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 2023

November 3, 2023

KPMG LLP
8350 Broad Street Suite 900
McLean, VA 22102

Donna Peterson-Jones
Supervisory Auditor/Contracting Officer's Representative
General Services Administration
Office of Inspector General
1800 F Street NW, Suite 5200
Washington, DC 20405

CC: Sonya Panzo, Associate Deputy Assistant Inspector General for Audits – Information Technology and Finance Audit Office (JA-T), and Bonnie Impastato, Contracting Officer

November 3, 2023

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 2023*. This report is provided to you in the format according to our contract GS-00F-275CA, order number 47HAA021F0040, modification PS0004, dated January 15, 2023, 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 2023 Federal Information Security Modernization Act of 2014 (FISMA) report are recommendations to address specific General Services Administration (GSA) entity-wide and system-level findings within the information security program and practices. When developing plans of actions and milestones or corrective actions, GSA management should assess whether these findings are contained to their respective areas as described in this report or whether the recommendations should be considered for other systems, security control areas, or processes within the information system security program.

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

Kind regards,

Raphael S. DiGrado

Raphael DiGrado
Managing Director, Technology Assurance – Audit

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

FISCAL YEAR 2023

November 3, 2023

Executive Summary

Why We Performed This Audit

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the United States (U.S.) 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 (OIG) monitored KPMG's work to ensure it met professional standards and contractual requirements.

To support the overall performance audit objective, we also performed an external penetration test and internal vulnerability scanning activities over a selected set of GSA-owned information systems in order to identify potential system flaws, misconfigurations, or vulnerabilities that could increase the risk of unauthorized access or elevation of privileges to GSA systems and data.

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, 2022, through May 31, 2023. In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA). The technical security testing was completed as of June 21, 2023.

What We Found

Our testing for Fiscal Year (FY) 2023 included procedures at the entity and system levels for five GSA-owned information systems and five contractor-owned information systems. We also followed up on the status of 15 prior year findings. As a result of our procedures and based on the maturity levels calculated in CyberScope,[1] we assessed GSA's information security program as "Effective" according to OMB guidance. We made this determination based on assessing a majority of the FY 2023 Core and Supplemental Group 1 Inspector General (IG) Metrics (FY 2023 IG FISMA Reporting Metrics) as "Managed and Measurable" and "Optimized." Specifically, the Identify, Respond, and Recover cybersecurity functions were assessed as "Managed and Measurable," while the Protect and Detect cybersecurity functions were assessed as "Optimized."

[1]The Department of Homeland Security (DHS) uses CyberScope, a web-based application, to collect data that OMB uses to assess federal agencies' information technology (IT) security. Agencies are required to use CyberScope to submit reporting metrics, including the annual IG FISMA Metrics. IGs are also required to input an independent assessment of the overall effectiveness of their respective agency's information security program. Results for FY 2023 IG FISMA Reporting Metrics were required to be submitted in CyberScope no later than July 31, 2023.

Based on our testing, we determined that GSA implemented corrective actions to remediate 13 of the 15 prior year findings and that these findings were closed (see Appendix I). However, we determined that the remaining two prior year findings remained open, and also reported two new findings (see Section IV) in the Identify and Protect cybersecurity functions in the following areas:

Cybersecurity Function – Identify

- Plans of Action and Milestones (POA&Ms) – Weaknesses in Timely Update of Entity-Wide and Certain System-Level POA&Ms (Risk Management)
- POA&Ms – Lack of POA&M Documentation for Identified Control Implementation Gap for one GSA-owned information system (Risk Management)

Cybersecurity Function – Protect

- Session Termination – Lack of POA&M Documentation for Identified Control Implementation Gap for one GSA-owned information system (Identity and Access Management)[2]

The nature of these findings did not affect our overall assessment of the Identify or Protect functions after determining the calculated average rating of the 11 IG metrics within the Identify function and the 18 IG metrics within the Protect function.

What We Recommend

We made two recommendations related to the two new findings that should strengthen GSA's information security program if effectively addressed by management. GSA management should also implement a process to determine if these recommendations apply to other information systems maintained within the organization's FISMA system inventory.

We recommend that GSA management:

1. Document updates in the entity-wide and system-level POA&M listing in a timely manner and include a rationale for delays, milestone changes, or new scheduled completion dates for delayed POA&Ms.
2. Document POA&Ms for any required security controls that system security plans (SSPs) list as partially implemented or scheduled for implementation.

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

[2]This finding spanned two cybersecurity functions (Identify and Protect) and two metric domains (Risk Management and Identity and Access Management).

Contents

I. KPMG Letter

8350 Broad Street
McLean, VA 22102

Administrator and Acting 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 2023

This report presents the results of the independent performance audit of the United States (U.S.) General Services Administration's (GSA's) information security program and practices performed by KPMG LLP ("KPMG" or "we") for the period of October 1, 2022, through May 31, 2023. We conducted our performance audit fieldwork from March 22, 2023, through July 31, 2023. To support the overall performance audit objective, we also performed an external penetration test and internal vulnerability scanning activities over a selected set of GSA-owned information systems in order to identify potential system flaws, misconfigurations, or vulnerabilities that could increase the risk of unauthorized access or elevation of privileges to GSA systems and data. The results of this technical testing are as of June 21, 2023.

