based on our testing, we determined that GSA management implemented corrective actions to remediate seven of the nine prior years' findings, and that these findings were closed (see Appendix I). However, we determined that two prior years' findings remained open, and we also reported three new findings (see Section IV) in the Protect cybersecurity function within the following areas:

Configuration Management

- Flaw Remediation – Remediation and Tracking of Vulnerabilities Not in Adherence with GSA Policy for two GSA-owned information systems

Identity and Access Management

- Least Privilege and Separation of Duties – Initial Access Authorization Not Documented Prior to Access Provisioning for New Privileged User for one GSA-owned information system

[1] OMB Memorandum 25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*.
[2] https://www.cisa.gov/sites/default/files/2025-04/Final%20FY%202025%20IG%20FISMA%20Reporting%20Metrics_Ver%202.0_April%202025-508_0.pdf.

- Least Privilege and Separation of Duties –Privileged User Self-Reviewed Access During Periodic User Access Review for one GSA-owned information system

The nature of these findings impacted our assessment of certain FY 2025 IG FISMA Reporting Metrics within the Protect function, which was then factored into the calculated average rating of the function.

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.[3] We made this determination based on the calculated averages of the FY 2025 IG FISMA Reporting Metrics being assessed as "Managed and Measurable" or "Optimized." Specifically, the calculated averages of metrics in the Govern, Identify, Protect, Respond, and Recover cybersecurity functions were assessed as "Managed and Measurable," while the Detect cybersecurity function was assessed as "Optimized."

What We Recommend

We made one recommendation related to one of the three new findings that should strengthen GSA's information security program if effectively addressed by management.[4] GSA management should also consider whether this recommendation applies to other information systems maintained in the organization's FISMA system inventory and implement remedial action as needed.

We recommend that GSA management:

1. Implement a secondary, independent review of access for the user(s) responsible for performing the periodic user access review for one GSA-owned information system, so that these users do not review their own access.

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

[3] The Department of Homeland Security has deployed 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 2025 IG FISMA Reporting Metrics were required to be submitted in CyberScope no later than August 1, 2025.

[4] Two of the three Notices of Findings and Recommendations (NFRs) were issued without recommendations for the flaw remediation and least privilege 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 2025 until remediation by management.

Contents

I. KPMG Letter

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

Acting 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) 2025

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, 2024, through May 31, 2025. We conducted our performance audit fieldwork from March 25, 2025, through July 31, 2025. To support the overall performance audit objective, we also performed external penetration testing activities over a selected GSA-owned information system, and performed internal vulnerability scanning activities over three selected 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 25, 2025.

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, 2024, through May 31, 2025, in the six cybersecurity function areas outlined in the FY 2025 Inspector General (IG) FISMA Reporting Metrics (FY 2025 IG FISMA Reporting Metrics) established in the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics,* dated April 3, 2025, and to follow-up on the status of prior years' 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 the calculated averages of the FY 2025 IG FISMA Reporting Metrics were assessed as "Managed and Measurable" and "Optimized." Specifically, the calculated averages of metrics in the Govern, 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 risk 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

December 4, 2025

II. Background, Objective, Scope, and Methodology

Background[5]

KPMG LLP ("KPMG" or "we") performed the Fiscal Year (FY) 2025 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[6]

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 $105 billion, oversees approximately 360 million square feet of workspace, manages over 235,000 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 provides a range of services described throughout this section that enable GSA's overall mission. The GSA IT security program protects GSA systems; 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 focuses 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

[5] The information in this section of the report is as of November 25, 2025.
[6] Since January 2025, there have been significant changes in the GSA workforce and organizational structure.

modernization efforts. The Office of the Deputy CIO includes:

