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

Independent Audit on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report - Fiscal Year 2021

December 16, 2021

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

December 16, 2021

Dear Ms. Peterson-Jones,

KPMG is pleased to submit the *Independent Audit on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2021*. This report is provided to you in the format according to our contract GS-00F-275CA, order number 47HAA021F0040, dated February17, 2021, 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 2021 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 S. DiGrado

Raphael DiGrado
Managing Director, Technology Assurance – Audit

INDEPENDENT AUDIT ON THE EFFECTIVENESS OF THE U.S. GENERAL SERVICES ADMINISTRATION'S INFORMATION SECURITY PROGRAM AND PRACTICES REPORT FISCAL YEAR 2021

December 16, 2021

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 monitored KPMG's work to ensure it met professional standards and contractual requirements.

KPMG conducted a performance audit of GSA's information security program in accordance with Generally Accepted Government Auditing Standards (GAGAS) and with the Office of Management and Budget's 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, 2020 through September 30, 2021. In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by the American Institute of Certified Public Accountants.

What We Found

Our testing for Fiscal Year (FY) 2021 included performing procedures at the entity level for five GSA-operated information systems and five contractor-operated information systems. We also followed up on the status of prior-year findings. As a result of our procedures, we assessed GSA's information security program as "Effective," according to Department of Homeland Security guidance. We made this determination based on assessing a majority of the FY 2021 Inspector General (IG) FISMA Reporting Metrics (FY 2021 IG FISMA Reporting Metrics) as "Managed and Measurable" and "Optimized." Specifically, the Identify, Protect, Detect, and Respond Cybersecurity functions were assessed as "Optimized," while the Recover function was rated as "Consistently Implemented."

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

- Configuration Management
  - Patch management – Patches to the operating system (OS) and database (DB) for two information systems were not authorized prior to being implemented, and one information system had patches that were not applied timely.

- Identity and Access Management
  - User Authorization – Users for two information systems were granted system access without formal authorization.
  - User Account Reauthorization – GSA did not perform a user access review and reauthorization for one information system.
  - Timely User Account Removal – Terminated users' access to one information system was not removed in a timely manner.

These findings did not affect our overall assessment of the Protect function after calculating the mode of the 30 Protect IG metric questions, as instructed by the FY 2021 IG FISMA Reporting Metrics guidance.

What We Recommend

We made 13 recommendations related to the 4 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. Design and implement a quality control process to validate that designated management authorizes information system OS and DB patches prior to their implementation in the production environment within the timeframes established by GSA policy.
2. Evaluate and document the unapproved patches to confirm that the information system's production environment was not adversely affected.
3. Obtain a formal authorized acceptance of risk when determining not to implement specific moderate or low patches for the information system's devices.
4. Adhere to GSA's and the 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 information system's DB patch to confirm that the information system's production environment was not adversely affected.
6. Implement a standardized information system user request form and require supervisor authorization to be documented before provisioning user access to the application.
7. Validate that access is appropriate for the three information system application accounts.
8. Enforce proper completion of user requests forms by the vendor to include obtaining supervisor authorization prior to provisioning user access to the information system application.
9. Validate that access is still appropriate for the one information system application account.
10. Update 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.
11. 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.
12. Disable or remove the two terminated users' accounts from the information system and confirm that their accounts were not used since their separation.
13. Implement a process to review terminated user listings on a periodic basis and disable or remove the information system user accounts of terminated users, regardless of whether these users' Personal Identity Verification cards were suspended and returned.

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

Contents

I. KPMG Letter

KPMG LLP
Suite 900
8350 Broad Street
McLean, VA 22102

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

Independent Audit on the Effectiveness of the U.S. General Services Administration's Information Security Program and Practices Report – Fiscal Year 2021

This report presents the results of KPMG LLP's (KPMG) independent performance audit of the U.S. General Services Administration (GSA) information security program and practices for its information systems as of September 30, 2021. We conducted our performance audit from April 5, 2021 through September 30, 2021.

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 Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA). This performance audit did not constitute an audit of financial statements or an attestation level report as defined under GAGAS and the AICPA standards for attestation engagements.

