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 2022

November 14, 2022

KPMG LLP
8350 Broad Street Suite 900
McLean, VA 22102

Donna Peterson-Jones
Supervisory Auditor/FISMA COR
General Services Administration
Office of Inspector General
1800 F St., NW, Suite 5037
Washington, DC 20405

CC: Carolyn Presley-Doss, Deputy Assistant Inspector General for Audit Policy and Oversight, and Bonnie Impastato, Team Lead - Contracting Officer

November 14, 2022

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 2022*. This report is provided to you in the format according to our contract GS-00F-275CA, order number 47HAA021F0040, modification PS0002, dated January 15, 2022, 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 FY 2022 FISMA Report are recommendations to address specific GSA and system-level findings within GSA's information security program and practices. When developing plans of actions and milestones or corrective actions, 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 GSA's 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 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 2022

November 14, 2022

Executive Summary

Why We Performed This Audit

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the 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") 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.

As recommended by the Office of Management and Budget's (OMB's) *Office of the Federal Chief Information Officer FY22 Core Inspector General (IG) Metrics Implementation Analysis and Guidelines,* we also performed technical security testing, consisting of an external penetration test and a vulnerability assessment.

KPMG conducted a performance audit of GSA's information security program in accordance with Generally Accepted Government Auditing Standards (GAGAS) and with the 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 October 1, 2021 through May 31, 2022. In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by the American Institute of Certified Public Accountants. The technical security testing was performed as of August 30, 2022.

What We Found

Our testing for Fiscal Year (FY) 2022 included performing procedures at the entity level for seven GSA-operated information systems and three contractor-operated information systems. We also followed up on the status of 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 to be "Effective," in accordance with OMB guidance, based on our assessment of the majority of the FY 2022 Core IG Metrics (FY 2022 Core IG Metrics) as "Managed and Measurable" or "Optimized." Specifically, the Identify, Protect, Detect, and Respond Cybersecurity functions were assessed as "Optimized," while the Recover function was assessed as "Managed and Measurable."

[1] CyberScope, operated by the Department of Homeland Security (DHS) on behalf of OMB, is a web-based application designed to streamline information technology (IT) security reporting for federal agencies. It gathers and standardizes data from federal agencies to support FISMA compliance. In addition, IGs provide an independent assessment of effectiveness of an agency's information security program. OIGs must also report their results to DHS and OMB annually through CyberScope.

Based on our testing, we determined that GSA implemented corrective actions to remediate the four prior-year findings and that these findings are closed (see Appendix I). However, we reported 10 new findings (see Section IV) in the Identify and Protect functions:

Cybersecurity Function - Identify
- Enterprise Information Security Policy – Weaknesses in GSA's compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5 (Risk Management)

Cybersecurity Function - Protect
- Flaw Remediation – Controls over flaw remediation not consistently implemented for two information systems (Configuration Management [CM])
- Patch Management – Controls over patch management not consistently implemented for two information systems (CM)
- Change Management – Authorization of application, database (DB), and operating system (O/S) changes not documented for one information system's production environment (CM)

Cybersecurity Function - Protect
- Audit Log Monitoring – Weaknesses in application, DB, and O/S audit log reviews for three information systems (Identity and Access Management)
- Privileged User Access Authorization – Weaknesses in authorization of new privileged application user access for one information system (Identity and Access Management)
- Access Authorization – Weaknesses in authorization of new users for two information systems' environments (Identity and Access Management)
- Access Review and Recertification – One information system's application user accounts not reviewed and recertified by an independent GSA Project Management Office (PMO) (Identity and Access Management)

The nature of these findings did not affect our overall assessment of the Identify or Protect functions after determining the mode of the six Identify IG metric questions and the eight Protect IG metric questions.

To support the overall performance audit objective, additional test procedures were performed on the GSA's risk management, application-level CM, and contingency planning controls that were not covered in the FY 2022 Core IG Metrics. Specifically, an assessment of the agency's controls for Authorization to Operate (ATO), System Security Plans (SSPs), Plan of Action and Milestones (POA&Ms), system backups, and application-level change management was performed. These additional test procedures will not impact the overall CyberScope score. We also performed an external penetration test and vulnerability scanning activities over a selected GSA information system's website to identify potential system flaws, misconfigurations, and vulnerabilities that could allow unauthorized access or elevation of privileges to GSA IT. As a result, we identified the following:

Cybersecurity Function – Identify
- SSP – SSPs not reviewed, updated, and approved for two information systems (Risk Management)

Cybersecurity Function – Protect
- Change Management – Application change approval and testing not consistently documented for two information systems (CM)

What We Recommend

We made 35 recommendations related to the 10 control findings that should strengthen GSA's information security program if effectively addressed by management. GSA should also implement a process to determine if these recommendations apply to other information systems maintained in its FISMA inventory.

We recommend that GSA management:

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 Information Security Program Plan (ISPP).
3. Document evidence of annual reviews, updates, and approvals for system-level SSPs, for both information systems, as required by GSA IT Security Procedural Guide.
4. Ensure system-level SSPs are authorized prior to completing a system authorization.
5. Design and implement a monitoring process to track and identify information system software components that are no longer supported by vendors.
6. Test and update the information system's DB to a current supported version, as appropriate.
7. Design and implement a quality control process to validate that designated management authorizes the information system's DB patches prior to implementing the patches in the production environment within the timeframes established by GSA IT Procedural Guide: *Vulnerability Management Process*, Chief Information Officer (CIO)-IT Security-17-80.
8. Test and implement the missing security patch for the information system's DB.
9. Obtain a formal Acceptance of Risk (AOR) when determining not to implement updated software versions and patches for the information system's devices and establish POA&M to mitigate the corresponding security risks.
10. Formally document and track all critical, high-risk, and moderate-risk vulnerabilities for the information system in its POA&M process, in accordance with agency policies.
11. 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.
12. Develop and implement a process to ensure follow-up validation tests are performed after remediating a vulnerability.
13. Perform vulnerability scans prior to system upgrades and cutovers to ensure vulnerabilities are not introduced by the new system.
14. Evaluate the agency's current web application security testing software to ensure it is configured and capable of identifying the vulnerabilities in their environment.
15. Adhere to GSA policy for documenting authorizations and testing of the information system's DB patches prior to their implementation in the production environment.
16. Evaluate and document the unapproved information system's DB patches to confirm that the production environment was not adversely affected.
17. Adhere to GSA's CM policy and the information system's policy for documenting authorizations and testing of the information system's O/S and DB patches prior to their implementation in the production environment.
18. Evaluate and document the unapproved information system's O/S and DB patches to confirm that the production environment was not adversely affected.
19. Ensure that evidence of successful testing and approval is documented and retained for the first information system's application changes prior to implementation.
20. Evaluate and document the unapproved application changes to the first information system to confirm that the production environment was not adversely affected.

21. Ensure that evidence of successful testing and approval before implementation in the production environment is documented and retained for the second information system's application changes.
22. Evaluate and document the unapproved application changes for the second information system.
23. Evaluate if a ticketing system is needed for the second information system's application to track change management activities.
24. Develop and implement procedures to require the documentation and retention of the Change Control Board's (CCB's) authorization of the third information system's application, DB, and O/S changes and patches prior to their implementation in the production environment.
25. Design and implement a quality control process to validate that designated management reviews the information system's application and DB audit logs in the production environment within the timeframes established by the information system's SSP.
26. Evaluate and document the previously reviewed logged events to confirm that the first information system's application production environment was not adversely affected.
27. Develop and implement a process to document evidence of the periodic review of privileged user account activities for the second information system's application, DB, and O/S levels, including the review of relevant administrators from external agencies.
28. Amend the third information system's System Security & Privacy Plan (SSPP) audit log review frequency to adhere to GSA IT Security Procedural Guide: *Audit and Accountability* (AU) or obtain an AOR or formal risk acceptance for the information system's controls that do not comply with GSA IT policies and directives.
29. Develop and implement a process to document evidence of the periodic review of privileged user account activities.
30. Ensure that all privileged access requests to the information system are approved by an independent authorized approver.
31. Enforce proper completion of application administrator request forms to include obtaining authorizations from designated management prior to provisioning administrator access to the first information system's application.
32. Validate that access is appropriate for all of the first information system's application administrator accounts.
33. 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 second information system's application and O/S, respectively.
34. Validate that access is appropriate for all of the second information system's application and O/S administrator accounts.
35. Ensure all of the information system's users are independently recertified no less than annually, in accordance with GSA policy.