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, 2022, through May 31, 2023 in the five cybersecurity function areas outlined in the Fiscal Year (FY) 2023 Core and Supplemental Group 1 Inspector General (IG) Metrics (FY 2023 IG FISMA Reporting Metrics) and follow-up on the status of prior year findings. As a result of our procedures and based on the maturity levels calculated in CyberScope, we determined that GSA's information security program was "Effective" according to OMB guidance, as a majority of the FY 2023 IG FISMA Reporting Metrics were assessed as "Managed and Measurable" and "Optimized." Specifically, the Identify, Respond, and Recover cybersecurity functions were assessed as "Managed and Measurable," while the Protect and Detect cybersecurity functions were assessed as "Optimized."

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

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

KPMG LLP

November 3, 2023

II. Background, Objective, Scope, and Methodology

Background[3]

KPMG LLP ("KPMG" or "we") performed the Fiscal Year (FY) 2023 independent Federal Information Security Modernization Act of 2014 (FISMA) evaluation under contract with United States (U.S.) General Services Administration (GSA) as a performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) and American Institute of Certified Public Accountants (AICPA) Consulting Services Standards. The GSA Office of Inspector General (OIG) monitored our work to ensure we met professional standards and contractual requirements.

Agency Overview

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

GSA is headquartered in Washington, D.C., and the organization employs nearly 12,000 employees nationwide across 11 regional offices. GSA has an annual contract volume of over 60 billion dollars, manages over 200,000 fleet vehicles, and assists tens of thousands of federal travelers through the GSA electronic travel system. Although GSA leverages billions of dollars in the marketplace, only one percent of GSA's total budget comes from direct congressional appropriations. The majority of GSA's operating costs must be recovered through the products and services it provides.

Program Overview

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

- *GSA's CIO*: The CIO oversees GSA IT and the entity-wide IT operations and budget to ensure 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 modernization efforts.

[3]The information in this section of the report is as of August 1, 2023.

- *Office of Corporate IT Services:* The Office of Corporate IT Services provides enterprise solutions for GSA's IT systems portfolio, advises GSA's Service and Staff Offices (SSOs) on IT tools that support or enhance GSA's enterprise functions, and delivers IT platforms, services, and solutions for the GSA IT enterprise.
- *Office of 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 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.
- *Chief Technology Officer (CTO):* The GSA CTO works across GSA IT and GSA business lines to help ensure that solutions developed by IT organizations are designed efficiently and incorporated into the shared services catalog as appropriate. The CTO also identifies emerging technologies and incorporates them into the existing technology portfolio as part of the overarching technology strategy for GSA.
- *Office of Chief Information Security Officer (OCISO):* The OCISO manages the GSA IT Security Office, which is responsible for the development and maintenance of the GSA IT security program. OCISO establishes and disseminates IT security policies, procedures, and guidelines which govern the use of IT across GSA. IS manages FISMA reporting processes and several of the control areas related to FISMA across the enterprise, such as identity and access management (IAM)[4], flaw remediation, change management, incident response, and information security continuous monitoring. OCISO includes five divisions:
    - *Security Engineering Division* – The Security Engineering Division provides security consulting and engineering support for systems, emerging IT, and IT security initiatives. In addition, the Security Engineering Division runs GSA's Development, Security, and Operations (DevSecOps) program to modernize security across the organization. The Security Engineering Division develops technical security standards and architectural security standards and provides software security testing in support of the GSA IT Standards process.
    - *Identity, Credential, and Access Management Shared Service Division* – The Identity, Credential, and Access Management Shared Service Division supports centralized IAM capabilities that improve coordination and governance across GSA IT and the development/delivery of enterprise certificate and key management capabilities. This division is also responsible for managing cyber supply chain risk management (SCRM) assurance for GSA IT and supports agencywide cyber SCRM activities.
    - *Security Operations Division* – The Security Operations Division provides real-time operational security through security operations center and enterprise network security capabilities. This division supports IT division offices by providing vulnerability management and operational support security services at the enterprise level including managing firewalls, intrusion prevention systems, domain name systems, and security information and event management (SIEM) tools.
    - *Policy and Compliance Division* – The OCISO Policy and Compliance Division provides management and maintenance of GSA Plans of Action and Milestones (POA&Ms) as well as the continuous monitoring program and security awareness and other role-based training programs. The Policy and Compliance Division also manages the processes for creating and maintaining GSA IT security policies,

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

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 and system Authorizing Officials 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 (ISSMs) 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 Chief Information Security Officer and Authorizing Officials during assessment and authorization (A&A) processes for GSA systems.

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 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, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the FY 2023 Core and Supplemental Group 1 Inspector General (IG) Metrics (FY 2023 IG FISMA Reporting Metrics)[5] for five cybersecurity functions outlined in the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* [6] (Cybersecurity Framework). These cybersecurity functions include: Identify, Protect, Detect, Respond, and Recover. In addition, FY 2023 IG FISMA Reporting Metrics use the CIGIE maturity models for nine metric domains: Risk Management (RM), Supply Chain Risk Management (SCRM), Configuration Management (CM), Identity and Access Management (IAM), Data Protection and Privacy (DPP), Security Training (ST), Information Security Continuous Monitoring (ISCM), Incident Response (IR), and Contingency Planning (CP).

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

[6]The President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013, which established that "[i]t is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the Executive Order calls for the development of a voluntary risk-based cybersecurity framework, a set of industry standards and leading practices to help organizations manage cybersecurity risks. The resulting framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

Table 1 below outlines the alignment of the five NIST Cybersecurity Framework functions to the nine FISMA metric domains.