Consistent with the Federal Information Security Modernization Act of 2014 (FISMA) and Office of Management and Budget (OMB) requirements, the objective of this performance audit was to determine the effectiveness of GSA's information security program and practices for its information systems for the period October 1, 2020, through September 30, 2021 in the five security function areas outlined in the Fiscal Year (FY) 2021 Inspector General (IG) FISMA Reporting Metrics (FY 2021 IG FISMA Reporting Metrics) and follow-up on the status of prior-year findings. As a result of our procedures, we assessed GSA's information security program as "Effective," according to Department of Homeland Security (DHS) guidance. We made this determination based on assessing a majority of the FY 2021 IG FISMA Reporting Metrics as "Managed and Measurable" and "Optimized." Specifically, the Identify, Protect, Detect, and Respond Cybersecurity functions were assessed as "Optimized," while the Recover function was rated as "Consistently Implemented."

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), DHS, and OMB and is not intended to be, and should not be, relied upon by anyone other than these specified parties.

KPMG LLP

December 16, 2021

II. Background, Objective, Scope, and Methodology

Background

KPMG performed the FY 2021 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[1]

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.

In the 21st century, GSA is focusing increasingly on adding value through new, efficient, and effective ways for federal employees to do their work. Building on GSA's strong record of accomplishment, GSA is helping to create a citizen-centric, results-oriented government that is even more productive and responsible to all Americans.

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

[1] The agency and program overview information are as of August 24, 2021.

management processes.

- *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 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 2021, OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) continued to develop the FY 2021 IG FISMA Reporting Metrics, Version 1.1, dated May 12, 2021, around five Cybersecurity functions outlined in the *National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity*[2] (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. In addition, FY 2021 IG FISMA Reporting Metrics use the CIGIE maturity models for the nine metric domains: Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning. **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 within the FY 2021 IG FISMA Reporting Metrics

Cybersecurity Framework Functions	FISMA Metric Domains
Identify	Risk Management (RM) Supply Chain Risk Management (SCRM)
Protect	Configuration Management (CM) Identity and Access Management (IAM) Data Protection and Privacy (DPP) Security Training (ST)
Detect	Information Security Continuous Monitoring (ISCM)
Respond	Incident Response (IR)
Recover	Contingency Planning (CP)

Changes for FY 2021

The FY 2021 IG FISMA Reporting Metrics included a new domain, SCRM, within the Identify function. This new domain focuses on the maturity of agency SCRM strategies, policies and procedures, plans, and processes to ensure that external providers' products, system components, systems, and services are consistent with the organization's cybersecurity program. The new domain references SCRM criteria in NIST Special Publication (SP) 800-53, Revision (Rev) 5, *Security and Privacy Controls for Information Systems and Organizations*. To provide agencies with sufficient time to fully implement NIST 800-53,

[2] 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.

Rev 5, in accordance with OMB Circular A-130, these new metrics are not considered for the Identify framework function rating in FY 2021. The risk management domain was reorganized to focus on the cyber risk management process and how an agency integrates with its enterprise risk management process. The IG metric questions have been streamlined to reduce redundancies, especially around implementing policies and procedures.

OMB also provided guidance for agencies to improve vulnerability identification, management, and remediation by issuing OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*. DHS issued Binding Operational Directive 20-01, *Develop and Publish a Vulnerability Disclosure Policy,* which provides guidance on the development and publishing of an agency's vulnerability disclosure policy and supporting handling procedures.

IG FISMA Scoring

The ratings in the nine domains (RM, SCRM,[3] CM, IAM, DPP, ST, ISCM, IR, and CP) were determined by a simple majority or mode,[4] with the most frequently assessed metric level across the metric questions serving as the domain rating. When responses are entered, the calculations will be performed by CyberScope[5] to determine 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. **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 2021 IG FISMA Reporting Metrics are at least Level 4: Managed and Measurable.

[3] According to the FY 2021 IG FISMA Reporting Metrics, we assessed the maturity levels of the SCRM metrics, but they are not considered in the overall maturity results used in determining the effectiveness of the Identify function and the overall information security program.

[4] The FY 2021 IG FISMA Reporting Metrics introduced a new pilot concept of weighting ten priority FISMA metrics for assessment and scoring. As part of the proposed weighted average approach to scoring, these priority metrics would be weighted twice as much in the maturity calculation. The simple majority scoring will still be used in calculating the overall scoring for FY 2021; however, the weighted average pilot will help the GSA evaluate the impact of the scoring change in the event it is implemented in the future.