GSA agreed with our findings and recommendations and the Chief Information Officer's response is included in Section VI.

Contents

I. KPMG Letter

Administrator and Inspector General
U.S. General Services Administration
1800 F Street NW
Washington, DC 20405

Independent Performance Audit on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2022

This report presents the results of KPMG LLP's ("KPMG's") independent performance audit of the U.S. General Services Administration's (GSA's) information security program and practices for its information systems as of May 31, 2022. We conducted our performance audit from May 12, 2022 through August 12, 2022. We also performed technical security testing, consisting of an external penetration test and a vulnerability assessment, and the results are as of August 30, 2022.

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 objectives of this performance audit were to determine the effectiveness of GSA's information security program and practices for its information systems for the period October 1, 2021, through May 31, 2022 in the five security function areas outlined in the Fiscal Year (FY) 2022 Core Inspector General (IG) Metrics (FY 2022 Core IG 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 2022 Core IG Metrics were assessed as "Managed and Measurable" or "Optimized." Specifically, the Identify, Protect, Detect, and Respond Cybersecurity functions were assessed as "Optimized," while the Recover function was rated as "Managed and Measurable."

To support the overall performance audit objective, additional test procedures were performed on the GSA's risk management, application-level configuration management (CM), and contingency planning controls that were not covered in the FY 2022 Core IG Metrics. Specifically, an assessment of the agency's controls for Authorization to Operate (ATO), System Security Plans (SSPs), Plan of Action and Milestones (POA&Ms), system backups, and application-level change management was performed. These additional test procedures will not impact the overall CyberScope score. We also performed an external penetration test and vulnerability scanning activities over a selected system to identify potential system flaws, misconfigurations, and vulnerabilities that could allow unauthorized access or elevation of privileges to GSA Information Technology (IT).

KPMG cautions 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, 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 14, 2022

II. Background, Objective, Scope, and Methodology

Background

KPMG performed the FY 2022 independent FISMA evaluation under contract with GSA as a performance audit in accordance with GAGAS and AICPA Consulting Standards. The GSA OIG monitored our work to ensure we met professional standards and contractual requirements.

Agency Overview[2]

The mission of GSA is to deliver the best value in real estate, acquisition, and technology services to the government and ultimately save money for the American taxpayer. GSA's four strategic goals—savings, efficiency, technology modernization, and shared services—align the agency's mission, set direction, and guide operational planning.

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, including legal, communications, information technology (IT), and congressional affairs. In addition, 11 regional offices serve federal customers nationwide.

GSA is the government landlord, creating a 21st century workplace across government to drive down costs and increase productivity. GSA is also the premier source for equipment, supplies, telecommunications, and integrated IT to federal agencies. GSA has an annual contract volume of over $60 billion, manages over 200,000 fleet vehicles, assists tens of thousands of federal travelers through GSA's electronic travel system, and serves as the focal point for data, information, and services offered by the federal government to its citizens. About 12,000 employees provide valuable support to other federal agencies and the general public.

Although GSA leverages billions of dollars in the marketplace, only 1 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 enables the agency's mission by delivering innovative, collaborative, and valuable IT solutions and services to its customers. GSA IT comprises seven offices:

- *GSA's Chief Information Officer (CIO) (I)*
  - Manages the agency's IT budget to help ensure alignment with agency and administration strategic objectives and priorities.
  - Plays a central role in modernizing the agency's enterprise application portfolio, formulating, and implementing the digital government strategy for GSA, and establishing enterprise IT project management processes.

[2] The agency and program overview information are as of September 15, 2022.

- *Office of the Deputy CIO (ID)*
  - Serves as an advisor to the CIO, Administrator, and other senior GSA officials on technology and data management initiatives, leveraging technology for innovative business practices and leading enterprise-wide modernization efforts.

- *Office of Corporate IT Services (IC)*
  - Provides enterprise solutions for GSA's IT systems portfolio.
  - Advises GSA's Service and Staff Offices [S/SO] on IT tools that support and enhance GSA's enterprise functions.
  - Focuses on the delivery of innovative IT platforms, services, and solutions for the GSA IT enterprise.

- *Chief Technology Officer (CTO)*
  - Works across GSA IT and GSA business lines to help ensure that solutions developed by IT organizations are forward thinking, designed efficiently, and incorporated into the shared services catalog as appropriate.
  - Identifies emerging technologies and incorporates them into the existing technology portfolio as part of the overarching technology strategy for GSA.

- *Office of Public Buildings Information Technology Services (PB-ITS/IP)*
  - Provides enterprise solutions for GSA's real estate mission and buildings portfolio.
  - Focuses on the delivery of innovative workspace IT programs, services, and solutions. IT and project management experts in PB-ITS understand the PBS real estate business requirements and its federal customers' unique workspace needs.

- *Office of Acquisition Information Technology Services (IQ)*
  - Provides transformational system development, incremental system development, operational, and management services for FAS business applications.
  - Advises FAS leadership and program areas on IT tools that support and enhance FAS's business operations. IQ is organizationally aligned to the FAS business areas to deliver the IT services, systems, and functions they need most effectively. Additionally, IQ provides cloud integration technology functions as a shared service for all of GSA IT.

- *Office of Chief Information Security Officer (OCISO) (IS)*
  - Manages the GSA IT Security Office, which is responsible for the development and maintenance of the GSA IT Security Program. Provides services and expertise across the agency to implement and maintain the IT Security Program and establishes and promulgates IT security policies, procedures, controls, and guidelines.
  - Monitors efforts to mitigate vulnerabilities affecting the GSA Enterprise in a timely manner, manages the annual FISMA assessment process, and conducts continuous monitoring of GSA systems and the Agency Incident Response Program. In addition, OCISO provides and monitors required enterprise IT security awareness and role-based training for GSA.

- Works to improve identity credential coordination and governance across GSA IT and develops/delivers enterprise certificate and key management capabilities. Additionally, the OCISO is responsible for managing Cyber Supply Chain Risk Management (C-SCRM) assurance for GSA IT and supports agencywide C-SCRM activities. OCISO also includes five divisions:
  - *Security Engineering Division (ISE)* – Provides security consulting and engineering support for systems, emerging IT, and IT security initiatives. In addition, ISE provides incident response and technical benchmarks. ISE directly supports IT division offices in developing technical security standards and architectural security standards in the support of IT systems. ISE also supports software security testing in support of the IT Standards process.

  - *Identity, Credential, and Access Management Shared Service Division (ISI)* – Supports consolidating Identity, Credential, and Access Management (ICAM)-related capabilities to focus on improving ICAM coordination and governance across GSA IT and development/delivery of enterprise certificate and key management capabilities. ISI is also responsible for managing C-SCRM assurance for GSA IT and supports agencywide C-SCRM activities.

  - *Security Operations (SecOps) Division (ISO)* – 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).

  - *Policy and Compliance Division (ISP)* – Provides management and maintenance of the GSA Plan of Action and Milestones (POA&M), Continuous Monitoring Program, and Security Awareness and Role Based Training Programs. ISP also manages the process to create and maintain GSA IT security policies and coordinates cybersecurity audits and the FISMA compliance agency reporting process, which directly supports the IT systems that are being developed by GSA IT division offices. ISP provides information to the Chief Information Security Officer (CISO) and Authorizing Officials (AO) to monitor the implementation of the GSA IT Security policy.

  - *Information System Security Officer (ISSO) Support Division (IST)* – Provides ISSO and Information System Security Manager (ISSM) support services to all Staff Offices and Services systems. The division facilitates integrating IT security in programs and compliance with required security and privacy requirements. Services provided by IST assist the CISO and AOs during the assessment process to grant an Authority to Operate.