    - *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 corporate IT systems, advises GSA's Service and Staff Offices (SSOs) on IT tools that support and enhance GSA's 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: Information & Data Operations Division, Data Governance & Privacy Division, Records Management Division, and IT Accessibility Division. The Office of Enterprise Data and Privacy Management also includes the Data to Decisions (D2D) program, which was previously under the Office of the Deputy CIO. The D2D program is a government-wide data analytics platform designed to collect, manage, and analyze complex data, and to make these analyses available to stakeholders within and outside of GSA.
- *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 leads the GSA IT Security Office and is responsible for the development and maintenance of the agency's IT security program. OCISO establishes and disseminates IT security policies, procedures, and guidelines which govern the use of IT across GSA. OCISO also manages FISMA reporting and oversees several key control areas, including identity and access management (IDAM), flaw remediation, change management oversight, incident response, and continuous monitoring.[7] OCISO is comprised of 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

[7] IDAM is interchangeable with identity, credential, and access management (ICAM).

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 IDAM 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 cybersecurity supply chain risk management (C-SCRM) assurance for GSA IT and supports agencywide C-SCRM activities for GSA systems. In addition, this division leads GSA's efforts in developing its zero trust strategy.
- *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 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 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 SSOs. 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 two divisions: Solutions Strategy Division and Service Delivery Division. The Office of the CTO also includes programs for Tech Guides and Playbooks, 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 25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, which established guidance for implementing the FY 2025 Inspector General (IG) Reporting Metrics (FY 2025 IG FISMA Reporting Metrics).[8] The FY 2025 IG FISMA Reporting Metrics are aligned to the six information security functions outlined in National Institute of Standards and Technology (NIST) publication *The NIST Cybersecurity Framework (CSF) 2.0* (Cybersecurity Framework), which include: Govern, Identify, Protect, Detect, Respond, and Recover. In addition, CIGIE maintained maturity models for ten FISMA metric domains: Cybersecurity Governance (CG), Cybersecurity Supply Chain Risk Management (C-SCRM), Risk and Asset Management (RAM), Configuration Management (CM), Identity and Access Management (IDAM), 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 2025 IG FISMA Reporting Metrics.

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

Cybersecurity Functions	FISMA Metric Domains
Govern	CG C-SCRM
Identify	RAM
Protect	CM IDAM DPP ST
Detect	ISCM
Respond	IR
Recover	CP

Consistent with FY 2024, the FY 2025 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.

[8] The FY 2025 IG FISMA Reporting Metrics were established in OMB's *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* document, dated April 3, 2025.

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 2025 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 2025 IG FISMA Reporting Metrics include Core Metrics and Supplemental Metrics, as depicted in **Table 3** below.

Table 3: FY 2025 Metric Scoping

Core Metrics	Supplemental Metrics
5. External Products, Components, Systems, and Services 7. Systems Inventory 8. Hardware Management 9. Software Management 11. Information System Risk Governance 12. Enterprise View of Risk 14. Secure Configuration Settings 15. Flaw Remediation 17. Non-privileged User Multifactor Authentication (MFA) 18. Privileged User MFA 19. Least Privilege and Separation of Duties 21. Security and Privacy Controls 22. Data Exfiltration 24. Knowledge, Skills, and Abilities 26. ISCM Strategy 28. Ongoing System Authorizations 30. Incident Detection and Analysis 31. Incident Handling 33. Business Impact Analyses 34. Contingency Testing/Exercises	1. Cybersecurity Profiles 2. Cybersecurity Risk Management 3. Cybersecurity Roles and Responsibilities 10. Data Inventories 27. Asset Integrity and Security Posture

According to the FY 2025 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 2025 testing, a calculated average scoring model was used in which Core Metrics and Supplemental 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 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 external penetration testing conducted 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 2025 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 2025 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, 2024, through May 31, 2025. Specifically, we assessed GSA's performance in the six cybersecurity functions outlined in the FY 2025 IG FISMA Reporting Metrics. To support the overall performance audit objective, we also performed external vulnerability scanning and penetration testing activities over one GSA-owned information system, and internal vulnerability scanning activities over three GSA-owned information systems. Our results for this testing are as of June 25, 2025. We conducted our fieldwork from March 25, 2025, through July 31, 2025. As part of our performance audit, we responded to the FY 2025 IG FISMA Reporting Metrics on the GSA OIG's behalf to assess maturity levels, and we also followed up on the status of prior years' findings.