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

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, 2020 through September 30, 2021. Specifically, we assessed the GSA's performance in the five security function areas outlined in the FY 2021 IG FISMA Reporting Metrics. We performed our fieldwork from April 5, 2021 through September 30, 2021. As part of our performance audit, we responded to the FY 2021 IG FISMA Reporting Metrics 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 2021 IG FISMA Reporting 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 (5 GSA information systems and 5 contractor-owned information systems) from a total population of 110 major applications and general support systems as of March 2, 2021. We also performed follow-up testing on four 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 FISMA metrics questions. 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 IG FISMA metric question.

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

- 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; and
  Execution of a targeted vulnerability assessment that focused on recent high-profile security incidents, such as the SolarWinds security breach, on selected devices for in-scope GSA information systems and a data exfiltration test.

We performed our fieldwork from April 5, 2021 through September 30, 2021. 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[6]	Optimized (Level 5)
Protect – CM, IAM, DPP, and ST	Optimized (Level 5)
Detect – ISCM	Optimized (Level 5)
Respond – IR	Optimized (Level 5)
Recover – CP	Consistently Implemented (Level 3)

Although we assessed GSA's information security program as effective, we reported four findings impacting practices within the Protect function. The nature of these findings did not affect our overall assessment of the Protect function after determining the mode of the 30 Protect IG metric questions. **Table 4** below depicts the four finding areas by function identified.

Table 4: Summary of Finding Areas by Cybersecurity Functions

Function	Finding Area
Protect – CM	Patch Management
Protect – IAM	User Authorization
Protect – IAM	User Account Reauthorization
Protect – IAM	Timely User Account Removal

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 could 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's information when establishing an information security program based on these documented risk management decisions.

Based on the results of our performance audit procedures, we did not report any testing exceptions or findings with GSA's RM program and associated controls. We noted that GSA implemented policies and

[6] The assessed maturity levels for SCRM metrics were not considered in the overall maturity results used in determining the effectiveness of the Identify function and the overall information security program.

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. For tracking software assets, GSA used tools, its GRC platform, and a ticketing system to track entitlements.

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 their cybersecurity tools, GSA could view risks and vulnerabilities that impact GSA information systems and allow stakeholders to make risk-based decisions.

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 testing exceptions or 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 risk factors of suppliers. GSA also has detailed guides for monitoring contractor-operated information systems. This includes the use of the GRC platform to monitor and review information security monitoring deliverables.

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 the ability of GSA to limit, contain, or prevent the impact of a cybersecurity event. This function is carried out by proper configuration management, identity and access management, data protection and privacy, and security training 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 focused on establishing and maintaining the integrity of products and information systems through the control of 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 has documented performance measures to determine the effectiveness of its configuration management 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 to its established common secure configurations. GSA monitored configuration compliance through endpoint detection and response and configuration/patch management tools and communicated biweekly configuration compliance reports to stakeholders.

Additionally, we determined GSA performed weekly vulnerability scanning to identify outstanding vulnerabilities associated with missing patches. GSA used an application whitelisting tool and another application to perform network access control to assist with blocking unauthorized hardware and software. We performed targeted vulnerability scans for in-scope information systems. 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 three prior-year CM issues.

However, we did report a finding for patch management. Specifically, an information system support team did not obtain GSA authorization to implement patches before implementing them to production servers. Furthermore, the support team did not implement medium-risk[7] patches for two devices in a timely manner or include them in an AOR. Also, another information system support team did not document the authorization of patches before implementing them to production servers.

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 required resources 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. These activities collectively are referred to as ICAM.

As a result of our performance audit procedures, we determined that GSA management developed an ICAM strategy. GSA utilized that ICAM strategy when developing new applications and continued integrating its legacy applications into its modern ICAM 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 used native technologies to manage accounts and separation of duties/least privilege by implementing role-based access. Lastly, GSA implemented strong authentication methods for privileged and nonprivileged user access by implementing the use of Personal Identity Verification (PIV) cards, two-factor authentication, and passwords to access GSA information systems. We determined that GSA closed the six prior-year IAM issues.