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 (1) reestablishment of the oversight authority of the Director of the OMB with respect to agency information security policies and practices, and (2) 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

For FY 2022, OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) continued to develop the FY 2022 Core IG Metrics[3] around five Cybersecurity functions outlined in the *National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity*[4] (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. In addition, FY 2022 Core IG Metrics use the CIGIE maturity models for the nine metric domains: Risk Management (RM), Supply Chain Risk Management (SCRM), CM, Identity and Access Management (IAM), Data Protection and Privacy (DPP), Security Training (ST), Information Security Continuous Monitoring (ISCM), Incident Response (IR), and Contingency Planning (CP). **Table 1** outlines the alignment of the Cybersecurity Framework to the FISMA Metric Domains.

Table 1: Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FISMA Metric Domains in the FY 2022 Core IG Metrics

Cybersecurity Framework Functions	FISMA Metric Domains
Identify	RM SCRM
Protect	CM IAM[5] DPP ST
Detect	ISCM
Respond	IR
Recover	CP

[3] The FY 2022 Core IG Metrics are described in OMB's *FY 2022 Core IG Metrics Implementation Analysis and Guidelines.*

[4] 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.

[5] Note that IAM is interchangeable with ICAM. CyberScope uses the term IAM, where ICAM is referenced in the *FY 2022 Core IG FISMA Metrics Evaluation Guide*. To be consistent with prior reports and CyberScope, this report will reference IAM.

Changes for FY 2022 Metrics

The FY 2022 Core IG Metrics were chosen based on alignment 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 provided the following guidance: *Moving the United States (U.S.) Government Toward Zero Trust Cybersecurity Principles* (M-22-09)*, Multifactor Authentication (MFA) and Encryption* (discussed in M-22-05)*, Improving the Federal Governments' Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (M-21-31)*, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (M-22-01)*, and Software Supply Chain Security & Critical Software* (Section 4 of EO 14028).

In addition, OMB M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements,* adjusted the timeline for the IG evaluation. Specifically, M-22-05 required that a core group of metrics be evaluated annually, and the remainder of the metrics be evaluated on a two-year cycle, agreed to by the CIGIE, Chief Information Security Officer Council, OMB, and Cybersecurity and Infrastructure Security Agency.

IG FISMA Scoring

The ratings in the nine domains (RM, SCRM, CM, IAM, DPP, ST, ISCM, IR, and CP) were determined by a simple majority or mode, with the most frequently assessed metric level across the metric questions serving as the domain rating. When responses are entered in CyberScope, it calculates the rating for each domain and function.

The maturity model has five levels: Level 1: Ad-hoc, Level 2: Defined, Level 3: Consistently Implemented, Level 4: Managed and Measurable, and Level 5: Optimized.[6] **Table 2** details the five maturity levels to assess the agency's information security program for each Cybersecurity Framework function. A security program is considered effective if a simple majority of the FY 2022 Core IG Metrics are at least Level 4: Managed and Measurable.

[6] The maturity levels are defined in OMB's *FY 2022 Core IG Metrics Implementation Analysis and Guidelines.*

Table 2: Inspector General Assessed Maturity Levels

Maturity Level	Description
Level 1: Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy 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 strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, 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 October 1, 2021 through May 31, 2022. Specifically, we assessed the GSA's performance in the five Cybersecurity Functions outlined in the FY 2022 Core IG Metrics. To support the overall performance audit objective, additional test procedures were performed on the GSA's risk management, application-level CM, and contingency planning controls that were not covered in the FY 2022 Core IG Metrics. We also performed an external penetration test and vulnerability scanning activities over the selected GSA information system's website, and the results are as of August 30, 2022. We performed our fieldwork from May 12, 2022 through August 12, 2022. As part of our performance audit, we responded to the FY 2022 Core IG Metrics on the GSA OIG's behalf to assess the maturity levels and followed up on the status of prior-year findings.

Scope

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation; FY 2022 Core IG Metrics; applicable NIST standards and guidelines, presidential directives, and OMB memorandums 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 (seven GSA-operated information systems and three contractor-operated information systems) from a total population of 117 major applications and general support systems as of April 6, 2022. We also performed follow-up testing on three GSA information systems to determine if GSA had closed the prior-year findings.

Methodology

We conducted this performance audit in accordance with 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 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 communicate its self-assessed maturity levels, where applicable, to assist us in our understanding of how GSA implemented relevant security controls and processes for the 20 questions in the FY 2022 Core IG Metrics. GSA described the applicable policies, procedures, and processes. This allowed us to design our audit procedures and request the appropriate artifacts for the respective maturity levels for each question in the FY 2022 Core IG Metrics.

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

- Inquiry of information system owners, ISSOs, ISSMs, system administrators, and other relevant individuals to walk through each control process.
- An inspection of the information security practices and policies established by the GSA IT.
- An inspection of the information security practices, policies, and procedures in use across GSA.
- An inspection of artifacts to determine the design, implementation, and operating effectiveness of security controls at the program and system levels.

Besides assessing the maturity levels of the FY 2022 Core IG Metrics and to support the FY 2022 performance audit objective, we also performed additional test procedures on the GSA's risk management, application-level CM, and contingency planning controls that were not covered in the FY 2022 Core IG Metrics. Specifically, an assessment of the agency's controls for ATO, SSPs, POA&Ms, system backups, and application-level change management was performed. These additional test procedures will not impact the overall CyberScope score. We also performed an external penetration test and vulnerability scanning activities over the selected GSA information system's website to identify potential system flaws, misconfigurations, and vulnerabilities that could allow unauthorized access or elevation of privileges to GSA IT.

We performed our fieldwork from May 12, 2022 through August 12, 2022. Due to the Coronavirus disease 2019 pandemic, all testing was performed remotely through virtual meetings, walk-throughs, and observations with representatives of GSA. We met with GSA management and the OIG virtually to discuss our report findings during our performance audit.

Criteria

We focused our FISMA performance audit approach on federal information security guidance developed by NIST and OMB. NIST SPs provide guidelines that are essential to the development and implementation of agencies' security programs. We also utilized GSA's information security policy directives, which outline GSA's requirements for information security. We included the relevant GSA criteria for each finding detailed in the "Audit Findings and Recommendations" section.

III. Overall Results

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, GSA established and maintained its information security program and practices for its information systems for the five Cybersecurity functions and nine FISMA metric domains. Based on the maturity levels calculated in CyberScope, we determined that GSA's information security program was effective. **Table 3** below depicts the maturity levels for the five Cybersecurity functions.

Table 3: Maturity Levels for Cybersecurity Functions

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

Although we assessed GSA's information security program as effective, we reported 10 findings that impact practices in the Identify and Protect functions. The nature of these findings did not affect our overall assessment of the Identify or Protect function after determining the mode of the six Identify IG metric questions and the eight Protect IG metric questions. **Table 4** below depicts the finding areas by function for the 10 reported findings.

Table 4: Summary of Finding Areas by Cybersecurity Functions

Function	Finding Area
Identify – RM	Enterprise Information Security Policy
Identify – RM	SSP
Protect – CM	Flaw Remediation
Protect – CM	Patch Management
Protect – CM	Change Management
Protect – IAM	Audit Log Monitoring
Protect – IAM	Privileged User Access Authorization
Protect – IAM	Access Authorization
Protect – IAM	Access Review and Recertification

Identify

The objective of the Identify function in the Cybersecurity Framework is to manage cybersecurity risk to the systems, people, assets, data, and capabilities of GSA. When an agency understands the cybersecurity risks that threaten its mission and services, it can establish controls and processes to manage and prioritize risk management decisions.

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 stem from various sources, including budget uncertainty, natural disasters, and cybersecurity threats. A sound risk management plan and program that has been developed to address the various risks can provide impactful information to an agency when establishing an information security program.

As a result of our performance audit procedures, we determined that GSA 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 information (e.g. accreditation status, system type, and ownership). GSA used other tools to maintain an inventory of hardware devices connected to the GSA network. GSA used tools, its GRC platform, and a ticketing system to track entitlements for tracking software assets.

GSA developed and implemented a process for 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.

Using native dashboards in its cybersecurity tools, GSA views risks and vulnerabilities that impact GSA information systems. Stakeholders base their risk-management decisions on these risks and vulnerabilities.