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

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

Changes for FY 2023 Metrics

The FY 2023 IG FISMA Reporting Metrics were chosen in accordance with Executive Order (EO) 14028, *Improving the Nation's Cybersecurity,* as well as OMB guidance provided to agencies to further the modernization of federal cybersecurity. OMB released memorandum *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* (M-23-03) during FY 2023 related to updated guidance for IG FISMA reporting. This memorandum rescinded memoranda *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* (M-22-05) and *Reporting Instructions for Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones* (M-02-09) and established that Core and Supplemental Group 1 metric ratings were required to be submitted in CyberScope by July 31, 2023.

IG FISMA Scoring

OMB's *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* guidance included updated scoring methodology in which ratings in the nine metric domains (RM, SCRM, CM, IAM, DPP, ST, ISCM, IR, and CP) were determined by a calculated average, wherein the average of the metrics in a particular domain were used to determine the effectiveness of the associated cybersecurity function. When individual metric ratings are entered in CyberScope, the system automatically determines the calculated average for each domain and function.

The FY 2023 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. According to the FY 2023 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).

Table 2: Inspector General 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.

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, 2022, through May 31, 2023. Specifically, we assessed GSA's performance in the five cybersecurity functions outlined in the FY 2023 IG FISMA Reporting Metrics. To support the overall performance audit objective, we also performed an external penetration test over one public-facing GSA-owned information system and internal vulnerability scanning activities over four GSA-owned information systems. Our results for this testing are as of June 21, 2023. We conducted our fieldwork from March 22, 2023, through July 31, 2023. As part of our performance audit, we responded to the FY 2023 IG FISMA Reporting Metrics on the GSA OIG's behalf to assess maturity levels, and we also followed up on the status of prior year findings.

Scope

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation; FY 2023 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 117 systems in the GSA FISMA system inventory as of February 8, 2023. We also performed follow-up testing over seven additional GSA information systems to determine whether GSA had addressed prior year findings related to those systems.

Methodology

We conducted this performance audit in accordance with GAGAS, which requires that we plan and conduct this performance audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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

We requested that GSA management provide a self-assessment of maturity levels for the FY 2023 IG FISMA Reporting Metrics to help us gain a better understanding of how the organization implemented relevant security controls and processes for the 40 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 the information security program and practices of GSA included the following:

- Inquiry of GSA System Owners, ISSOs, ISSMs, 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 of Provided by Client (PBC) artifacts requested 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 period.

As discussed above, we also performed an external penetration test over one public-facing GSA-owned information system and internal vulnerability scanning activities over four GSA-owned information systems. Our procedures for this testing included those listed above in addition to the performance of external web application penetration testing activities and other automated/manual testing techniques used to determine whether GSA's incident response and monitoring capabilities detected attempted suspicious activity. Our results for this testing are as of June 21, 2023.

We conducted our fieldwork from March 22, 2023, through July 31, 2023. All testing was conducted remotely through virtual walkthroughs and observations with GSA management. We also periodically met with GSA management and the GSA OIG virtually to discuss our audit progress and identified findings.

Criteria

We focused our FISMA performance audit approach on federal information security guidance developed by NIST and OMB. NIST Special Publications (SPs) establish guidelines that are essential to 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 2023 in the "Audit Findings and Recommendations" section of this report.

III. Overall Results

GSA established and maintained its information security program and practices for its information systems across the five cybersecurity functions and nine FISMA metric domains consistent with applicable FISMA requirements, OMB guidance, and NIST standards. Based on the ratings for each metric and associated averages calculated in CyberScope, we determined that GSA's information security program was effective. **Table 3** below depicts assessed maturity levels for each cybersecurity function.

Table 3: Maturity Levels for Cybersecurity Functions

Cybersecurity Function / Metric Domains	Assessed Maturity Level
Identify (RM and SCRM)	Managed and Measurable (Level 4)
Protect (CM, IAM, DPP, and ST)	Optimized (Level 5)
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 two findings within the Identify and Protect cybersecurity functions. The nature of these findings did not affect our overall assessment of the Identify or Protect functions after determining the calculated average rating of the 11 IG metrics within the Identify function and the 18 IG metrics within the Protect function. **Table 4** below depicts the finding areas by function for the two reported findings.

Table 4: Summary of Finding Areas by Cybersecurity Functions

Function	Finding Area
Identify – RM	POA&Ms
Protect – IAM	Session Termination

Identify

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

Risk Management (RM)

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

Based on the results of our audit procedures, we determined that GSA management implemented policies and procedures to maintain a complete and accurate inventory of its major information systems by using a Governance, Risk, and Compliance (GRC) platform, which maintains system security information (e.g.,

accreditation status, system type, and ownership). GSA also implemented a suite of security tools to maintain an inventory of hardware devices connected to the GSA network and to track software assets and their associated licenses.
GSA management developed and implemented processes for assessing and authorizing information systems, performing risk assessments, developing and implementing secure architecture, and tracking and monitoring POA&Ms. These processes allow GSA stakeholders to identify, manage, and track cybersecurity risks that the OCISO incorporates into GSA's overall risk register. GSA management also utilized dashboards to analyze data from implemented security tools related to risks and vulnerabilities that impacted GSA information systems.