Based on our performance audit procedures, we reported three findings related to IAM:

1. User accounts were not authorized for two information systems. For a selection of 25 user accounts for 1 information system, 3 accounts did not have evidence of authorization before the accounts were

[7] As defined by Common Vulnerability Scoring System ranking scores.

provisioned. For another information system, one user account was not authorized by the designated approving official before the user's account was provisioned.
2. User accounts were not reauthorized for an information system. The support team did not perform a users' access review and reauthorization within FY 2021 to determine if the users' information system access and privileges were appropriate based on current job responsibilities.
3. User accounts that were no longer valid were not removed for an information system. Specifically, user accounts belonging to 2 of 3,045 terminated individuals were not removed in a timely manner.

Data Protection and Privacy (DPP)

DPP refers to a collection of activities focused on the security objective of confidentiality, the preservation of authorized restrictions on information access, and the protection of improper disclosure of personal privacy and proprietary information. Effectively managing the risk to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their personally identifiable information (PII) increasingly depends on the safeguards employed for the information systems that process, store, and transmit the information. As such, OMB Circular A-130, *Managing Information as a Strategic Resource,* requires federal agencies to develop, implement, and maintain agency-wide privacy programs that, where PII is involved, play a key role in information security and proper implementation of the NIST Risk Management Framework. The head of each federal agency remains ultimately responsible for ensuring that privacy interests are protected and for managing PII responsibly within their agency. Executive Order 13719, *Establishment of the Federal Privacy Council,* requires agency heads to designate a senior agency official for privacy who has agency-wide responsibility and accountability for the agency's privacy program.

Based on the results of our performance audit procedures, we did not identify any testing exceptions or 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.

As part of the FY 2021 GSA FISMA performance audit, we performed a data exfiltration test to send sensitive information from the GSA network to a KPMG controlled server. GSA's security controls prevented the establishment of a successful connection; therefore, we could not transfer data outside of GSA's network.

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 testing exceptions or findings with GSA's ST program and associated security controls. We noted that GSA implemented security awareness and training strategies, plans, and programs. GSA captured security awareness course evaluation statistics, performed analysis over phishing exercise results using phishing software and updated training based on feedback received from users and evolving threats and risks.

Detect – Information Security Continuous Monitoring (ISCM)

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

To enhance further 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 impacts, and enable an agency's cybersecurity personnel to first mitigate the most significant problems.

Based on our performance audit procedures, we did not report any testing exceptions or 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. GSA had practices to allocate resources in a risk-based manner and to hold relevant stakeholders accountable for carrying out their roles and responsibilities effectively. In addition, we determined that GSA requires information systems to be monitored using the cybersecurity tools.

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 testing exceptions or 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 IR 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 utilizes 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 contingency planning 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 testing exceptions or 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 develop and implement qualitative and quantitative performance metrics and monitor them for the effectiveness of the Recover function.

IV. Audit Findings and Recommendations

Protect – Configuration Management – Patch Management

For an information system, GSA management did not document its authorization for a selection of three of three patches for the operating system (OS) and two of two patches for the database (DB) prior to their implementation into the production environment. Furthermore, management did not formally document an AOR for not installing four medium risk level OS 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.

GSA IT Procedural Guide: Configuration Management (CM) CIO-IT Security-01-05, Revision 4, January 17, 2018, Section 4.3 CM-3 Configuration Change Control, page 11, states:

- Authorize, document, and control changes to the information system. Include emergency changes in the configuration change control process.
- Use automated tools/processes to control/manage system changes. If automated tools are not used, a GSA Change Request Form (Appendix A) is provided.

GSA documents the deadlines to remediate vulnerabilities in the GSA IT Procedural Guide: Vulnerability Management Process CIO-IT Security-17-80, Revision 1, August 21, 2019, Appendix B – GSA Deadlines to Remediate Vulnerabilities.

A contractor, who provides support to various GSA programs, sent email notifications to the information system support team to install OS and DB patches to the operating system and database, and, subsequently, these patches were installed by the information system support team. The support team informed us that it failed to obtain GSA authorization for these patches and relied on the contractor's authorization process. In addition, the support team stated that it forgot to obtain an AOR when it decided not to install the medium OS patches on two devices.