However, we did report a finding for GSA's enterprise information security policies. Specifically, we noted that not all of GSA's entity-wide policies and procedural guides were aligned with new requirements outlined in the NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organization*. Moreover, we noted GSA's policies and IT security procedural guides were not reviewed or updated in accordance with the corresponding frequencies noted in GSA's Information Security Program Plan (ISPP). Additionally, we noted weaknesses with the agency's system security plan review and authorization for two of seven GSA-operated information systems.

Supply Chain Risk Management (SCRM)

SCRM requires agencies to develop policies, procedures, and programs to manage supply chain risks associated with systems' 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 did not report any findings with GSA's SCRM program and associated security controls. We noted that GSA has created an SCRM Executive Board responsible for agency-wide governance and updated and created specific SCRM policy and procedure guides. GSA also uses third-party tools to provide suppliers' risk factors. GSA also has detailed guides for monitoring contractor-operated information systems. This includes the use of the GRC platform to for information security monitoring and review.

Protect

The objective of the Protect function in the Cybersecurity Framework is to develop and implement appropriate safeguards to ensure the delivery of critical services of GSA. The Protect function supports GSA's ability to limit, contain, or prevent the impact of a cybersecurity event. This function is carried out by 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 configuration requirements. CM refers to a collection of activities that establish and maintain the integrity of products and information systems through processes for initializing, changing, authorizing, and monitoring their configurations. This includes patch and application change management.

As a result of our performance audit procedures, we determined that GSA documented performance measures to determine the effectiveness of its CM process. GSA established an Engineer Review Board and Change Approval Board, configuration and change management processes, and configuration and change management performance measures and monitoring.

We determined GSA had processes to identify the compliance of its information systems with common secure configurations and established a formal process to remediate or approve deviations from its established common secure configurations. GSA monitored configuration compliance through endpoint detection and response and configuration/patch management tools and forwarded biweekly configuration compliance reports to stakeholders.

Additionally, we determined GSA performed weekly vulnerability scanning to identify outstanding vulnerabilities associated with missing patches. We determined that GSA followed its policy by implementing patches timely or documenting the noncompliance with an authorized acceptance of risk (AOR). We also determined that GSA closed the one prior-year CM issue.

During our independent external penetration test of an information system's website, we noted GSA's network boundary defenses and system configuration prevented the execution of network and web application-based attacks. Also, the information system's website functionality and design restrictions made it more difficult to find attack vectors.

However, we did report multiple findings for CM. Specifically, an information system's support team had unsupported software with un-remediated critical and high-risk vulnerabilities that were not tracked for remediation in the information system's POA&M. Similarly, another information system's support team had an un-remediated high vulnerability that was not tracked for remediation in the information system's POA&M, which was validated through our external penetration testing. Furthermore, another information system's support team did not obtain GSA authorization to implement patches before implementing them on production servers. Also, two information systems' support teams did not perform testing or obtain GSA authorization to implement patches prior to implementing them on the information systems' production servers. Finally, for some of the selected changes to two information systems' applications, management was unable to provide supporting documentation evidencing that it completed testing and approved the migration of the changes into the information systems' production environments. Similarly, approval of an information system's application, DB, and O/S changes was not consistently documented.

Identity and Access Management (IAM)

The IAM function includes the requirement that an agency implements a set of capabilities to ensure that users authenticate to IT resources and have access to only those resources required for their job function; a concept referred to as "need to know." The supporting activities include conducting onboarding and personnel screening, issuing, and maintaining user credentials, and managing logical and physical access privileges.

As a result of our performance audit procedures, we determined that GSA management developed an IAM strategy. GSA utilized that IAM strategy when developing new applications and continued integrating its legacy applications into its modern IAM architecture.

Additionally, GSA utilized various tools to assist with single sign-on and user access management. GSA also controlled privileged access using short name accounts that require a token to be used when accessing these accounts. This allowed GSA to separate the access of normal user accounts from privileged user accounts. GSA implemented role-based access using native technologies in order to manage accounts and enforce separation of duties/least privilege. Lastly, GSA implemented strong authentication methods for privileged and nonprivileged user access by implementing Personal Identity Verification (PIV) cards, two-factor authentication, and passwords to access GSA information systems. We determined that GSA closed the three prior-year IAM issues.

Based on our performance audit procedures, we reported four findings. Audit logs were not consistently monitored or reviewed for three information systems. Privileged user access was not authorized in accordance with one information system's SSP. Furthermore, authorization of new application and O/S user accounts for one information system was not consistently documented. Finally, for another information system, application user accounts were not reviewed and recertified by an independent GSA Project Management Office (PMO).

Data Protection and Privacy (DPP)

DPP refers to a collection of activities focused on confidentiality, preserving authorized restrictions on information access, and protecting personal and proprietary information from improper disclosure. Effectively managing the risk associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of individuals' personally identifiable information (PII) increasingly depends on the safeguards employed for the information systems that process, store, and transmit such information. OMB Circular A-130, *Managing Information as a Strategic Resource,* requires federal agencies to develop, implement, and maintain agency-wide privacy programs that protect PII. The head of each federal agency is ultimately accountable for ensuring that privacy interests are protected and for managing PII responsibly within 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 for the agency's privacy program.

Based on the results of our performance audit procedures, we did not identify any findings with GSA's DPP program and associated security controls. We noted that GSA management implemented a PII privacy program and security controls to protect PII.

GSA performed data exfiltration tests and cyber exercises to analyze the performance of its enhanced network defenses and the effectiveness of its Data Breach Response Plan. Further, GSA implemented an effective privacy awareness training program through feedback received from users that completed the privacy awareness training and phishing exercises.

Security Training (ST)

Security training is a cornerstone of a strong information security program as both nonprivileged and privileged IT users must have the knowledge to perform their jobs appropriately using information system resources without exposing the GSA to unnecessary risk.

Based on our performance audit procedures, we did not report any findings with GSA's ST program and associated security controls. We noted that GSA's security awareness and training program includes an assessment of its workforce needs to account for a changing risk environment. Further, GSA documented target metrics to address any identified gaps in its staff's knowledge, skills, or abilities through training or talent acquisition. Additionally, we noted that GSA's personnel collectively possessed a training level that had demonstrably reduced the number of security incidents resulting from personnel actions or inactions.

Detect – Information Security Continuous Monitoring (ISCM)

The objective of the Detect function in the Cybersecurity Framework is to discover and identify cybersecurity events in a timely manner. The Cybersecurity Framework states that continuous monitoring processes be used to detect anomalies and changes in the organization's operating environment and to provide knowledge of threats and security control effectiveness.

To enhance the government's ISCM capabilities, Congress established the Continuous Diagnostics and Mitigation (CDM) program. The CDM program provides agencies with capabilities and tools to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impact, and enable an agency's cybersecurity personnel to mitigate the most significant problems first.

Based on our performance audit procedures, we did not report any findings with GSA's ISCM program and associated security controls. We noted that GSA management implemented cybersecurity tools. GSA analyzed the data retrieved from the CDM toolset and generated actionable insights into its security posture. In addition, we determined that GSA required information systems to be monitored using the cybersecurity tools. Finally, GSA implemented an ongoing authorization program where eligible systems undergo periodic assessments of critical controls.

Respond – Incident Response (IR)

The objective of the Respond function in the Cybersecurity Framework is to implement processes to contain the impact of detected cybersecurity events. Activities include developing and implementing IR plans and procedures, analyzing security events, and effectively communicating IR activities. FISMA requires each agency to develop, document, and implement an agency-wide information security program that includes policies and procedures for IR.

Based on the results of our performance audit procedures, we did not report any findings with GSA's IR program and associated security controls. We noted that GSA implemented IR policies, procedures, plans, strategies, and technologies through weekly reports that capture incident response activities. GSA utilized multiple advanced tools to support the IR processes. These tools fed into GSA's SIEM tool to give a centralized view of the activities.

We noted that GSA utilized its threat vector taxonomy to classify incidents and capture metrics over the incidents reported in accordance with United States Computer Emergency Readiness Team guidelines. In

addition, GSA captured the impact of incidents and used the information to mitigate related vulnerabilities on other systems.

