



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 2026

October 14, 2026



INDEPENDENT PERFORMANCE AUDIT
ON THE EFFECTIVENESS OF THE U.S.
GENERAL SERVICES ADMINISTRATION'S
INFORMATION SECURITY PROGRAM
AND PRACTICES REPORT
FISCAL YEAR 2026

October 14, 2026

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, 2025, through May 31, 2026. 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) 2026 included procedures at the entity and system levels for five GSA-owned information systems and five contractor-owned information systems. As directed by OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), the FY 2026 Inspector General (IG) FISMA Reporting Metrics (FY 2026 IG FISMA Reporting Metrics) served as the basis for our test procedures.¹

To support the overall performance audit objective, we also performed external penetration testing over a selected GSA-owned information system 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 July 8, 2026.

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

Identity and Access Management

- Least Privilege and Separation of Duties – Lack of Access Review for Database Administrators for one GSA-owned information system

The nature of this finding impacted our assessment of one of the associated FY 2026 IG FISMA Reporting Metrics within the Protect function, which was then factored into the calculated average rating of the function.

¹ Per OMB and CIGIE guidance, IGs should apply the FY 2025 IG FISMA Reporting Metrics for FY 2026 testing. Therefore, all references to the ‘FY 2026 IG FISMA Reporting Metrics’ throughout this report should be interpreted as references to the FY 2025 metrics. The FY 2025 metrics can be found in the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* document, dated April 3, 2025 (https://www.cisa.gov/sites/default/files/2025-04/Final%20FY%202025%20IG%20FISMA%20Reporting%20Metrics_Ver%202.0_April%202025-508_0.pdf).

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 the calculated averages of the FY 2026 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 the new finding that should strengthen GSA's information security program if effectively addressed by management. 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. Design and implement a process to formally review and reauthorize database administrator access for one GSA-owned information system at the defined frequency in accordance with GSA policy.

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

² The Department of Homeland Security has deployed CyberScope, a web-based application, to collect data that OMB uses to assess federal agencies' information security program. 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 the FY 2026 IG FISMA Reporting Metrics were required to be submitted in CyberScope no later than July 31, 2026.

Contents

I.	KPMG Letter	6
II.	Background, Objective, Scope, and Methodology	9
	Background	10
	Agency Overview.....	10
	Program Overview	10
	FISMA	11
	FISMA Inspector General Metrics and Reporting	12
	Objective, Scope, and Methodology	14
	Objective	14
	Scope.....	14
	Methodology	15
	Criteria	15
III.	Overall Results.....	16
	Govern	17
	Cybersecurity Governance (CG).....	17
	Cybersecurity Supply Chain Risk Management (C-SCRM).....	18
	Identify	18
	Risk and Asset Management (RAM)	18
	Protect.....	19
	Configuration Management (CM).....	19
	Identity and Access Management (IDAM)	19
	Data Protection and Privacy (DPP).....	20
	Security Training (ST)	20
	Detect – Information Security Continuous Monitoring (ISCM)	21
	Respond – Incident Response (IR)	21
	Recover – Contingency Planning (CP).....	22
IV.	Audit Finding and Recommendation	23
	Protect – IDAM – Least Privilege and Separation of Duties.....	24
V.	Conclusions	25
VI.	Agency Comments – Management Response to the Report	27

Appendix I – Status of Prior Years’ Findings.....	29
Appendix II – Glossary	32

I. KPMG Letter



KPMG LLP
Suite 12000
1801 K Street, NW
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) 2026

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, 2025, through May 31, 2026. We conducted our performance audit fieldwork from February 11, 2026, through July 31, 2026. To support the overall performance audit objective, we also performed external penetration testing over a selected GSA-owned information system 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 July 8, 2026.

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) as well as Office of Management and Budget (OMB) and Council of the Inspectors General on Integrity and Efficiency (CIGIE) 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, 2025, through May 31, 2026, in the six cybersecurity function areas outlined in the FY 2026 Inspector General (IG) FISMA Reporting Metrics, and to follow-up on the status of prior years’ findings.³ 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 2026 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.”