GSA management informed us that the other information system support team previously instructed the contractor, who provides operations support, to conduct patching, as needed, which was inadvertently taken as a one-time verbal authorization to move forward with applying all future required patches. The support contract originates from the Office of Information and Regulatory Affairs, which is still in place, but will transition to being fully supported by GSA IT in FY 2022.

Without implementing effective configuration management controls, the risk increases of fraudulent data or malicious code being implemented into the two information systems and the supporting OSs and DBs without detection. This also increases the risk that the confidentiality, integrity, and availability of the data residing on the information system's environments could be compromised.

RECOMMENDATIONS:

We recommend that GSA:

1. Design and implement a quality control process to validate that designated management authorizes OS and 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.
2. Evaluate and document the three OS and two DB unapproved patches noted above to confirm that the production environment for the information system was not adversely affected.
3. Obtain a formal AOR when determining not to implement specific moderate or low patches for the information system's devices.
4. Adhere to GSA's and the 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 information system's DB patch to confirm that the information system's production environment was not adversely affected.

Protect – Identity and Access Management – User Authorization

For 25 selected information system user accounts, 3 accounts did not have evidence of approval before the accounts were provisioned for the information system, which did not adhere to GSA IT Security Policy CIO 2100.1M. In addition, the information system support team accepted 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, for another information system, only one user account 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.

GSA IT Security Policy CIO 2100.1M, March 26, 2021, 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 [contracting officer's representative], 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[.]

GSA management informed us that it permitted one user to request information system access on his own behalf, without approvals, due to the user's elevated position at his respective federal agency. For another user, the access approval was maintained by an individual who was on long-term leave and could not provide authorization evidence during the FY 2021 GSA FISMA performance audit period. For the third information system user, GSA management informed us that it was aware of the GSA IT Security Policy CIO 2100.1M authorization requirements, but it did not maintain the documentation due to human error.

The other information system support team informed us that it relied on the vendor to capture and maintain its access authorizations. However, the approval for the new user could not be produced because of a defect in the vendor's access management system.

Without formally authorizing the access of new users, GSA has an increased risk that unauthorized access could be permitted. Therefore, the confidentiality, integrity, and availability of data residing on information systems could be compromised.

RECOMMENDATIONS:

We recommend that GSA:

1. Implement a standardized user request form and require supervisor authorization to be documented before provisioning user access to the information system.
2. Validate that access is appropriate for the three information system user accounts noted above.
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.
4. Validate that access is still appropriate for the one user account noted above.

Protect – Identity and Access Management – User Account Reauthorization

An information system users' supervisors did not perform reviews and reauthorizations of application-level user accounts to determine if access was still required and if the users' assigned privileges were commensurate with their job responsibilities. Users performed annual self-reauthorizations to maintain their privileges, which does not adhere to GSA IT Security Policy CIO 2100.1M.

CRITERIA:

GSA IT Security Policy CIO 2100.1M, March 26, 2021, Chapter 2: Security Roles and Responsibilities, Section 14. System Owners, page 27, states:

> k. Conducting annual reviews and validation of system users' accounts to ensure the continued need for access to a system and verify users' authorizations (rights/privileges).

Chapter 4: Policy for Protect Function, Section 1. Identity Management, Authentication and Access Control, page 46, states:

> d. Information system accounts must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Reviews and validations of all user accounts shall be completed annually to ensure the continued need for system access.

GSA management informed us that the information system users were customer agencies users and not GSA employees or contractors. Therefore, the information system support team allowed those information system users to self-reauthorize their access. Without implementing an effective reauthorization process where the system owner or supervisor performs the validation that the individual still has a business need for his/her access, unauthorized access to information system could be permitted. Therefore, the confidentiality, integrity, and availability of the information system data could be compromised.

RECOMMENDATIONS:

We recommend that GSA:

1. Update the information system security policy, processes, and procedures to require supervisors to review information system 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 the information system users' access and update or remove any access and privileges that are not commensurate with current job responsibilities.

Protect – 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.

GSA IT Security Policy CIO 2100.1M, March 26, 2021, Chapter 4: Policy for Protect Function, Section 1. Identity Management, Authentication and Access control, page 46, states:

> e. Disabling and removal of user accounts supporting account management processes, to include:
>
> (1) Supervisors being responsible for coordinating and arranging system access termination for all departing or resigning personnel, both Federal employees and contractors.
>
> (2) Account removal being initiated by a user's supervisor, COR, or through the review of information provided by the OCISO (e.g., separation lists, role revisions). Data and system owners must verify within 30 days that separated personnel no longer maintain access to GSA IT systems or resources.