Recover – Contingency Planning (CP)

The objective of the Recover function in the Cybersecurity Framework is to ensure that organizations maintain resilience by implementing appropriate activities to restore capabilities or infrastructure services that were impaired by a cybersecurity event. The Cybersecurity Framework outlines CP processes that support timely recovery to normal operations and reduce the impact of a cybersecurity event.

Based on the results of our performance audit procedures, we did not report any findings with GSA's CP program and associated security controls. We noted that GSA management implemented its CP procedures and information system contingency plans. To achieve a Managed and Measurable maturity level, GSA should employ automated mechanisms to test system contingency plans more thoroughly and effectively.

IV. Audit Findings and Recommendations

Identify – Risk Management – Enterprise Information Security Policy

The GSA policies and IT procedural guides were not fully updated to be aligned with new requirements outlined in the 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 to the 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 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: *Contingency Planning (CP)*, CIO-IT Security-06-29, Revision 5, July 27, 2020
10. IT Procedural Guide: *Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (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 the 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

OMB Circular No. A-130, *Managing Information as a Strategic Resource*, Section 5. Discussion of the Major Provisions in the Appendix, Appendix I-16 a., page 53, states:

> For legacy information systems, agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines within one year of their respective publication dates unless otherwise directed by OMB. The one-year compliance date for revisions to NIST publications applies only to new or updated material in the publications. For information systems under development or for legacy systems undergoing significant changes, agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines immediately upon deployment of the systems.

GSA IT Security Policy CIO 2100.1M, Chapter 4: Policy for Protect Function, Section 4. Information Protection Processes and Procedures, page 64, states:

> […]
> o. The OCISO shall update this security policy and IT Security Procedural guides biennially, or more frequently as Federal or GSA guidance or the threats, vulnerabilities, or risks to GSA dictate.

IT Security Procedural Guide: *ISPP*, CIO-IT Security-18-90, June 16, 2020, Version 3, Section 3. Security Controls, pages 6-101, states:

> 3.1.1 Access Control Policy and Procedures (AC-1), page 7, AC-1 Control Implementation:
> […]
> b. The GSA OCISO is responsible for reviewing and updating CIO-IT Security-01-07 biennially.
> […]
> 3.7.1 Identification and Authentication Policy and Procedures (IA-1), page 36, IA-1 Control Implementation:
> […]
> b. The GSA OCISO is responsible for reviewing and updating CIO-IT Security 01-01 biennially.
> […]
> 3.14.1 Information Security Program Plan (PM-1), pages 61-62, PM-1 Control Implementation:
> […]
> b. The GSA OCISO is responsible for reviewing the ISPP annually.
> c. As part of the annual review, the ISPP is updated (as necessary) to address organizational changes or issues identified with control implementations or assessments.
> […]
> 3.18.1 System & Communications Protection Policy and Procedures (SC-1), page 94, SC-1 Control Implementation:
> […]
> b. The GSA OCISO is responsible for reviewing and updating procedural guides biennially.
> […]
> 3.19.1. System & Information Integrity Policy & Procedures (SI-1), page 101, SI-1 Control Implementation
> […]
> b. The GSA OCISO is responsible for reviewing and updating CIO-IT Security 12-63 and other guides biennially.

GSA management informed us that it waited until more guidance was released by the OMB for how agencies should modify their policies and procedures to comply with the new NIST SP 800-53, Revision 5. Once more guidance was released, including NIST SP 800-53B, *Control Baselines for Information Systems and Organizations,* and NIST SP 800-53A, *Assessing Security and Privacy Controls in Information Systems and Organizations*, GSA management created an implementation plan for reviewing and updating its policies and procedures. Management anticipates completing its updates by September 30, 2022.

Agency-wide information security policies and procedures provide guidance over controls implemented for its offices and information systems. Outdated policies and procedures can lead to a misunderstanding of the GSA information security program. This in turn increases the risk of improper control implementation, thereby exposing the agency to control deficiencies or cyber security risks.

RECOMMENDATIONS:

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.

Identify – Risk Management – SSP

During FY 2022, two information systems' SSPs were not reviewed and 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* (Chief Information Officer (CIO) IT Security-06-30). Moreover, one of the two information systems received its ATO prior to the approval of the SSP.

GSA IT Security Procedural Guide: *Managing Enterprise Cybersecurity Risk*, CIO-IT Security-06-30, Revision 23, May 9, 2022, Section 8.2.2 PL-2 System Security and Privacy Plans, Page 53, states:

> Control:
>
> […]
>
> c. Review the plans [annually];
>
> d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments;[…]

One information system's team informed us that it reviewed the SSP but determined changes were not required and, therefore, did not document their review. Further, due to competing priorities, GSA management did not formally maintain evidence of its annual review.

The other information system's team informed us that it was in the process of updating the SSP to reflect the Security Assessment Report (SAR) findings from the assessment. These updates were prolonged to ensure that, as items were being addressed from the SAR, the items were accurately reflected in the SSP. Therefore, the team did not review, update, and approve the SSP in the required timeframe or as part of the ATO prior to the system going live.

The lack of an adequately documented review and updated security plan increases the risk that the security controls could be performed incorrectly or inconsistently. This can negatively affect the accuracy, integrity, and availability of the system and its data residing on the information systems.

RECOMMENDATIONS:

We recommend that GSA:

1. Document its annual reviews, updates, and approvals for system-level SSPs, including for both information systems, as required by GSA IT Security Procedural Guide.
2. Ensure system-level SSPs are authorized prior to completing a system authorization.

Protect – Configuration Management – Flaw Remediation

1. Information System's Database Version No Longer Supported

The version of the DB that was in production and supporting the information system was no longer supported by the vendor as of February 2021. In addition, installation of one software application on the remote host that was in production and supporting the information 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.

The information 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.

GSA IT Security Procedural Guide: *Managing Enterprise Cybersecurity Risk*, CIO-IT Security-06-30, Revision 23, May 9, 2022, Appendix F: Showstopper Capabilities and Associated Controls, pages 85-86, states:

#	Showstopper Description	Control Reference
[…]		
2	Critical and High vulnerabilities: GSA requires ongoing remediation actions including patching, updating, and upgrading out of date components, addressing known vulnerabilities, completing POA&Ms, maintaining secure configurations of components. If an assessment identifies ongoing remediation actions are not being addressed, then the system will not be approved for a 3-year ATO or OA, until the associated risks are mitigated.	SI-2 Flaw Remediation
[…]		
4	EOL Software: The continued usage of End of Life (EOL) Software requires a risk evaluation to be performed by the OCISO. An EOL Software usage justification to include POA&M tracking requirements or an approved Acceptance of Risk (AOR), are the possible documentation outcome requirements of the risk evaluation. If an assessment identifies EOL software usage has not been properly evaluated and documented, then the system will not be approved for a 3-year ATO or OA, until completed.	SA-22 Unsupported System Components

GSA IT Procedural Guide: *Vulnerability Management Process,* CIO-IT Security-17-80, Revision 3, May 19 2022, 3.1 Implementation of NIST Controls, pages 5-6, states:

> GSA systems must implement NIST controls RA-5, Vulnerability Monitoring and Scanning, and SI-2(3), Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions in accordance with the frequencies and timelines established in the control statements and parameters as indicated below (only the parts of RA-5 and SI-2(3) that address frequencies or timelines are listed).
>
> RA-5:
> […]
> d. Remediate Legitimate Vulnerabilities
> […]
> (2) GSA Standard Timelines
> (a) Within 30 days for Critical (Very High) and High vulnerabilities.
> (b) Within 90 days for Moderate vulnerabilities.
> (c) Within 120 days for Low vulnerabilities for Internet-accessible systems/services.]

The information system team informed us that the system requires an up-time close to 100 percent, which prevented the team from upgrading the DB version and installing the necessary security patches as well as remediating vulnerabilities in a timely manner.

Without having current and supported software running on its production DBs, security vulnerabilities could be exploited, therefore increasing the risk that the confidentiality, integrity, and availability of the data residing on the information system could be compromised.

RECOMMENDATIONS:

We recommend that GSA:

1. Design and implement a monitoring process to track and identify information system software components that are no longer supported by vendors.
2. Test and update the information system's DB to a current supported version, as appropriate.
3. Design and implement a quality control process to validate that designated management authorizes the information system's 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 information system's DB.
5. Obtain a formal AOR when determining not to implement updated software versions and patches for an information system's devices and establish POA&Ms to mitigate the corresponding security risks.