Scope

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation; FY 2025 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 116 systems in the GSA FISMA system inventory as of February 27, 2025. We also performed follow-up testing over five additional GSA information systems to determine whether GSA had addressed prior years' 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 2025 IG FISMA Reporting Metrics to help us gain a better understanding of how the organization implemented relevant security controls and processes for the 25 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 performed external vulnerability scanning and penetration testing activities over one GSA-owned information system, and internal vulnerability scanning activities over three GSA-owned information systems. Our procedures for this testing included those listed above in addition to the performance of penetration testing activities, review of vulnerability scan results, 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 25, 2025.

We conducted our fieldwork from March 25, 2025, through July 31, 2025. All inquiries and observations were conducted through walkthroughs with GSA management. We also periodically met with GSA management and the GSA OIG 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 2025 in the "Audit Findings and Recommendation" section of this report.

III. Overall Results

GSA established and maintained its information security program and practices for its information systems across the six cybersecurity functions and ten 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
Govern (CG and C-SCRM)	Managed and Measurable (Level 4)
Identify (RAM)	Managed and Measurable (Level 4)
Protect (CM, IDAM, 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 three findings within the Protect function. The nature of these findings impacted our assessment of certain FY 2025 IG FISMA Reporting Metrics within the Protect function, which was then factored into the calculated average rating of the function. **Table 5** below depicts the finding areas by function for the three reported findings. There were two reported findings related to Least Privilege and Separation of Duties.

Table 5: Summary of Finding Areas by Cybersecurity Functions

Function	Finding Area
Protect – CM	Flaw Remediation
Protect – IDAM	Least Privilege and Separation of Duties

Govern

The objective of the Govern function in the NIST Cybersecurity Framework is to establish, communicate, and monitor an organization's cybersecurity risk management strategy, expectations, and policy. The Govern function integrates cybersecurity with enterprise risk management, serving as the backbone of a resilient cybersecurity program. This function is carried out through proper CG and C-SCRM processes.

Cybersecurity Governance (CG)

CG requires agencies to enhance the rigor of cybersecurity risk governance and management practices. It aims to help organizations understand, assess, prioritize, and communicate their cybersecurity efforts effectively, taking into account cybersecurity objectives, the risk environment, and lessons learned from past experiences.

Based on the results of our performance audit procedures, we determined that GSA management developed and maintained cybersecurity profiles used to understand, tailor, assess, prioritize and communicate its cybersecurity objectives. GSA management also utilized cybersecurity risk management strategy and cybersecurity roles, responsibilities, and authorities to support operational risk decisions and foster accountability, performance assessments, and continuous improvement. We did not report any findings related to GSA's CG program and associated security controls.

Cybersecurity Supply Chain Risk Management (C-SCRM)

C-SCRM requires agencies to establish and manage a comprehensive program to identify, assess, and respond to cybersecurity risks throughout the supply chain at all organizational levels. This involves setting up strategies, objectives, policies, and processes for effective risk management and ensuring cybersecurity roles and responsibilities are communicated and coordinated internally and externally.

Based on the results of our performance audit procedures, we determined that GSA management created an Executive Board responsible for enterprise-wide governance and established C-SCRM policies and procedures. GSA management also implemented tools to monitor critical supplier risks and C-SCRM events. GSA management also developed detailed guides for monitoring contractor-owned information systems. This included the use of a Governance, Risk, and Compliance (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.

Identify

The objective of the Identify function in the NIST Cybersecurity Framework is to develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The Identify function focuses on asset management, risk assessment, and continuous improvement to enhance cybersecurity. This function is carried out through proper RAM processes.

Risk and Asset Management (RAM)

FISMA requires federal agencies to establish an information security program that protects systems, data, and assets commensurate with their risk environment. RAM is the process of identifying, assessing, and controlling threats to an organization's operating environment. These threats 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 through its deployment of a GRC platform, which is used 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 security tools to track and mitigate risks and vulnerabilities that impacted GSA information systems. We did not report any findings related to GSA's RAM program and associated security controls.