GSA IT Security Procedural Guide: Termination and Transfer CIO-IT Security-03-23, Revision 5, May 25, 2021, Section 6.1. PS-4 Personnel Termination, pages 13–14, states:

> Control: Upon termination of individual employment:
>
> a. Disable system access within [*30 days of personnel termination*]; …
>
> ***System Specific Expectations***: The supervisor/CO [contracting officer]/COR is responsible for notifying the appropriate ISSMs/ISSOs of a user's off-boarding so they can take appropriate action at a system/application level.

Because the information system users must first authenticate to the GSA network using their PIV cards and Personal Identification Numbers before accessing information system, GSA management stated that it did not disable the information system access of the two terminated users since the users' PIV cards were suspended and returned. Without removing the terminated users' accounts from the information system within 30 days of separation from GSA, an unauthorized user may utilize the information system accounts to gain access to the system. This could result in the unauthorized modification, destruction, or exposure of critical information system data. However, since the two users' PIV cards were returned, there is a lower risk of unauthorized access.

RECOMMENDATIONS:

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 user accounts of terminated users, regardless of whether these users' PIV cards were suspended and returned.

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. We made this determination based on assessing most of the FY 2021 IG FISMA Reporting Metrics as "Managed and Measurable" and "Optimized." Specifically, the Identify, Protect, Detect, and Respond Cybersecurity functions were assessed as "Optimized," while the Recover function was rated as "Consistently Implemented." We also followed up on the status of nine prior-year findings and reported that they were closed (see Appendix I). However, we did identify four findings within one of the five Cybersecurity functions (Protect) and within two of the nine FISMA Metric Domains (Configuration Management and Identity and Access Management). The nature of these findings did not affect our overall assessment of the Protect function after determining the mode of the 30 Protect IG metric questions.

We made 13 recommendations related to the 4 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

12/8/2021

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

FROM DAVID A. SHIVE
CHIEF INFORMATION OFFICER – I

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 2021

The Office of the Chief Information Officer appreciates the opportunity to review and comment on the draft evaluation report entitled Independent Audit on the Effectiveness of the U.S.General Services Administration's Information Security Program and Practices Report – Fiscal Year 2021. 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 nine prior-year findings were closed.

Prior-year Findings – 2018 Evaluation

Finding Number	Prior-year Condition	Recommendation(s)	Status
3. Protect Function – Identity and Access Management **Account Management**	We identified the following exceptions: For one out of 634 separated users, GSA did not remove access to the user's network account timely (within 30 days of user separation).	We recommend GSA perform the following actions: 2. Compare the Separations Report to the Active Directory user listing on a monthly basis to ensure separated users are removed from the Active Directory.	Closed

Prior-year Findings – 2019 Evaluation

Finding Number	Prior-year Condition	Recommendation(s)	Status
2. Protect Function – Identity and Access Management **Account Management**	We determined that 1 out of 613 separated GSA employees from October 1, 2018 through June 30, 2019 maintained an active network account past the allotted 30 days from separation.	1. We recommend that GSA implement a monitoring control to review rejected tickets related to separated employees and contractors on a monthly basis.	Closed

Prior-year Findings – 2020 Evaluation

Finding Number	Prior-year Condition	Recommendation(s)	Status
1. Protect Function – Configuration Management **Unsupported Software**	We determined that as of December 2018, the vendor no longer supports the database version that was in production and supporting a system. GSA implemented a current version of the database on August 20, 2020.	1. Implement a monitoring process to track and identify software components that are no longer supported by vendors and update to a currently supported version, as appropriate. 2. For platform as a service providers, implement a monitoring process that verifies that vulnerability scans, which are provided to GSA, are configured to identify outdated software, which is the responsibility of GSA to update.	Closed Closed
2. Protect Function – Configuration Management **Unauthorized Application Changes**	We determined that five out of five selected application changes did not have authorization prior to implementation into the production environment for one information system selected for testing.	1. Design and implement a quality control process to validate that designated agency officials have authorized all application changes prior to implementing these changes in the production environment. 2. Evaluate and document the five unauthorized changes to confirm that the system's production environment was not adversely affected.	Closed Closed
3. Protect Function – Configuration Management **Lack of Baseline Configuration**	We determined that for one out of five selections for one information system selected for testing, evidence of management's baseline configuration scan review was not available.	1. Implement a consistent method to document and retain management's review of system baseline configuration scans that includes the actions performed,	Closed