2. *Lack of Timely Remediation of Identified Information System Vulnerabilities*

GSA management did not remediate identified high-risk vulnerabilities for one information system's 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 a 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 an external penetration test of the information system's 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 one vulnerability 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.

GSA IT Procedural Guide: *Vulnerability Management Process*, CIO-IT Security-17-80, Revision 3, May 19, 2022, Appendix B – GSA Deadlines to Remediate Vulnerabilities, page 19, states:

Corrective Action Deadline	**Required Actions**	**Target**	**Primary References**
BOD [Binding Operational Directive] Timelines			
Within 15 days of initial detection	Remediate **Critical (Very High)** vulnerabilities for systems or services with Internet-accessible IP addresses.	Any GSA system identified in a DHS Cyber Hygiene Report with critical vulnerabilities.	BOD 19-02/ BOD 20-01
Standard GSA Timelines			
Within 30 days of initial detection	Remediate **Critical (Very High)** and **High** vulnerabilities.	Any GSA system identified with critical (very high) vulnerabilities.	RA-5 control parameter
Within 90 days of initial detection	Remediate **Moderate** vulnerabilities.	Any GSA system identified with moderate vulnerabilities.	RA-5 control parameter

GSA IT Security Procedural Guide: *Managing Enterprise Cybersecurity Risks,* CIO-IT Security-06-30, Revision 23, May 9, 2022, Section 5.5.6.2 POA&Ms from Other Assessments, page 34, states:

> POA&Ms from other assessments adhere to the following conventions:
>
> […]
>
> - Vulnerability Scans
>
> […]
>
> - POA&Ms must be created for vulnerabilities exceeding the remediation timelines listed below.
>   - 15 days for Critical (Very High) vulnerabilities for Internet-accessible systems or services.
>   - 30 days for Critical (Very High) and High vulnerabilities.
>   - 90 days for Moderate vulnerabilities.

GSA management informed us that, due to competing priorities, it did not establish a POA&M for the high-risk vulnerability that was identified for the information system's environment within the 30-day timeline.

After management implemented its corrective actions to remediate the vulnerability, it did not perform a follow-up validation test to verify that the vulnerability had been fully remediated. Further, GSA management did not perform proper testing during an application upgrade and, as a result, was not aware that the vulnerability continued to exist in the information system's environment after the cutover to the upgraded application due to a system limitation with their web application security testing software. Due to competing priorities, management did not update the POA&M after performing its penetration test.

Without effective controls in place to identify, track, and remediate critical, high, and moderate-risk vulnerabilities, there is an increased risk that vulnerabilities are exploited by intruders and attackers trying to gain access to the information system, which could compromise the confidentiality, integrity, and availability of the data residing on the information system.

RECOMMENDATIONS:

We recommend that GSA:

1. Formally document and track all critical, high, and moderate-risk vulnerabilities, for the information 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 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.

Protect – Configuration Management – Patch Management

For one of two of the information system's DB patches tested, GSA management did not document evidence of authorization or testing prior to its implementation into production. Additionally, GSA management configured another information system's O/S and DB to install automatic patches from the vendors, but management could not provide evidence that it tested and authorized the patches.

GSA IT Procedural Guide: *CM,* CIO-IT Security-01-05, Revision 5, March 1, 2022, Section 4.3 CM-3 Configuration Change Control, pages 12-14, states:

- Authorize, document, and control changes to the information system. Include emergency changes in the configuration change control process.
  […]
- Ensure that any testing performed does not adversely impact the information system (perform the test on a test platform, not a production platform).
  […]

For enhancement CM-3(2), FIPS 199 Moderate and High systems are required to test, validate, and document changes before implementation in the operational environment.

GSA management informed us that the information system's DB was inadvertently left off the change ticket that documented the testing and approval of the DB patch for multiple servers.

GSA management informed us that formal evidence of authorization and testing was not documented for the other information system as the team has moved to a more efficient method for installing patches.

Without implementing effective CM controls, the risk increases that unauthorized access could be permitted that introduces fraudulent data or malicious code into the DB and O/S without detection. This also increases the risk that the confidentiality, integrity, and availability of the data residing on the information system may be compromised.

RECOMMENDATIONS:

We recommend that GSA:

1. Adhere to GSA policy for documenting authorizations and testing of an information system's DB patches prior to their implementation in the production environment.
2. Evaluate and document the unapproved information system's DB patches to confirm that the production environment was not adversely affected.
3. Adhere to GSA's CM policy and information system's policy for documenting authorizations and testing of the information system's O/S and DB patches prior to their implementation in the production environment.
4. Evaluate and document the unapproved information system's O/S and DB patches to confirm that the production environment was not adversely affected.

Protect – Configuration Management – Change Management

During FY 2022, weaknesses in an information system's CM controls 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 of the information system's application changes selected.
- Appropriate management approval could not be provided for 10 of 15 of the information system's application changes selected.

Similarly, we noted the following weaknesses while testing the second information system's application configuration controls:

- For three of five of the second information system's application changes selected, evidence of successful testing could not be provided.
- For five of five of the second information system's application changes selected, evidence of approval could not be provided.

In addition, controls to formally authorize changes to third 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 the third information system's application, DB, and O/S changes and patches occurred prior to their implementation into the production environment.

The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*, dated September 2014, paragraph 10.03, states:

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

GSA IT Procedural Guide: *CM,* Chief Information Officer (CIO)-IT Security-01-05, Revision 5, March 1, 2022, states:

> Section 4.3 CM-3 Configuration Change Control, page 14:
> Authorize, document, and control changes to the information system. Include emergency changes in the configuration change control process. […]
>
> For enhancement CM-3(2), FIPS 199 Moderate and High systems are required to test, validate, and document changes before implementation in the operational environment.

Management informed us that the selected changes for the first information were executed by the initial launch development team, which did not complete or retain supporting evidence that the aforementioned changes were successfully tested and migration to production was approved. The system owner identified the need for more robust processes, and the current team has since included a dedicated security role and they have implemented a more robust process with enhanced documentation requirements.

GSA management informed us that there was no formal ticketing system that tracks ongoing and completed efforts related to the second information system's application changes, testing, and approvals.

The third information system team informed us that application, DB, and O/S patches were verbally approved during weekly Change Control Board (CCB) meetings when other security-related matters were discussed. However, CCB's approvals were not documented and retained.

Without implementing effective CM controls, the risk increases that unauthorized changes could be permitted that introduce unintended changes or malicious code into the application without detection. This also increases the risk that the confidentiality, integrity, and availability of the data residing on the information system is compromised.

RECOMMENDATIONS:

We recommend that GSA:

1. Ensure that evidence of successful testing and approval is documented and retained for the first information system's application changes prior to implementation.
2. Evaluate and document the unapproved application changes to the first information system to confirm that the production environment was not adversely affected.
3. Ensure that evidence of successful testing and approval before implementation in the production environment is documented and retained for the second information system's application changes.
4. Evaluate and document the unapproved application changes for the second information system.
5. Evaluate if a ticketing system is needed for the second information system's application to track change management activities.
6. Develop and implement procedures to require the documentation and retention of the CCB's authorization of the third information system's application, DB, and O/S changes and patches prior to their implementation in the production environment.

Protect – Identity and Access Management – Audit Log Monitoring

Controls over security audit log monitoring were not consistently implemented at GSA. Specifically, we noted:

- GSA management noted in the first information system's SSP 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 it in FY 2020, but its status was "delayed." Therefore, GSA management did not periodically review the first information system's application and DB audit logs 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.

- Management did not consistently develop and implement a process to document the periodic review of privileged user account activities for the production second information system's application, DB, and O/S.

- Management did not develop and implement a manual or automated process to document the periodic review of privileged user account activities for third information system.

The GAO's *Standards for Internal Control in the Federal Government*, dated September 2014, Principle 10.03, pages 45-48, states:

> 2.11 – Management develops and maintains documentation of its internal control system.
>
> 2.12 – Effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors.
>
> 2.13 – Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity.
>
> Management clearly documents internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination.
> […]
> Documentation and records are properly managed and maintained.