Protect

The objective of the Protect function in the NIST Cybersecurity Framework is to develop and use safeguards to prevent or reduce cybersecurity risks. The Protect function encompasses essential safeguards and controls needed to ensure the security and resilience of an organization's systems and data. This function is carried out through proper CM, IDAM, 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 and, as a result, 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 established processes to monitor the IT environment 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 one finding related to GSA's flaw remediation processes for certain selected GSA-owned systems. Specifically, we noted that a total of three vulnerabilities—two high-risk vulnerabilities for one GSA-owned information system and one low-risk vulnerability for another GSA-owned information system—were not remediated in accordance with GSA-defined timeframes or tracked in POA&Ms as required by GSA policy. We also identified one Performance Improvement Observation (PIO) related to retention of evidence to indicate that the dashboard for one GSA-owned information system was reviewed as part of monthly compliance scan reviews for the information system. Additionally, we noted that one prior year finding related to GSA's flaw remediation processes remained open during FY 2025. Specifically, we noted that moderate- and low-risk vulnerabilities identified for one GSA-owned information system were not remediated in accordance with GSA-defined timeframes or tracked in POA&Ms as required by GSA policy. The reported new and prior year findings impacted our assessed maturity ratings for the associated metric, and therefore impacted our overall assessment of GSA's CM program. The PIO did not impact our assessed maturity rating for the associated metric, as the nature of the observation did not cause controls related to compliance scan reviews to be deficient.

Identity and Access Management (IDAM)

IDAM 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 IDAM 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 IDAM program. Additionally, we determined that GSA management utilized tools to implement the IDAM 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, least privilege and segregation of duties, and remote access operated effectively during the period.

However, we reported two findings related to GSA's account management processes for certain selected GSA-owned systems. Specifically, we noted GSA management did not document an initial access authorization for one of two selected new users that were provisioned privileged access to one GSA-owned information system during the period, as required by GSA policy. Additionally, we noted that one user reviewed and reauthorized their own access to one GSA-owned information system, which was not in accordance with separation of duties principles. The reported findings impacted our assessed maturity ratings for the associated metric, and therefore impacted our overall assessment of GSA's IDAM 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.

Based on the results of our audit procedures, we determined that GSA management implemented a privacy program and associated 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. We also determined that GSA management implemented a comprehensive data inventory to track data and metadata.

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. We did not report any findings related to GSA's ST program and associated security controls.

Detect – Information Security Continuous Monitoring (ISCM)

The objective of the Detect function in the NIST Cybersecurity Framework is to enable organizations to promptly identify cybersecurity events. The Detect function involves constant supervision and observation of the network, enhanced anomaly detection, and analysis of possible cybersecurity attacks and compromises. The 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. However, we did identify one PIO related to Security Assessment Reports (SARs) for certain selected GSA-owned and contractor-owned systems missing a required signature. The PIO did not impact our assessed maturity rating for the associated metric, as the nature of the observation did not cause controls related to security assessments to be deficient.

Respond – Incident Response (IR)

The objective of the Respond function in the NIST Cybersecurity Framework is to manage cybersecurity incidents through effective incident management, analysis, mitigation, reporting, and communication. The Respond function helps organizations better understand and manage cybersecurity risks by safeguarding data and systems against online attacks. 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. This function is carried out through agency requirements 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 restore systems or assets affected by cybersecurity incidents to normal operations while minimizing the impact of the incident. The Recover function emphasizes the importance of preparation to ensure timely and effective recovery. 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 Recommendation

Protect – CM – Flaw Remediation

Controls for remediating and tracking external website-based and internal application vulnerabilities for configuration and patch management requirements within two GSA-owned information systems did not operate effectively during the period. Specifically, we identified a total of three vulnerabilities—two high-risk vulnerabilities for one GSA-owned information system and one low-risk vulnerability for another GSA-owned information system—that were not remediated in accordance with GSA-defined timeframes or tracked in a POA&M, as required by GSA policy.