Finding Number	Prior-year Condition	Recommendation(s)	Status
Scan Review Documentation		who performed the review, and the date of the review.	
4. Protect Function – Identity and Access Management **Accounts Not Reauthorized**	We determined individuals who have privileged access for infrastructure accounts (operating system and database) perform a self-reauthorization.	1. Implement the new controls that restrict privileged operating system and database users from self-reauthorizing their accounts. 2. Update GSA Security policies to require privileged operating system and database user accounts to be reauthorized on a more frequent basis.	Closed Closed
5. Protect Function – Identity and Access Management **Inconsistent Documenting of Splunk Audit Alerts**	We determined that management, for three information systems selected for testing, was not consistently documenting its review of the audit log alerts for each system.	1. Implement a consistent method to document the review of audit log alerts that includes the actions performed, who performed the review, the date of the review, and maintain the evidence.	Closed
6. Protect Function – Identity and Access Management **User Accounts Not Removed Timely**	We determined that GSA did not remove user accounts timely for separated individuals from October 1, 2019, through June 30, 2020, for three systems: • Five out of 721 separated individuals maintained an active network account past the allotted 30 days after separation from the Agency. One of the accounts was accessed after the separation date. • One out of 721 separated GSA individuals maintained	1. Disable/remove the separated users' accounts. 2. Implement a monitoring control to perform a comparison of the separations listing, ticketing system deletes, and active user accounts on a monthly basis to identify and remove user accounts that were missed during the normal exiting/off-boarding process.	Closed Closed

Finding Number	Prior-year Condition	Recommendation(s)	Status
	an active user account past the allotted 30 days after separation from the Agency, for one information system selected for testing. • Two out of 721 separated GSA individuals maintained active user accounts past the allotted 30 days after separation from the Agency, for one other information system selected for testing. All separated individuals' user accounts, cited above, have subsequently been removed.		
7. Protect Function – Identity and Access Management **User Accounts Not Authorized**	We determined the following: • Management did not formally authorize one out of one new application user account selected for testing before the account was created in the system. • Management did not formally authorize one out of seven new application user accounts selected for testing before the account was created in the system.	1. Provide training to individuals responsible for information system user account creation and authorization to emphasize adherence to the access authorization controls described in the respective SSPs and GSA IT Security Procedural Guide: AC CIO-IT Security-01-07.	Closed

Appendix II – Glossary

Acronym	Definition
AC	Access Control
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
AOR	Acceptance of Risk
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
COR	Contracting Officer's Representative
CP	Contingency Planning
C-SCRM	Cyber Supply Chain Risk Management
CTO	Chief Technology Officer
Cybersecurity Framework	National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity
DB	Database
DHS	Department of Homeland Security
DPP	Data Protection and Privacy
FAS	Federal Acquisition Service
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GRC	Governance Risk and Compliance
GSA	U.S. General Services Administration
I	GSA's Chief Information Officer (CIO)
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
IQ	Office of Acquisition Information Technology Services
IR	Incident Response
IS	Office of Chief Information Security Officer (OCISO)
ISCM	Information Security Continuous Monitoring
ISE	Security Engineering Division
ISI	Identity, Credential, and Access Management Shared Service Division
ISO	Security Operations (SecOps) Division
ISP	Policy and Compliance Division
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IST	Information System Security Officer (ISSO) Support Division
IT	Information Technology
KPMG	KPMG LLP
NIST	National Institute of Standards and Technology
OCISO	Office of Chief Information Security Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OS	Operating System
PB-ITS/IP	Office of Public Buildings Information Technology Services
PBS	Public Buildings Service

Acronym	Definition
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
Rev	Revision
RM	Risk Management
SCRM	Supply Chain Risk Management
SecOps	Security Operations
SIEM	Security Information and Event Management
SP	Special Publication
ST	Security Training