GSA IT Security Procedural Guide: *AU*, CIO-IT Security-01-08, Revision 6, December 3, 2020, Section 3.7 AU-6 Audit Review, Analysis, and Reporting, pages 14-15, states:

> Control: The organization:
> a. Reviews and analyzes information system audit records [on business days when security related events are forwarded to the Enterprise Logging Platform for automated analysis and correlation, otherwise on a periodic basis (specific period recommended by the GSA S/SO or Contractor and approved by the GSA AO)] for indications of [GSA S/SO or Contractor recommended inappropriate or unusual activity as approved by the GSA AO];

GSA IT Procedural Guide: *AU*, CIO-IT Security-01-08, Revision 6, December 3, 2020, 3.7 AU-6 Audit Review, Analysis, and Reporting, Table 3-3: Log Review Responsibility, page 15 - 16, states:

System Layers	Who Reviews Logs	
	(Integrated with ELP [Enterprise Logging Platform])	**(Not Integrated with ELP)**
Cloud Service Provider (e.g., AWS [Amazon Web Services])	SecOps (Only Reviewed Under Incident)	System Team
Operating Systems	SecOps (Only Reviewed Under Incident)	System Team
Log types reviewed only if PII or sensitive data (e.g., financial, CUI [Controlled Unclassified Information]) is in scope: ▪Databases ▪Applications ▪Tools	System Team	System Team
Security Agent/Device Events	SecEng	System Team

Federal System System-Specific Expectation:
For systems not integrated with the ELP and for logs not sent to the ELP, the system owner maintains the responsibility to ensure information system logs are reviewed for unusual activity on a periodic basis defined on a system-by-system basis as approved by the GSA AO. Logs must be kept to validate that such a review has taken place. Systems storing and/or processing PII or sensitive (e.g., financial, CUI) data must review database/application/tool logs. Systems without such data are not required to review database/application/tool logs.

For systems hosting PII/sensitive (e.g., financial, CUI) data, system personnel assigned by the System Owner, are responsible for conducting reviews for anomalous activity for layers identified in Table 3-3. A list of specific anomalous activities for a system with PII/sensitive (e.g., financial, CUI) should be identified for review and analysis. Some examples are:

- Unusual authentication and authorization events
- Unauthorized data or content manipulation
- Excessive web application or database activity
- Unauthorized or unusual transactions

Teams must define their own approach for conducting review of these events and activities, at a frequency accepted and approved by the AO. It is not necessary for every team to deploy their own centralized tool such as a SIEM in order to comply with this guide. Teams can construct an approach which covers audit log review within specific applications, tools, and databases that form their system.

GSA management informed us that the first information system's team consists of a small number of administrators. These resourcing constraints have prevented the team from fully implementing the first information system's application and DB audit log review control.

Without periodic monitoring of management-defined security events, the risk exists that unauthorized or inappropriate activity could occur in the first information system's application and DB without detection. As a result, this could negatively affect the accuracy, integrity, and availability of the system and its data.

GSA management relied on external agency administrators to review privileged user activity for their respective agencies for second information system. However, GSA management did not validate that the review was performed. Additionally, GSA management informed us that DB and O/S alerts were sent to the respective information system's security teams on a daily basis, but evidence of review is only captured on a ticket when further action is required and not regularly after a review is performed.

Not periodically reviewing privileged access increases the risk that unauthorized access could exist. This increases the opportunity for the confidentiality, integrity, and availability of the data residing on the second information system to be compromised.

The third information system's System Security and Privacy Plan (SSPP) defines the frequency for audit log review as event-driven, while GSA's IT Procedural Guide: *AU* requires a periodic review. Despite this discrepancy, GSA management informed KPMG that it believes the current third information system's SSPP has the appropriate requirement for the frequency of audit log review. Therefore, management did not request a control waiver for its SSPP AU-6 control against agency policy. Further, management relied on a real-time audit log review that is not documented.

The lack of consistently documented policies and procedures increases the risk that the audit log review controls are performed incorrectly or inconsistently. Therefore, there is an increased risk that unauthorized or inappropriate activity may not be investigated and that critical system data could be compromised.

RECOMMENDATIONS:

We recommend that GSA:

1. Design and implement a quality control process to validate that designated management reviews the first information system's application and DB audit logs in the production environment within the timeframes established by the information system's SSP.
2. Evaluate and document the previously reviewed logged events to confirm that the first information system's application production environment was not adversely affected.
3. Develop and implement a process to document evidence of the periodic review of privileged user account activities for the second information system's application, DB, and O/S levels, including the review of relevant administrators from external agencies.
4. Amend the third information system's SSPP audit log review frequency to adhere to GSA IT Security Procedural Guide: *AU* or obtain an AOR or formal risk acceptance for the information system's controls that do not comply with GSA IT policies and directives.
5. Develop and implement a process to document evidence of the periodic review of privileged user account activities.

Protect – Identity and Access Management – Privileged User Access Authorization

The information system's application super-administrator granted herself an additional, less privileged, standard administrator account without appropriate approval, which did not adhere to the information system's SSP.

GSA IT Security Procedural Guide: *AC*, CIO-IT Security-01-07, Revision 4, May 8, 2017, Section 5.2 AC-2 Account Management, Page 16, states:

> Control: The organization:
>
> […]
>
> d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
>
> e. Requires approvals by [System Owner and GSA Authorizing Official] for requests to create information system accounts;

The information system's application super-administrator needed to test standard-administrator access functionality and created a standard-administrator account for herself in order to perform testing at a lower privileged level.

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

RECOMMENDATION:

We recommend that GSA ensure that all privileged access requests to the information system are approved by an independent authorized approver.

Protect – Identity and Access Management – Access Authorization

Controls to authorize new user access was not consistently implemented. Specifically, we noted:

- Management indicated that it does not require documented approvals prior to granting individuals access to the first information system. Further, because of a system upgrade, all of the first information system's application administrator accounts were recreated without documented access approvals as management relied on verbal authorizations from the approving official.

- GSA management did not document its authorization of access for two of two new O/S administrators and two of two new application administrators supporting the second information system, which did not adhere to the information system's SSP and *GSA IT Security Policy* CIO 2100.1M.

GSA IT Security Policy CIO 2100.1M, Chapter 4: Policy for Protect Function, Section 1 Identity Management, Authentication and Access Control, pages 45-46, states:

> f. Request, including modifications, and approval routing in support of account management processes must ensure:
>
> (1) All access requests require at least one supervisor approval. Access requests submitted directly from a user must not be accepted, regardless of position;
>
> (2) Users complete and send access requests to their supervisor or COR, not directly to the data or system owner;
>
> (3) Access requests are routed to the data or system owner by a user's supervisor, COR, ISSO, ISSM, director, or designated official.

GSA IT Security Procedural Guide: *AC*, CIO-IT Security-01-07, Revision 4, May 8, 2017, Section 5.2 AC-2 Account Management, Page 16, states:

> Control: The organization:
>
> d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
>
> e. Requires approvals by [System Owner and GSA Authorizing Official] for requests to create information system accounts;
>
> […]
>
> i. Authorizes access to the information system based on:
>
> a. A valid access authorization;
>
> b. Intended system usage; and
>
> c. Other attributes as required by the organization or associated missions/business functions;

The first information system's team informed us that it is a small team and that application administrators are approved verbally during monthly security meetings when other security-related matters are discussed, including related upgrades.

For the second information system, GSA management informed us that the previously documented approvals were attached in the legacy ticketing system and were not migrated to the new ticketing system after it went live in December 2021.

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

RECOMMENDATIONS:

We recommend that GSA:

1. Enforce proper completion of application administrator request forms to include obtaining authorizations from designated management authorizations prior to provisioning administrator access to the first information system's application.
2. Validate that access is appropriate for all of the first information system's application administrator accounts.
3. 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 second information system's application and O/S, respectively.
4. Validate that access is appropriate for all of the second information system's application and O/S administrator accounts.

Protect – Identity and Access Management – Access Review and Recertification

An information system's application users were required to recertify their access; however, an independent recertification by the GSA PMO was not performed.