The following criteria support the noted condition:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 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; and […].
>
> 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, Revision 5, dated April 2, 2025, Section 3.1: "Implementation of NIST Controls," states:

> GSA systems must implement NIST controls RA-05, Vulnerability Monitoring and Scanning, and SI-02(03), 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-05 and SI-02(03) that address frequencies or timelines are listed).

RA-05:

a. Monitor and scan for vulnerabilities in the system and hosted applications [weekly authenticated scans for operating systems (OS)-including databases (DB), 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 [within:

- 14 days for Cybersecurity and Infrastructure Security Agency (CISA) Known Exploitable Vulnerabilities (KEV)
- 15 days for Critical vulnerabilities for Internet-accessible systems or services
- 30 days for Critical and High vulnerabilities
- 90 days for Moderate vulnerabilities
- 180 days for Low vulnerabilities].

in accordance with an organizational assessment of risk[.]

SI-02(03):

(b) Establish the following benchmarks for taking corrective actions: [within:

- 14 days for CISA Known Exploitable Vulnerabilities (KEV)
- 15 days for Critical vulnerabilities for Internet-accessible systems or services
- 30 days for Critical and High vulnerabilities
- 90 days for Moderate vulnerabilities
- 180 days for Low vulnerabilities].

GSA IT Security Procedural Guide: Plan of Action and Milestones (POA&M) CIO-IT Security-09-44, Revision 9, dated November 7, 2024, Table 3-1: "POA&M Requirement Guidance," states:

POA&M Requirements			
Finding Source	**Type/Risk Level**	**Remediation Timeline**	**When is a POA&M Required?**
[…]			
Continuous Monitoring Findings • Configuration scans • Vulnerability scans (OS/Network, etc.) • Web vulnerability scans	KEV	14 days	Immediately upon detection
	Critical (Internet-facing)	15 days	Immediately upon detection
	Critical/High	30 days	Immediately upon detection
	Moderate	90 days	Within 60 days of detection
	Low	180 days	Not applicable**
[…]			

**Low findings from vulnerability scans are generally informational or false positives and are typically addressed during normal system patching and updates.

For one GSA-owned information system, this condition occurred because GSA management did not formally assess the risk of the identified vulnerabilities. For the other GSA-owned information system, GSA management indicated they did not timely remediate or create a POA&M to track the identified low-risk vulnerability due to prioritization of remediation for critical- and high-risk vulnerabilities.

The ineffective operation of controls for remediating and tracking vulnerabilities within two GSA-owned information systems poses a risk to GSA's security posture and exposes the systems to potential exploitation. This could lead to unauthorized access, data breaches, or system disruptions, compromising the confidentiality, integrity, and availability of critical organizational data and services. The absence of timely remediation and tracking undermines the agency's compliance with its own policy and increases the likelihood of security incidents.

RECOMMENDATION:

GSA management implemented full corrective action for this finding in July 2025 by remediating the noted vulnerabilities. As a result, this finding was issued without an associated recommendation.[9]

[9] Our testing determined that management implemented full corrective actions for this finding prior to issuance of this NFR, so we did not issue an associated recommendation. However, we noted that the finding was present within the GSA IT environment during FY 2025 until it was remediated in July 2025, and therefore issued this NFR to report on the condition we identified through the audit.

Protect – IDAM – Least Privilege and Separation of Duties

Controls to document access authorization prior to provisioning privileged access to one GSA-owned information system did not operate effectively during the FY 2025 FISMA performance audit period. Specifically, we noted that GSA management did not document initial access authorization for one of two selected new users that were provisioned privileged access to the GSA-owned information system, as required by GSA policy.

The following criteria support the noted condition:

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

> AC-2 Account Management
> <u>Control:</u>
> […]
> e. Require approvals by [*Assignment: organization-defined personnel or roles*] for requests to create accounts; […]
> i. Authorize access to the system based on:
>   1. A valid access authorization;
>   2. Intended system usage; and
>   3. [*Assignment: organization-defined attributes (as required)*]; […].