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

Additionally, we identified two performance improvement opportunities related to SSPs for selected GSA information systems. Specifically, we noted that a signature line for the Vendor ISSO was included in the SSP for each selected GSA system; however, we were informed by management that this signature was not applicable for certain selected systems because they did not have a Vendor ISSO. We recommended that, for clarity, GSA management remove this signature line for systems where Vendor ISSO signature is not required. Based on our review of audit logging requirements within selected SSPs, we also recommended that GSA management review and update the documented implementation statements for NIST SP 800-53 Audit and Accountability (AU) control AU-6 (*Audit Record Review, Analysis, and Reporting*) to clarify whether reviews are performed at a defined frequency or on an event-driven basis. We determined that these performance improvement opportunities did not rise to the level of audit findings but could further strengthen GSA's information security program if effectively addressed by management.

Supply Chain Risk Management (SCRM)

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

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

Protect

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

Configuration Management (CM)

FISMA requires agencies to develop an information security program that includes policies and procedures to ensure compliance with minimally acceptable system security configuration requirements. CM refers to processes

used to control changes/patches to information systems (i.e., change management and patch management) to establish and maintain the integrity of the systems and their underlying data.

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

Additionally, we determined that GSA management established processes related to flaw remediation, including asset discovery and vulnerability scanning across the enterprise. Vulnerability scan results are reviewed by management at defined frequencies, and vulnerabilities must be remediated within established timeframes or tracked in POA&Ms through resolution. During our independent external penetration test of one public-facing GSA-owned information system, we noted that GSA's network boundary defenses and secure configuration settings prevented the execution of our attempted attacks on the network and the selected web-based application. We did not report any findings related to GSA's CM program and associated security controls.

Identity and Access Management (IAM)

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

Based on the results of our audit procedures, we determined that GSA management developed and implemented an IAM program and strategy aligned with federal requirements and leading practices across the enterprise. Additionally, we determined that GSA management utilized tools to implement the IAM program. These tools were used to enforce multi-factor authentication, manage user accounts and monitor their behavior, and retain access authorization documentation. GSA processes related to access agreements, privileged and non-privileged user multi-factor authentication, and remote access operated effectively during the period.

However, we did report one finding related to GSA's session termination control process. Specifically, we noted that a system-level POA&M had not been developed for a session termination control implementation gap that was identified in the SSP for one GSA-owned information system as required.

Data Protection and Privacy (DPP)

DPP refers to a collection of activities focused on preserving the confidentiality, integrity, and availability of information systems and their underlying data through proper access restrictions and protections against unauthorized disclosure of information. Effectively managing risks associated with the creation, collection, use, maintenance, dissemination, disclosure, and disposal of personally identifiable information (PII) depends on the safeguards in place for the information systems that process, store, and transmit this information. OMB Circular A-130, *Managing Information as a Strategic Resource,* requires federal agencies to develop, implement, and maintain enterprise-wide privacy programs that align with the NIST Risk Management Framework to protect PII and other sensitive data. The head of each federal agency is ultimately responsible for managing PII and ensuring that privacy is protected for their agency. EO 13719, *Establishment of the Federal Privacy Council,* requires

agency heads to designate a Senior Agency Official for Privacy who has agency-wide responsibility and accountability for the agency's privacy program.
Based on the results of our audit procedures, we determined that GSA management implemented a privacy program and related security controls, such as those related to encryption and media sanitization, to protect PII and other sensitive data. GSA management utilized tools to implement security and privacy controls and monitor the network for data leaks.

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

Security Training (ST)

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

Based on the results of our audit procedures, we determined that GSA management implemented an effective security awareness training program, which included simulated phishing exercises to assess information system users' ability to identify and prevent attempts to obtain sensitive information through social engineering attacks. Performance measures to assess the effectiveness of the program, such as metrics related to training completion and successful simulated phishing attempts, were established and tracked across the enterprise. GSA management also performed detailed workforce assessments and addressed gaps in the knowledge, skills, and/or abilities of program staff through talent acquisition and training. We determined that GSA employees collectively possessed a training level that reduced the number of security incidents resulting from personnel actions/inactions throughout the period tested during our performance audit fieldwork. 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 focuses on the timely discovery of cybersecurity events. This function is critical to a robust information security program as the effects of cybersecurity events can be mitigated more quickly if they are identified in a timely manner. The NIST Cybersecurity Framework states that ISCM processes should be used to detect anomalies and continuously monitor information systems across the enterprise to identify events. The Detect function is carried out through ISCM tools and processes intended to promote timely identification of cybersecurity events.

To further enhance federal agencies' ISCM capabilities, Congress established the Continuous Diagnostics and Mitigation (CDM) Program in 2012. The CDM Program supports agency efforts to identify cybersecurity risks on an ongoing basis and prioritize risks 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 A&A processes to authorize information systems and periodically assess the implementation of required security controls. Additionally, GSA management implemented an enterprise-wide ongoing authorization (OA) program to maintain a continuous Authorization to Operate (ATO) status for the 18 GSA information systems enrolled in the program. We did not report any findings related to GSA's ISCM program and associated security controls.

Respond – Incident Response (IR)

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

Based on the results of our audit procedures, we determined that GSA management implemented an effective incident response program through the execution of incident response plans and procedures and the use of advanced incident response 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 incident response activities to relevant stakeholders in accordance with the channels defined in incident response plans and procedures.

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

Recover – Contingency Planning (CP)

The objective of the Recover function in the NIST Cybersecurity Framework is to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident or other disaster. Activities that are part of this function, such as contingency planning, 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 on recovery activities to relevant stakeholders, and to incorporate lessons learned into contingency planning. We did not report any findings related to GSA's CP program and associated security controls.