GAO's *Standards for Internal Control in the Federal Government Documentation of the Internal Control System*, states:

> 3.09 – Management develops and maintains documentation of its internal control system.
>
> 3.10 – Effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors.
>
> 3.11 - Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity.

GSA management failed to recertify an information system's application users due to an overreliance on the self-certification process.

Not periodically reviewing privileged access increases the risk that unauthorized access could exist. This increases the opportunity for the confidentiality, integrity, and availability of the information system's data and computing resources could be compromised.

RECOMMENDATION:

We recommend that GSA ensure all of the information system's users are independently recertified no less than annually, in accordance with GSA policy.

V. Conclusions

GSA established and maintained its information security program and practices for its information systems for the five Cybersecurity functions and nine FISMA Metric Domains. We assessed GSA's information security program as "Effective," according to CyberScope, based on our assessment of most of the FY 2022 Core IG Metrics as "Managed and Measurable" or "Optimized." Specifically, the Identify, Protect, Detect, and Respond Cybersecurity functions were assessed as "Optimized," while the Recover function was rated as "Managed and Measurable." We also followed up on the status of four prior-year findings and reported that they were closed (see Appendix I). However, we identified 10 findings that affected the Identify and Protect Cybersecurity functions and the RM, CM, 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 mode of the six Identify IG metric questions and the eight Protect IG metric questions.

We made 35 recommendations related to the 10 control findings that should strengthen GSA's information security program if effectively addressed by management. GSA should also implement a process to determine if these recommendations apply to other information systems maintained in its FISMA inventory. In a written response, the CIO agreed with our findings and recommendations and should develop corrective actions that are responsive to the intent of our recommendations (see Section VI).

VI. Agency Comments – Management Response to the Report

November 14, 2022

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

FROM DAVID A. SHIVE
CHIEF INFORMATION OFFICER – I

DocuSigned by:
David Shive
A3AE4284A2754F9...

SUBJECT: Agency Management Response – Discussion Draft
Independent Audit on the effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report - Fiscal Year 2022

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 2022. 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 this year's FISMA performance audit, we performed procedures to determine whether management closed prior-year findings. If there was evidence that the recommendations had been sufficiently implemented, then we closed the finding. If there was evidence that the recommendations were partially implemented or not implemented, then we determined the findings to be open. Based on the procedures we performed, we concluded that all four prior-year findings were closed.

Prior-year Finding – 2021 Evaluation

Finding Number	Prior-year Condition	Recommendation(s)	Status
1. Protect Function – Configuration Management **Patch Management**	For the information system's environment, GSA management did not document its authorization for a selection of three of three patches for the O/S and two of two patches for the DB prior to their implementation into the production environment. Furthermore, management did not formally document an AOR for not installing four medium security O/S patches on two devices within 90 days of initial detection. For another information system, one of two selected DB patches did not have documented GSA evidence of authorization prior to implementation into the production environment.	We recommend that GSA: 1. Design and implement a quality control process to validate that designated management authorizes information system O/S and DB patches prior to their implementation in the production environment within the timeframes established by GSA policy. 2. Evaluate and document the three O/S and two DB unapproved patches noted above to confirm that the information system's production environment was not adversely affected. 3. Obtain a formal authorized AOR when determining not to implement specific moderate or low patches for the information system's devices. 4. Adhere to GSA's and the other information system-specific policies by documenting authorizations of the information system's DB patches prior to their implementation in the production environment. 5. Evaluate and document the unapproved DB patch for the other information system to confirm that the information system's production environment was not adversely affected.	Closed Closed Closed Closed Closed

Finding Number	Prior-year Condition	Recommendation(s)	Status
2. Protect Function – Identity and Access Management **User Authorization**	For 25 selected information system application user accounts, 3 accounts did not have evidence of approval before the accounts were provisioned, which did not adhere to GSA IT Security Policy CIO 2100.1M. In addition, the information system's support team accepts emails as approval documentation for information system access, which did not adhere to requirements specified in GSA IT Security Procedural Guide: Access Control (AC) CIO-IT Security-01-07. In addition, we noted that only one application account for another information system was created for a new GSA user. This account was verbally authorized by the designated approving official, but the authorization was not documented before the user's account was provisioned.	We recommend that GSA: 1. Implement a standardized information system user request form and require supervisor authorization to be documented before provisioning user access to the application. 2. Validate that access is appropriate for the three information system application accounts. 3. Enforce proper completion of user request forms by the vendor to include obtaining supervisor authorization prior to provisioning user access to the information system application. 4. Validate that access is appropriate for the other information system's application account.	Closed Closed Closed Closed
3. Protect Function – Identity and Access Management **User Account Reauthorization**	One information system's users' supervisors did not perform reviews and reauthorizations of the information system's application-level user accounts to determine if access was still required and if the users' assigned privileges were commensurate with their job responsibilities. The information system's application users performed annual self-reauthorizations to maintain their privileges, which does not adhere to GSA IT Security Policy CIO 2100.1M.	We recommend that GSA: 1. Update the information system security policy, processes, and procedures to require supervisors to review application users' access and assigned privileges to determine whether they are commensurate with their job responsibilities. 2. Establish milestones for supervisors to complete the review and reauthorization of information system application users' access and update or remove any access and privileges that are not commensurate with current job responsibilities.	Closed Closed

Finding Number	Prior-year Condition	Recommendation(s)	Status
4. Protect Function – Identity and Access Management **Timely User Account Removal**	Two of the 3,045 terminated GSA individuals from October 1, 2020 through August 2, 2021 maintained active information system user accounts past the allotted 30 days of separation from the GSA.	We recommend that GSA: 1. Disable or remove the two terminated users' accounts from the information system and confirm that their accounts were not used since their separation. 2. Implement a process to review terminated user listings on a periodic basis and disable or remove the information system's user accounts of terminated users, regardless of whether these users' PIV cards were suspended and returned.	Closed Closed

Appendix II – Glossary

Acronym	Definition
AC	Access Control
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
AOR	Acceptance of Risk
ATO	Authorization to Operate
AU	Audit and Accountability
AWS	Amazon Web Services
BOD	Binding Operational Directive
CCB	Change Control Board
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CMS	Content Management System
COR	Contracting Officer's Representative
CP	Contingency Planning
C-SCRM	Cyber Supply Chain Risk Management
CTO	Chief Technology Officer
CUI	Controlled Unclassified Information
DB	Database
DBA	Database Administrator
DHS	Department of Homeland Security
DPP	Data Protection and Privacy
ELP	Enterprise Logging Platform
EO	Executive Order
EOL	End of Life
FAS	Federal Acquisition Services
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Officer
GRC	Governance, Risk, and Compliance
GSA	U.S. General Services Administration
I	GSA's Chief Information Officer (CIO)
IA	Identification and Authentication
IAM	Identity and Access Management
IC	Office of Corporate IT Services
ICAM	Identity, Credential, and Access Management
ID	Office of the Deputy CIO
IG	Inspector General
IP	Internet Protocol
IQ	Office of Acquisition Information Technology Services
IR	Incident Response
IS	Office of the Chief Information Security Officer
ISCM	Information Security Continuous Monitoring

Acronym	Definition
ISE	Security Engineering Division
ISI	Identity, Credential, and Access Management Shared Service Division
ISO	Security Operations (SecOps) Division
ISP	Policy and Compliance Division
ISPP	Information Security Program Plan
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IST	ISSO Support Division
IT	Information Technology
KPMG	KPMG LLP
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
OA	Ongoing Authorization
OCISO	Office of the Chief Information Security Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
O/S	Operating System
PB-ITS/IP	Office of Public Buildings Information Technology Services
PBS	Public Buildings Service
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PM	Program Management
PM	Program Manager
PMO	Program Management Officer
POA&M	Plan of Action and Milestones
QA	Quality Assurance
Rev	Revision
RM	Risk Management
SAR	Security Assessment Report
SC	System and Communications
SCRM	Supply Chain Risk Management
SecOps	Security Operations
SI	System and Information Integrity
SIEM	Security Information and Event Management
SO	System Owner
SP	Special Publication
SSP	System Security Plan
SSPP	System Security and Privacy Plan
ST	Security Training
S/SO	Service and Staff Offices