GSA *IT Security Procedural Guide: Access Control (AC) CIO-IT Security-01-07*, Revision 7, dated February 10, 2025, Section 3.2: "AC-02 Account Management," states:

> Control:
> […]
> e. Require approvals by [designated account managers as specified in AC-02.b] for requests to create accounts; […]
> i. Authorize access to the system based on:
>   1. A valid access authorization;
>   2. Intended system usage; and
>   3. [Role privileges identified in GSA [System Security and Privacy Plan] Section 9: Types of Users]; […].

This condition occurred because GSA management preemptively provisioned the noted user access to the GSA-owned information system once he completed new hire onboarding, because he required access in order to perform his assigned job responsibilities, but failed to concurrently document the user's initial access authorization before provisioning the access as required by GSA policy due to human error.

The ineffective operation of controls to document access authorizations prior to provisioning privileged access increases the risk of unauthorized or inappropriate access to the system, which could result in data breaches or system disruptions, compromising the confidentiality, integrity, and availability of critical organizational data and services. The absence of proper authorization documentation undermines the agency's compliance with its own policy and weakens the overall security framework.

RECOMMENDATION:

GSA management implemented full corrective action for this finding in June 2025 by counseling the control operator on the required process and subsequently revoking the user's access, documenting an access authorization for the user, and reprovisioning the user's access in accordance with the documented authorization. As a result, this finding was issued without an associated recommendation.[10]

[10] Our testing determined that management implemented full corrective actions for this finding prior to issuance of this NFR, so we did not issue an associated recommendation. However, we noted that the finding was present within the GSA IT environment during FY 2025 until it was remediated in June 2025, and therefore issued this NFR to report on the condition we identified through the audit.

Protect – IDAM – Least Privilege and Separation of Duties

Controls to periodically review privileged user access to one GSA-owned information system were not designed in accordance with separation of duties principles. Specifically, we noted that one user reviewed and reauthorized their own access to the system.

The following criteria support the noted condition:

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

> AC-5 Separation of Duties
> <u>Control:</u>
> a. Identify and document [*Assignment: organization-defined duties of individuals requiring separation*]; and
> b. Define system access authorizations to support separation of duties.

GSA *IT Security Procedural Guide: Access Control (AC) CIO-IT Security-01-07*, Revision 7, dated February 10, 2025, Section 3.5: "AC-05 Separation of Duties," states:

> Control:
> a. Identify and document [GSA SSO or Contractor recommended duties of individuals requiring separation, to be approved by the GSA CISO and AO];
> b. Define system access authorizations to support separation of duties.
>
> System-Specific Guidance:
> For AC-05, the System Owner must ensure separation of duties which ensures that no single user has complete control over a single critical process […].

This condition occurred because the individual responsible for performing the user access review also had privileged access to the GSA-owned information system. GSA management had not assessed the risk of this individual reviewing his/her own access, so management did not implement mitigating controls, such as a secondary, independent review of the individual's access.

The absence of effective controls to periodically review user access in accordance with separation of duties principles increases the risk of unauthorized or inappropriate access rights being granted or maintained, which could result in data breaches or system disruptions, compromising the confidentiality, integrity, and availability of critical organizational data and services. Failure to implement proper separation of duties could also lead to an increased risk of undetected fraudulent activities.

<u>RECOMMENDATION:</u>

We recommend that GSA management implement a secondary, independent review of access for the user(s) responsible for performing the periodic user access review for one GSA-owned information system, so that these users do not review their own access.