IV. Audit Findings and Recommendations

Identify – Risk Management – POA&Ms

Weaknesses were identified in the process for updating entity-wide and system-level POA&Ms on a quarterly basis in accordance with GSA policy and procedures. Specifically, we identified the following weaknesses:

- Two entity-wide POA&Ms with a status of "Delayed" had not been updated since August 2022 to indicate a rationale for the delays, milestone changes, or new scheduled completion dates in the listing.
- For one GSA-owned information system, five system-level POA&Ms with a status of "Delayed" had not been updated at the time of our testing to indicate a rationale for the delays, milestone changes, or new scheduled completion dates in the listing. Additionally, scheduled completion dates or statuses were not documented for three system-level POA&Ms for the system.
- For one GSA-owned system component, three system-level POA&Ms with a status of "Delayed" had not been updated at the time of our testing to indicate a rationale for the delays, milestone changes, or new scheduled completion dates in the listing.

The following criteria support the noted condition:

GSA Order CIO 2100.1N, *GSA Information Technology (IT) Security Policy*, dated September 21, 2022, Section 4cc, states:

> The OCISO will review POA&Ms quarterly and provide system-level and management reports in accordance with GSA CIO-IT Security-09-44.

GSA *IT Security Procedural Guide: Plan of Action and Milestones (POA&M) CIO-IT Security-09-44*, Revision 8 dated September 14, 2022, 1. Introduction states:

> The General Services Administration (GSA) requires POA&M updates to document the progress of the remediation efforts associated with identified weaknesses, including schedule changes. The GSA Office of the Chief Information Security Officer's (OCISO) Policy and Compliance Division (ISP) reviews POA&Ms on a quarterly basis.

GSA *IT Security and Privacy Procedural Guide: Common Control Catalog (CCC) CIO-IT Security-Privacy-18-90*, Revision 4 dated March 8, 2023, Control PM-4: Plan of Action and Milestones Process, states:

> **PM-4 Control Implementation**
> […]
> b. The GSA OCISO ISP Division reviews POA&Ms quarterly and coordinates reviews with the ISSOs and ISSMs. The reviews are focused on ensuring POA&Ms are accurately documented, and progress is made on resolving POA&M items in line with agency-wide priorities and risk tolerance. […] Outstanding and delayed POA&M items associated with signed and approved Acceptances of Risk (AORs) are discussed with [Authorizing Officials (AOs)] on a quarterly basis during AO sync meetings.

GSA management indicated that updates for the identified POA&Ms were consistently tracked by their respective ISSOs and ISSMs throughout the period and were documented through other processes, including SSP updates and ISSO checklists, but the updates were not captured in the POA&M listing due to a lack of oversight. For the identified GSA-owned system component, GSA management stated that two of the three identified POA&Ms were considered closed based on rationale documented in the listing. However, the POA&M statuses were not updated to reflect that the items were closed, and the listing did not include information related to completion dates, a rationale for the delays, or other information regarding milestone changes.

Entity-wide and system-level POA&M documentation provides a formal mechanism to track and manage risks associated with GSA's information systems and overall information security program. Outdated POA&Ms could

lead to unmitigated risks in the IT environment, which could be leveraged to adversely impact GSA's systems and data.

RECOMMENDATION:

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.

Identify – Risk Management – POA&Ms and Protect – Identity and Access Management – Session Termination

GSA management did not document a system-level POA&M for a control implementation gap identified in the SSP for NIST SP 800-53 Revision 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.

The following criteria support the noted condition:

GSA Order CIO 2100.1N, *GSA Information Technology (IT) Security Policy*, dated September 21, 2022, Section 4h, states:

> All information systems must develop and maintain a POA&M in accordance with GSA CIO-IT Security-09-44. POA&Ms are the authoritative agency management tool for managing system risk and are used in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in agency programs and systems.

GSA *IT Security Procedural Guide: Plan of Action and Milestones (POA&M) CIO-IT Security-09-44*, Revision 8 dated September 14, 2022, Section 5.2 states:

> System weaknesses identified by the following sources must be documented in the POA&M within one quarter of identification. ISP strongly suggests that POA&M updates be entered when the status of an entry changes and not just when quarterly submissions are due for review. […]
>
> The following sources of weaknesses must be included in POA&Ms:
> […]
> - Assessment and Authorization (A&A). Include vulnerabilities of the information system discovered during the A&A process and/or security continuous monitoring […].

GSA *IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk CIO-IT Security-06-30*, Revision 24 dated June 26, 2023, Section 5.7.4 states:

> The System Owner and ISSO will update the following items as part of the system and GSA continuous monitoring plans, processes, and program.
> - [System security and privacy plan (SSPP)] (and all appendices and attachments);
> - POA&M.

GSA management indicated that a POA&M to track the risk of the partially implemented control was not documented due to a lack of oversight.

System-level POA&M documentation provides a formal mechanism to track and manage risks associated with GSA's information systems and overall information security program. Outdated POA&Ms could lead to unmitigated risks in the IT environment, which could be leveraged to adversely impact GSA's systems and data.

RECOMMENDATION:

We recommend that GSA management document POA&Ms for any required security controls noted as partially implemented and/or planned within system security plans.