³ Per OMB and CIGIE guidance, IGs should apply the FY 2025 IG FISMA Reporting Metrics for FY 2026 testing. Therefore, all references to the ‘FY 2026 IG FISMA Reporting Metrics’ throughout this report should be interpreted as references to the FY 2025 metrics. The FY 2025 metrics can be found in the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* document, dated April 3, 2025 (https://www.cisa.gov/sites/default/files/2025-04/Final%20FY%202025%20IG%20FISMA%20Reporting%20Metrics_Ver%202.0_April%202025-508_0.pdf).



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

October 14, 2026

II. Background, Objective, Scope, and Methodology

Background

KPMG LLP (“KPMG” or “we”) performed the Fiscal Year (FY) 2026 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 Overview⁴

GSA provides innovative solutions for federal agencies that include products, services, workspaces, and expertise to help create a citizen-centric, results-oriented government that is productive and responsible to all Americans. GSA’s strategic goals – savings, efficiency, technology modernization, and shared services – align the agency’s mission, set direction, and guide operational planning. GSA is the government’s landlord, providing workspaces across the government as well as equipment, supplies, telecommunications, and information technology (IT) to federal agencies. GSA’s two main lines of business are the Federal Acquisition Service (FAS) and the Public Buildings Service (PBS). Various staff offices support GSA’s operations in fields including legal, communications, IT, and congressional affairs.

GSA employs nearly 12,000 employees to support other federal agencies and the general public. GSA has an annual contract volume of approximately \$104 billion, manages over 200,000 fleet vehicles, assists tens of thousands of federal travelers through the GSA electronic travel system, and serves as the focal point for data, information, and services offered by the federal government to its citizens. 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 Overview⁵

GSA IT provides a broad range of services that support GSA’s mission. Its security program protects GSA systems, while its infrastructure serves as the backbone for the agency’s business and management applications. GSA IT establishes policies and procedures governing the use of information technology across the organization and promotes agencywide compliance with government-wide guidance issued by the Office of Management and Budget (OMB). Through its focus on customer experience, employee experience, and digital experience, GSA IT works to accelerate technology transformation, strengthen cybersecurity modernization, and maximize data as a strategic asset. The major GSA IT organizations are described below.

- *Chief Information Officer (CIO)*: The GSA 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 Business Applications IT Systems*: The Office of Business Applications IT Systems delivers and manages enterprise business applications and systems for FAS, PBS, the Office of Government-wide Policy, and other GSA organizations through managed services, Software as a Service solutions, commercial off-the-shelf applications, low-code/no-code platforms, and complex business/legacy system operations and management.

⁴ The information in this section of the report is as of August 6, 2026.

⁵ The information in this section of the report is as of August 12, 2026.

- *Office of Innovation*: The Office of Innovation drives GSA's enterprise-wide data, privacy, analytics, and artificial intelligence strategy. Establishes trusted data governance and compliance frameworks, builds and operates secure data infrastructure, ensures seamless technology integration, and delivers innovative solutions to program offices.
- *Office of Digital Management*: The Office of Digital Management manages end-user technology services including device delivery and installation, IT asset management (standards, supply chain management, software license management), help desk operations, user training and communications, resource governance and management (efficiency, performance, analysis, and Capital Planning and Investment Control), contract oversight, and records management.
- *Office of the Chief Information Security Officer (OCISO)*: OCISO protects GSA's information systems and data through comprehensive cybersecurity programs including Identity and Access Management (IDAM), Cybersecurity Supply Chain Risk Management (C-SCRM), and FISMA compliance oversight.⁶ OCISO operates the GSA Security Operations Center (SOC), provides cyber engineering services, implements continuous diagnostics and mitigation (CDM), manages technology authorizations, and supports Information System Security Officers (ISSOs) and Information Systems Security Managers (ISSMs). OCISO is comprised of three divisions:
 - *Security Risk and Compliance Division* – The Security Risk and Compliance Division manages enterprise cybersecurity risk and compliance programs including IDAM systems and policies. This division also develops and implements cybersecurity policies, conducts FISMA audit activities and compliance oversight, and administers C-SCRM programs to ensure GSA maintains appropriate security posture and regulatory compliance across all information systems and operations.
 - *Security Operations and Engineering Division* – The Security Operations and Engineering Division operates the GSA SOC and provides comprehensive cybersecurity engineering services including application security programs, cyber engineering and architecture design, and CDM implementation. This division is responsible for real-time security monitoring, threat detection and response, security architecture development, and automated security tools deployment to protect GSA's information systems and data assets.
 - *ISSO Support Division* – The ISSO Support Division manages technology system authorizations and provides support services for ISSOs and ISSMs. This division operates enterprise Governance, Risk, and Compliance (GRC) platforms and processes to ensure proper security authorization, risk management, and compliance oversight for GSA's information systems throughout their lifecycle.
- *Office of Digital Infrastructure Technologies*: The Office of Digital Infrastructure Technologies provides and maintains the foundational technology infrastructure that enables GSA operations including cloud and on-premises infrastructure, network systems, telecommunications services, and building systems technologies to ensure reliable, secure, and scalable digital services across the agency.