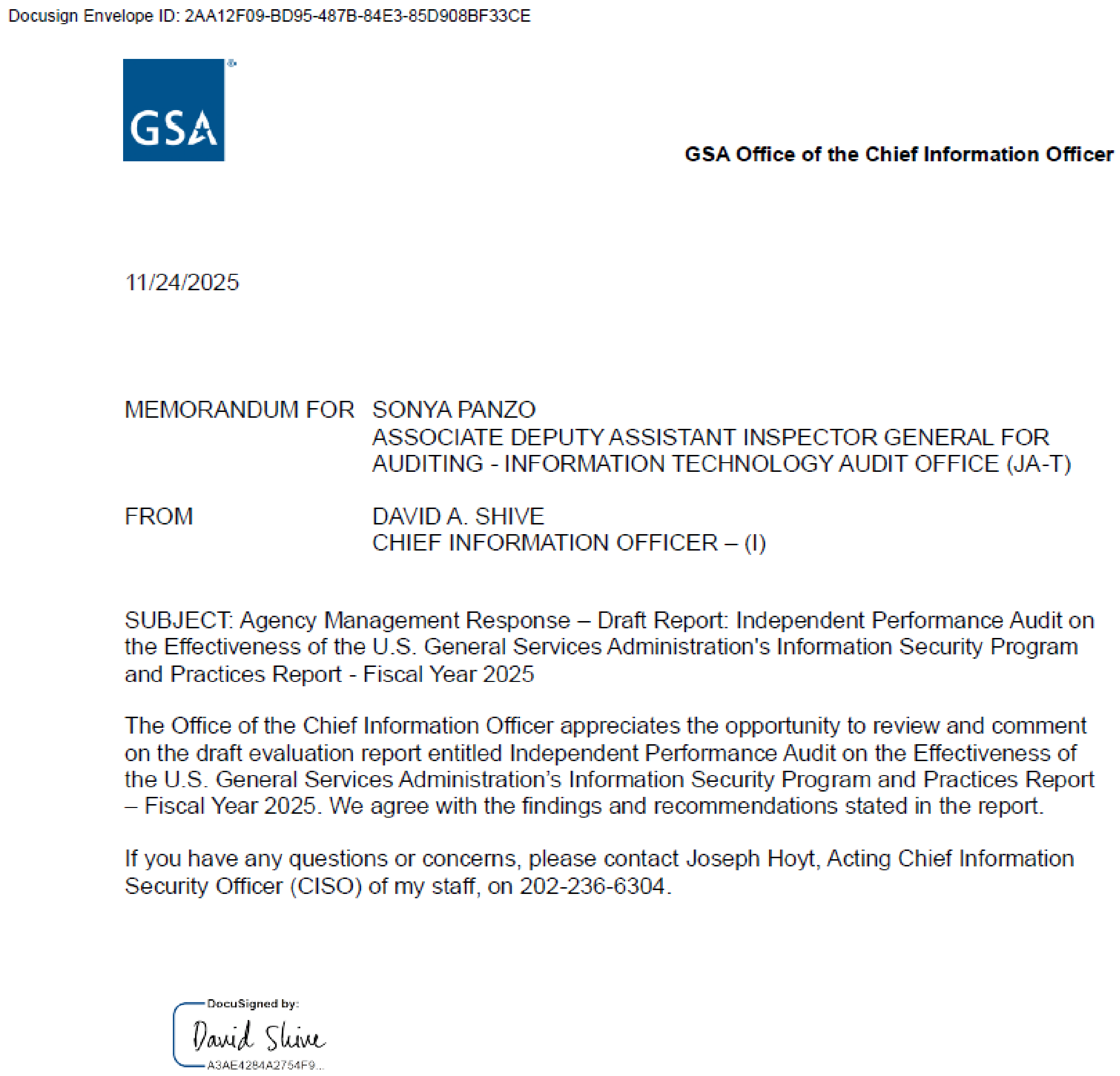
V. Conclusions

GSA management established and maintained its information security program and practices for its information systems for the six cybersecurity functions and ten FISMA metric domains during FY 2025. We assessed GSA's information security program as "Effective" within CyberScope; this determination was made because the majority of the FY 2025 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 Govern, 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 the nine prior years' findings. Based on our testing, we determined that GSA management implemented corrective actions to remediate seven of the nine prior years' findings, and that these findings were closed (see Appendix I). However, we determined that two prior years' findings remained open, and we also reported three new findings (see Section IV) in the Protect cybersecurity function, which spanned the CM and IDAM FISMA metric domains. The nature of these findings impacted our assessment of certain FY 2025 IG FISMA Reporting Metrics within the Protect function, which was then factored into the calculated average rating of the function.