V. Conclusions

GSA management established and maintained its information security program and practices for its information systems for the five cybersecurity functions and nine FISMA metric domains during FY 2023. We assessed GSA's information security program as "Effective" within CyberScope; this determination was made because the majority of the FY 2023 IG FISMA Reporting Metrics and the associated calculated averages for the metric domains and cybersecurity functions were assessed as "Managed and Measurable" or "Optimized." Specifically, the Identify, Respond, and Recover cybersecurity functions were assessed as "Managed and Measurable," while the Protect and Detect cybersecurity functions were assessed as "Optimized." We also performed follow-up testing to determine the status of 15 prior year findings and reported that 13 of 15 were closed (see Appendix I). However, we determined that the other two prior year findings remained open, and also reported two new findings that impacted the Identify and Protect cybersecurity functions and the RM and IAM FISMA metric domains. The nature of these findings did not affect our overall assessment of the Identify or Protect functions after determining the calculated average rating of the 11 IG metrics within the Identify function and the 18 IG metrics within the Protect function.

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

VI. Agency Comments – Management Response to the Report

GSA

GSA Office of the Chief Information Officer

10/26/2023

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

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

DocuSigned by:
David Shive
A3AE4264A2754FB...

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 2023

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 2023. We agree with the findings and recommendations stated in the report.

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

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

Appendix I –
Status of Prior Year Findings

As part of the FY 2023 FISMA performance audit, we performed procedures to determine whether management closed prior year findings. Findings were closed if management provided sufficient documentation to evidence that the associated recommendations were fully implemented. Findings with recommendations that were determined to be partially implemented or not implemented remained open. As outlined in the table below, we determined that 13 of 15 prior year findings were closed.

Prior Year Findings - 2022 Evaluation

Finding Number	Prior Year Condition	Recommendation(s)	Status
1. Identify – RM **SSP**	During FY 2022, the SSPs for two GSA-owned information systems were not reviewed or updated to address any changes to the systems and their environments (if appropriate), and were not approved annually by the designated approving officials in accordance with the GSA IT Security Procedural Guide: *Managing Enterprise Cybersecurity Risk* (CIO IT Security-06-30). Moreover, one of the systems received its ATO prior to the approval of the SSP.	We recommend that GSA: 1. Document its annual reviews, updates, and approvals for system-level SSPs as required by GSA IT Security Procedural Guide. 2. Ensure system-level SSPs are authorized prior to completing a system authorization.	Closed Closed
2. Protect – IAM **Audit Log Monitoring**	GSA management noted in the SSP for one GSA-owned information system that the control AU-6: Audit Record Review, Analysis, and Reporting was partially implemented. However, no AOR was documented for this control not being fully implemented, in accordance with GSA policies. We did note that management established a POA&M for the issue in FY 2020, but its status was "delayed." Therefore, GSA management did not periodically review the application and database (DB) audit logs for the system to determine if unusual or suspicious activities were recorded within these systems' production environments. As such, management did not respond to potential activities in a timely manner.	We recommend that GSA: 1. Design and implement a quality control process to validate that designated management reviews the system's application and DB audit logs in the production environment within the timeframes established by the SSP. 2. Evaluate and document the previously reviewed logged events to confirm that the system's application production environment was not adversely affected.	Closed Closed
3. Protect – IAM **Audit Log Monitoring**	Weaknesses were noted with audit logging and access administration controls for one GSA-owned information system. Specifically, we noted:	We recommend that GSA: 1. Amend the SSP audit log review frequency to adhere to GSA IT Security Procedural	Closed

Finding Number	Prior Year Condition	Recommendation(s)	Status
Access Review and Recertification	1. Management did not develop and implement a manual or automated process to document the periodic review of privileged system user account activities. 2. System application users were required to recertify their access; however, an independent recertification by the GSA Program Management Office (PMO) was not performed.	Guide: *AU* or obtain an AOR or formal risk acceptance for system controls that do not comply with GSA IT policies and directives. 2. Develop and implement a process to document evidence of the periodic review of privileged user account activities. 3. Ensure all system users are independently recertified no less than annually, in accordance with GSA policy.	Closed Open
4. Protect – IAM **Privileged User Access Authorization**	For one GSA-owned information system, the application super-administrator granted herself an additional, less privileged, standard administrator account without appropriate approval, which did not adhere to the SSP.	We recommend that GSA ensure that all privileged access requests to the system are approved by an independent authorized approver.	Closed
5. Identify – RM **Enterprise Information Security Policy**	The GSA policies and IT procedural guides were not fully updated to be aligned with new requirements outlined in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organization*, dated September 2020. We were informed that the GSA policies and procedural guides are under review and expected to be formalized after the FISMA performance audit period of October 1, 2021 through May 31, 2022. The following 12 of 25 selected GSA policies and IT procedural guides relevant to our performance audit were not aligned and updated with new requirements outlined in the NIST SP 800-53, Revision 5, in accordance with OMB Circular No. A-130: 1. *GSA IT Security Policy* CIO 2100.1M, March 26, 2021 2. IT Security Procedural Guide: *GSA Information Security*	We recommend that GSA: 1. Finalize its updates to the GSA policies and IT security procedural guides to incorporate the new NIST SP 800-53, Revision 5 requirements. 2. Perform reviews of its policies and IT security procedural guides, consistent with the corresponding frequencies noted in GSA's ISPP.	Closed Closed