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

⁶ IDAM is interchangeable with identity, credential, and access management.

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 Chief Information Security Officer 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 2026 Inspector General (IG) Reporting Metrics (FY 2026 IG FISMA Reporting Metrics).⁷ The FY 2026 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 2026 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 2025, the FY 2026 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.

⁷ Per OMB and CIGIE guidance, IGs should apply the FY 2025 IG FISMA Reporting Metrics for FY 2026 testing. Therefore, all references to the 'FY 2026 IG FISMA Reporting Metrics' throughout this report should be interpreted as references to the FY 2025 metrics. The FY 2025 metrics can be found in the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* document, dated April 3, 2025 (https://www.cisa.gov/sites/default/files/2025-04/Final%20FY%202025%20IG%20FISMA%20Reporting%20Metrics_Ver%202.0_April%202025-508_0.pdf).

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 2026 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 2026 IG FISMA Reporting Metrics include Core Metrics and Supplemental Metrics, as depicted in **Table 3** below.

Table 3: FY 2026 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 2026 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 2026 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, reviews of internal vulnerability scan results, 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 use CyberScope to calculate the maturity levels for each function and domain and then submit the results of the FY 2026 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 2026 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, 2025, through May 31, 2026. Specifically, we assessed GSA's performance in the six cybersecurity functions outlined in the FY 2026 IG FISMA Reporting Metrics. To support the overall performance audit objective, we also performed external penetration testing over one GSA-owned information system. Our results for this testing are as of July 8, 2026. We conducted our fieldwork from February 11, 2026, through July 31, 2026. As part of our performance audit, we responded to the FY 2026 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 2026 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 125 systems in the GSA FISMA system inventory as of January 27, 2026. We also performed follow-up testing over three 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 2026 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 penetration testing over one GSA-owned information system. Our procedures for this testing included those listed above in addition to the performance of external 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 July 8, 2026.

We conducted our fieldwork from February 11, 2026, through July 31, 2026. 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 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 the finding identified in FY 2026 in the "Audit Finding 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 one finding within the Protect function. The nature of this finding impacted our assessment of one of the FY 2026 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 area by function for the reported finding.

Table 5: Summary of Finding Areas by Cybersecurity Functions

Function	Finding Area
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 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 Plans of Action and Milestones (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.

We identified one Performance Improvement Observation (PIO) as a result of the external penetration testing performed for one GSA-owned information system. Specifically, two low-risk vulnerabilities were identified during penetration testing. GSA management should determine whether these vulnerabilities require corrective action or should be documented as false positives. Additionally, we noted that one prior year finding related to GSA's flaw remediation processes remained open during FY 2026. Specifically, we noted that critical/high- and moderate-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 open prior year finding impacted our assessed maturity rating 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 indicate that vulnerability management controls were 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 one finding related to GSA's account management processes for one selected GSA-owned system. Specifically, we noted GSA management did not design or implement a control to

periodically review and reauthorize administrative access to the database supporting one GSA-owned information system during the performance audit period. The reported finding impacted our assessed maturity rating 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 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 security information and event management (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 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 Finding and Recommendation

Protect – IDAM – Least Privilege and Separation of Duties

A control to periodically review and reauthorize administrative access to the database supporting one GSA-owned information system was not designed or implemented during the performance audit period of October 1, 2025, through May 31, 2026.