We made one recommendation related to one of the three new findings that should strengthen GSA's information security program if effectively addressed by management.[11] GSA management should also consider whether this recommendation applies 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 recommendation for strengthening their information security program (see Section VI).

[11] Two of the three Notices of Findings and Recommendations (NFRs) were issued without recommendations for the flaw remediation and least privilege 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 2025 until remediation by management.

VI. Agency Comments – Management Response to the Report



GSA Office of the Chief Information Officer

11/24/2025

MEMORANDUM FOR SONYA PANZO
ASSOCIATE DEPUTY ASSISTANT INSPECTOR GENERAL FOR
AUDITING - 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 2025

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 2025. We agree with the findings and recommendations stated in the report.

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

DocuSigned by:
David Shive
A3AE4284A2754F9...

Appendix I –
Status of Prior Years' Findings

As part of the FY 2025 FISMA performance audit, we performed procedures to determine whether management closed prior years' 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 seven of nine prior years' findings were closed.

Prior Year Findings - 2023 Audit[12]

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 information 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[13]

[12] These findings were first reported in FY 2023, but certain recommendations were determined to be open during the FY 2024 FISMA performance audit. As a result, we performed follow-up testing for these findings in FY 2025.

[13] This recommendation remained open for one GSA-owned information system but was closed for the entity level and one GSA-owned information system.

Finding Number	Prior Year Condition	Recommendation(s)	Status
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 system security plan (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 documented to track the risk related to a required security control not being implemented for the system in accordance with GSA policy and procedures.	We recommend that GSA management document POA&Ms for any required security controls noted as partially implemented and/or planned within SSPs.	Closed

Prior Year Findings - 2024 Audit

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

Finding Number	Prior Year Condition	Recommendation(s)	Status
2. 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).	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.	Open[14]
		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.	Open
		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.	Open
3. 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.	GSA management remediated the identified condition as of April 30, 2024; therefore, this finding was issued without an associated recommendation.	Closed[15]
4. Protect - IAM[16] **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.	GSA management remediated the identified condition as of April 30, 2024; therefore, this finding was issued without an associated recommendation.	Closed[17]

[14] This recommendation remained open for one GSA-owned information system but was closed for two GSA-owned information systems. This footnote also applies to open recommendations 2 and 3 for the finding.

[15] This finding was identified, remediated, and closed, but still reported without an associated recommendation in FY 2024.

[16] There was no final FISMA-2024-04 NFR issued in FY 2024 because GSA management provided evidence between draft and final issuance of the NFR which caused it to be closed.

[17] This finding was identified, remediated, and closed, but still reported without an associated recommendation in FY 2024.

Finding Number	Prior Year Condition	Recommendation(s)	Status
5. 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.	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.	Closed Closed
6. 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.	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.	Closed
7. 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	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.	Closed

Finding Number	Prior Year Condition	Recommendation(s)	Status
	completed the trainings between 9 and 22 days after the required due dates.		

Appendix II – Glossary

Acronym	Definition
AC	Access Control
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
CDM	Continuous Diagnostics and Mitigation
CG	Cybersecurity Governance
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
C-SCRM	Cybersecurity – Supply Chain Risk Management
CTO	Chief Technology Officer
D2D	Data to Decisions
DB	Database
DHS	Department of Homeland Security
DPP	Data Protection and Privacy
FAS	Federal Acquisition Services
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
FY 2025 IG FISMA Reporting Metrics	FY 2025 Inspector General FISMA Reporting Metrics
GAGAS	Generally Accepted Government Auditing Standards
GRC	Governance, Risk, and Compliance
GSA	General Services Administration
ICAM	Identity, Credential, and Access Management
IDAM	Identity 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
PII	Personally Identifiable Information

Acronym	Definition
PIO	Performance Improvement Observation
POA&M	Plan of Action and Milestones
RAM	Risk and Asset Management
Rev.	Revision
SAR	Security Assessment Report
SIEM	Security Information and Event Management
SP	Special Publication
SSO	Service and Staff Office
SSP	System Security Plan
ST	Security Training