Finding Number	Prior Year Condition	Recommendation(s)	Status
	Program Plan (ISPP), CIO-IT Security-18-90, Revision 3, June 16, 2020 3. IT Security Procedural Guide: *FISMA Implementation*, CIO-IT Security-04-26, Revision 2, April 16, 2019 4. IT Security Procedural Guide: *Plan of Action and Milestones*, CIO-IT Security-09-44, Revision 6, August 25, 2021 5. IT Security Procedural Guide: *Identification and Authentication (IA)*, CIO-IT Security-01-01, Revision 6, March 20, 2019 6. IT Security Procedural Guide: *Access Control*, CIO-IT Security-01-07, Revision 4, May 8, 2017 7. IT Security Procedural Guide: *Audit and Accountability (AU)*, CIO-IT Security-01-08, Revision 6, December 3, 2020 8. IT Security Procedural Guide: *Security and Privacy Awareness and Role Based Training Program*, CIO-IT Security-05-29, Revision 6, May 1, 2020 9. IT Security Procedural Guide: *CP*, CIO-IT Security-06-29, Revision 5, July 27, 2020 10. IT Procedural Guide: *ISCM Strategy & OA Program*, CIO-IT Security-12-66, Revision 3, April 23, 2020 11. IT Security Procedural Guide: *Web Server Log Review*, CIO-IT Security-08-41, Revision 4, March 30, 2020 12. IT Security Procedural Guide: *System and Information Integrity (SI)*, CIO-IT Security-12-63, Revision 2, February 7, 2019 Additionally, we noted five of GSA's policies and IT security procedural guides were not reviewed or updated in accordance with their		

Finding Number	Prior Year Condition	Recommendation(s)	Status
	corresponding frequencies noted in GSA's ISPP: 1. IT Security Procedural Guide: *GSA ISPP*, CIO-IT Security-18-90, Revision 3, June 16, 2020 2. IT Security Procedural Guide: *FISMA Implementation*, CIO-IT Security-04-26, Revision 2, April 16, 2019 3. IT Security Procedural Guide: *IA*, CIO-IT Security-01-01, Revision 6, March 20, 2019 4. IT Security Procedural Guide: *Access Control*, CIO-IT Security-01-07, Revision 4, May 8, 2017 5. IT Security Procedural Guide: *SI*, CIO-IT Security-12-63, Revision 2, February 7, 2019		
6. Protect – IAM **Access Authorization**	Management indicated that it does not require documented approvals prior to granting individuals access to one GSA-owned information system. Further, because of a system upgrade, all system application administrator accounts were recreated without documented access approvals as management relied on verbal authorizations from the approving official.	We recommend that GSA: 1. Enforce proper completion of application administrator requests forms to include obtaining authorizations from designated management authorizations prior to provisioning administrator access to the system's application. 2. Validate that access is appropriate for all system application administrator accounts.	Closed Closed
7. Protect – CM **Flaw Remediation**	The version of the DB that was in production and supporting one GSA-owned information system was no longer supported by the vendor as of February 2021. In addition, installation of a software application on the remote host that was in production and supporting the system was no longer supported by the vendor as of 2016. Finally, one critical and three high vulnerabilities were not remediated for at least two months as of February 2022.	We recommend that GSA: 1. Design and implement a monitoring process to track and identify system software components that are no longer supported by vendors. 2. Test and update the system DB to a current supported version, as appropriate. 3. Design and implement a quality control process to	Closed Closed Closed

Finding Number	Prior Year Condition	Recommendation(s)	Status
	The system team did not obtain a formal AOR for not upgrading the DB version and installing the security patches and did not establish a POA&M to mitigate security risks.	validate that designated management authorizes system DB patches prior to implementing the patches in the production environment within the timeframes established by GSA IT Procedural Guide: *Vulnerability Management Process*, CIO-IT Security-17-80. 4. Test and implement the missing security patch for the system DB. 5. Obtain a formal AOR when determining not to implement updated software versions and patches for system devices and establish POA&Ms to mitigate the corresponding security risks.	Closed Closed
9.[7] Protect – CM **Flaw Remediation**	GSA management did not remediate identified high-risk vulnerabilities for one GSA-owned information system environment within 30 days as required by GSA IT security policy. Specifically, we noted the following: 1. GSA management did not remediate one high-risk vulnerability relating to the DB software version until 43 days after it was identified through GSA's January 11, 2022 vulnerability scan. Additionally, GSA management did not appropriately track the vulnerability in a POA&M and did not obtain a formal risk waiver to extend the remediation period. 2. From July 12, 2022 through August 30, 2022, we conducted	We recommend that GSA: 1. Formally document and track all critical, high, and moderate-risk vulnerabilities for the system in its POA&M process, in accordance with agency policies. 2. Ensure that all identified vulnerabilities are remediated by the timeframes established in *GSA IT Security Policy* or obtain a formal risk waiver if more time is needed to address a vulnerability. 3. Develop and implement a process to ensure follow-up validation tests are performed after remediating a	Closed Closed Closed

[7]NFR FISMA-2022-08 was not issued in final during the prior year because it was withdrawn; as a result, the FY 2022 NFR numbering skips 8.