The following criteria support the noted condition:

NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, Release 5.2.0, dated August 27, 2025, states:

AC-2 Account Management

Control:

[...]

- j. Review accounts for compliance with account management requirements [*Assignment: organization-defined frequency*] [...].

GSA *IT Security Procedural Guide: Access Control (AC) CIO-IT Security-01-07*, Revision 8, dated February 5, 2026, Section 3.2: “AC-02 Account Management,” states:

Control:

[...]

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

This condition occurred because GSA management did not formally assess the risk of access not being periodically reviewed and reauthorized for one GSA-owned information system.

The absence of effective controls to review privileged user access 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.

RECOMMENDATION:

We recommend that GSA IT management design and implement a process to formally review and reauthorize database administrator access for one GSA-owned information system at the defined frequency in accordance with GSA policy.

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 2026. We assessed GSA's information security program as "Effective" within CyberScope; this determination was made because the majority of the FY 2026 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 three prior years' findings. Based on our testing, we determined that GSA management implemented corrective actions to remediate two of the three prior years' findings, and that these findings were closed (see Appendix I). However, we determined that one prior year finding remained open, and we also reported one new finding (see Section IV) in the Protect cybersecurity function within the IDAM FISMA metric domain. The nature of these findings impacted our assessment of certain FY 2026 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 the new finding that should strengthen GSA's information security program if effectively addressed by management. 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 finding and recommendation for strengthening their information security program (see Section VI).

VI. Agency Comments – Management Response to the Report



GSA Office of the Chief Information Officer

10/1/2026

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 2026.

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 2026. We agree with the findings and recommendations stated in the report.

If you have any questions or concerns, please contact Joseph Hoyt, 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 2026 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 two of three prior years' findings were closed.

Prior Year Finding - 2023 Audit⁸

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.	Closed

⁸ This finding was first reported in FY 2023, but the recommendation was determined to be open for one GSA-owned information system during the FY 2025 FISMA performance audit. As a result, we performed follow-up testing for this finding in FY 2026.

Prior Year Finding - 2024 Audit⁹

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 ¹⁰
		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

Prior Year Finding - 2025 Audit

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

⁹ This finding was first reported in FY 2024, but the recommendation was determined to be open for one GSA-owned information system during the FY 2025 FISMA performance audit. As a result, we performed follow-up testing for this finding in FY 2026.

¹⁰ This recommendation remained open for one GSA-owned system but was closed for two GSA-owned information systems. This footnote also applies to open recommendations 2 and 3 for the finding.

Appendix II – Glossary

Acronym	Definition
AC	Access Control
AICPA	American Institute of Certified Public Accountants
CDM	Continuous Diagnostics and Mitigation
CG	Cybersecurity Governance
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CM	Configuration Management
CP	Contingency Planning
C-SCRM	Cybersecurity – Supply Chain Risk Management
DHS	Department of Homeland Security
DPP	Data Protection and Privacy
FAS	Federal Acquisition Service
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
FY 2026 IG FISMA Reporting Metrics	FY 2026 Inspector General FISMA Reporting Metrics
GAGAS	Generally Accepted Government Auditing Standards
GRC	Governance, Risk, and Compliance
GSA	General Services Administration
IDAM	Identity and Access Management
IG	Inspector General
IR	Incident Response
ISCM	Information Security Continuous Monitoring
ISSO	Information System Security Officer
ISSM	Information System Security Manager
IT	Information Technology
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
PBS	Public Buildings Service
PII	Personally Identifiable Information
PIO	Performance Improvement Observation
POA&M	Plan of Action and Milestones
RAM	Risk and Asset Management
Rev.	Revision
SIEM	Security Information and Event Management
ST	Security Training