Finding Number	Prior Year Condition	Recommendation(s)	Status
	an external penetration test of the system's public-facing website and identified a high-risk vulnerability. Management indicated that the exploit was also previously identified during the February 2022 annual penetration test conducted by GSA; however, it was not remediated before we started our external penetration test. We noted that GSA's February 2022 annual test reported 17 instances of the exploit as a "moderate" risk vulnerability. However, when we conducted our testing starting on July 12, 2022, we identified 43 instances that had not been remediated within the timeline set for in GSA IT security policy for internet-accessible systems. Additionally, the vulnerability noted in GSA's annual penetration test was not appropriately tracked and updated within GSA's POA&M process. The vulnerability was added to the POA&M report July 11, 2022, which was five months after initial identification.	vulnerability. 4. Perform vulnerability scans prior to system upgrades and cutovers to ensure vulnerabilities are not introduced by the new system. 5. Evaluate the Agency's current web application security testing software to ensure it is configured and capable of identifying the vulnerabilities in their environment.	Closed Closed
10. Protect – IAM **Access Authorization**	GSA management did not document its authorization of access for two of two new operating system (O/S) administrators and two of two new application administrators supporting one GSA-owned information system, which did not adhere to the SSP and *GSA IT Security Policy* CIO 2100.1M.	We recommend that GSA: 1. Enforce proper completion of application administrator and O/S administrator request forms to include obtaining authorizations from designated management prior to provisioning administrator access to the system's application and O/S, respectively. 2. Validate that access is appropriate for all system application and O/S administrator accounts.	Closed Open

Finding Number	Prior Year Condition	Recommendation(s)	Status
11. Protect – CM **Change Management**	During FY 2022, weaknesses in CM controls for one GSA-owned information system were noted. Specifically, we noted the following actions were not performed prior to migration to production: • Successful testing could not be provided for 12 of 15 system application changes selected. • Appropriate management approval could not be provided for 10 of 15 system application changes selected.	We recommend that GSA: 1. Ensure that evidence of successful testing and approval is documented and retained for system application changes prior to implementation. 2. Evaluate and document the unapproved system application changes to confirm that the production environment was not adversely affected.	Closed Closed
12. Protect – CM **Patch Management**	For one of two DB patches tested for one GSA-owned information system, GSA management did not document evidence of authorization or testing prior to its implementation into production.	We recommend that GSA: 1. Adhere to GSA policy for documenting authorizations and testing of system DB patches prior to their implementation in the production environment. 2. Evaluate and document the unapproved system DB patches to confirm that the system's production environment was not adversely affected.	Closed Closed
13. Protect – CM **Change Management**	The following weaknesses were noted while testing application configuration controls for one GSA-owned information system: • For three of five system application changes selected, evidence of successful testing could not be provided. • For five of five system application changes selected, evidence of approval could not be provided.	We recommend that GSA: 1. Ensure that evidence of successful testing and approval before implementation in the production environment is documented and retained for system application changes. 2. Evaluate and document the unapproved system application changes. 3. Evaluate if a ticketing system is needed for the system application to track change management activities.	Closed Closed Closed
14. Protect – CM	GSA management configured the O/S and DB for one GSA-owned	We recommend that GSA: 1. Adhere to GSA's CM	Closed

Finding Number	Prior Year Condition	Recommendation(s)	Status
Patch Management	information system to install automatic patches from the vendors, but management could not provide evidence that it tested and authorized the patches.	policy and the system's policy for documenting authorizations and testing of system O/S and DB patches prior to their implementation in the production environment. 2. Evaluate and document the unapproved system O/S and DB patches to confirm that the production environment was not adversely affected.	Closed
15. Protect – CM **Change Management**	Controls to formally authorize changes to one GSA-owned information system's environment were not fully designed and implemented. Specifically, there was no supporting documentation evidencing that the designated approving official's authorization of system application, DB, and O/S changes and patches occurred prior to their implementation into the production environment.	We recommend that GSA develop and implement procedures to require the documentation and retention of the Configuration Control Board's (CCB) authorization of system application, DB, and O/S changes and patches prior to their implementation in the production environment.	Closed
16. Protect – IAM **Audit Log Monitoring**	Management did not consistently develop and implement a process to document the periodic review of privileged user account activities for the production application, DB, and O/S for one GSA-owned information system.	We recommend that GSA develop and implement a process to document evidence of the periodic review of privileged system user account activities for the application, DB, and O/S levels, including the review of relevant administrators from external agencies.	Closed

Appendix II – Glossary

Acronym	Definition
A&A	Assessment and Authorization
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
AOR	Acceptance of Risk
ATO	Authorization to Operate
AU	Audit and Accountability
CCB	Configuration Control Board
CCC	Common Control Catalog
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CM	Configuration Management
CP	Contingency Planning
CTO	Chief Technology Officer
DB	Database
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DPP	Data Protection and Privacy
EO	Executive Order
FAS	Federal Acquisition Services
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
FY 2023 IG FISMA Reporting Metrics	FY 2023 Core and Supplemental Group 1 IG Metrics
GAGAS	Generally Accepted Government Auditing Standards
GRC	Governance, Risk, and Compliance
GSA	General Services Administration
IA	Identification and Authentication
IAM	Identity and Access Management
IG	Inspector General
IR	Incident Response
ISCM	Information Security Continuous Monitoring
ISPP	Information Security Program Plan
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
KPMG	KPMG LLP
NIST	National Institute of Standards and Technology
OA	Ongoing Authorization
OCIO	Office of the Chief Information Officer
OCISO	Office of the Chief Information Security Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget

Acronym	Definition
O/S	Operating System
PBC	Provided by Client
PBS	Public Buildings Services
PII	Personally Identifiable Information
PMO	Program Management Office
POA&M	Plan of Action and Milestones
RM	Risk Management
SCRM	Supply Chain Risk Management
SI	System and Information Integrity
SIEM	Security Information and Event Management
SP	Special Publication
SSO	Service and Staff Offices
SSP	System Security Plan
SSPP	System Security and Privacy Plan
ST	Security Training
U.S.	United States
US-CERT	United States Computer Emergency Readiness Team