U.S. SMALL BUSINESS ADMINISTRATION OFFICE OF INSPECTOR GENERAL

Fiscal Year 2023 Federal Information Security Modernization Act

Evaluation Report

Report 24-07

March 7, 2024

Make a Difference

To report fraud, waste, or mismanagement, contact the U.S. Small Business Administration's Office of Inspector General Hotline at https://www.sba.gov/oig/hotline. You also write to the U.S. Small Business Administration, Office of Inspector General, 409 Third Street, SW (5th Floor), Washington, DC 20416. In accordance with the Inspector General Act of 1978, codified as amended at 5 U.S.C. §§ 407(b) and 420(b)(2)(B), confidentiality of a complainant's personally identifying information is mandatory, absent express consent by the complainant authorizing the release of such information.

NOTICE:

Pursuant to the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Public Law 117-263, Section 5274, any nongovernmental organizations and business entities identified in this report have the opportunity to submit a written response for the purpose of clarifying or providing additional context as it relates to any specific reference contained herein. Comments must be submitted to AIGA@sba.gov within 30 days of the final report issuance date. We request that any comments be no longer than two pages, Section 508 compliant, and free from any proprietary or otherwise sensitive information. The comments may be appended to this report and posted on our public website.

U.S. Small Business Administration
Office of Inspector General

Executive Summary

Fiscal Year 2023 Federal Information Security Modernization Act (Report 24-07)

What OIG Reviewed

This report summarizes the results of our fiscal year (FY) 2023 Federal Information Security Modernization Act (FISMA) of 2014 evaluation and assessment of the U.S. Small Business Administration's (SBA) information security systems policies, procedures, and practices.

Our objectives were to determine whether SBA complied with FISMA and assess the maturity of controls used to address risks in each of the nine security domains.

The Office of Inspector General (OIG) contracted with KPMG LLP, an independent public accounting firm, that then used FISMA's maturity model spectrum to test a subset of systems and security controls to assess SBA's adherence to FISMA requirements.

The maturity model uses scores of 1 (worst) to 5 (best) to determine if domains were ad hoc, 1; defined, 2; consistently implemented, 3; managed and measurable, 4; or optimized, 5. Also of note, a rating of 4, managed and measurable, describes security controls that are effective, so baseline. Ratings of ad hoc, defined, and consistently implemented are below the baseline for an effective security program.

What OIG Found

We found SBA generally responded to previously identified vulnerabilities and made progess in three of the nine domains. The agency met the baseline in the area of incident response but fell below the baseline for an effective security program in the following areas:

- Risk management: consistently implemented
- Supply chain risk management: defined
- Configuration management: defined
- Identity and access management: consistently implemented
- Data protection and privacy: consistently implemented
- Security training: defined
- Information security continuous monitoring: consistently implemented
- Contingency planning: defined

We rated SBA's overall information security program as "not effective."

OIG Recommendations

There are five open recommendations from two previous evaluations (Appendix 2). In this report, we made 11 recommendations for improvements in 6 domains: risk management, supply chain risk management, identity and access management, data protection and privacy, security training, and contingency planning. We did not repeat recommendations from previous years being implemented in the areas of risk management, supply chain risk managment, and contingency planning.

Agency Response

The agency agreed with all 11 recommendations. To address these recommendations, the agency is implementing corrective measures to include inventory software, personal identity verification card compliance, and updating applicable policies and procedures.

OFFICE OF INSPECTOR GENERAL
U.S. SMALL BUSINESS ADMINISTRATION

MEMORANDUM

Date: March 7, 2024

To: Isabel Casillas Guzman
Administrator

From: Hannibal "Mike" Ware
Inspector General

Subject: Evaluation of Fiscal Year 2023 Federal Information Security Modernization Act (Report 24-07)

This report presents the results of our evaluation on information security weaknesses, *Fiscal Year 2023 Federal Information Security Modernization Act*. SBA management agreed with all our recommendations. In this report we made 11 recommendations for improvements.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact me or Andrea Deadwyler, Assistant Inspector General for Audits, at (202) 205-6586.

cc: Dilawar Syed, Deputy Administrator
Arthur Plews, Chief of Staff
Isabelle James, Deputy Chief of Staff
Steve Kucharski, Acting Chief Information Officer, Office of the Chief Information Officer
Luis Campudoni, Deputy Chief Information Officer, Office of the Chief Information Officer
Kelvin Moore, Chief Information Security Officer, Office of the Chief Information Officer
Therese Meers, General Counsel
Katherine Aaby, Associate Administrator, Office of Performance, Planning, and the Chief Financial Officer
Deborah Chen, Deputy Chief Financial Officer, Office of Performance, Planning, and the Chief Financial Officer
Walter B. Hill Jr., Chief Risk Officer, Office of Strategic Management and Enterprise Integrity
Kathryn Frost, Associate Administrator, Office of Capital Access
John Miller, Deputy Associate Administrator, Office of Capital Access
Peter Meyers, Senior Adviser, Office of Capital Access
Michael Simmons, Attorney Advisor, Office of General Counsel
Tonia Butler, Director, Office of Internal Controls
Anna Maria Calcagno, Director, Office of Program Performance, Analysis, and Evaluation

Contents

Figures

Appendices

Introduction

The Federal Information Security Modernization Act (FISMA) of 2014 requires each office of inspector general, or an independent external auditor, to independently evaluate the effectiveness of the information security program and practices of its agency.[1]

This report summarizes the results of our fiscal year (FY) 2023 evaluation of the U.S. Small Business Administration's (SBA) information technology (IT) systems. The purpose of this report is to assess the effectiveness, or maturity, of the controls used to address risks in each of the required review areas, referred to as domains.

The Office of Inspector General (OIG) contracted with KPMG LLP, an independent public accounting firm, for our FY 2023 FISMA evaluation. KPMG tested a representative subset of SBA systems and security controls and assessed whether SBA adhered to or made progress in implementing minimum security standards and requirements appropriate for each system's security categorization and level of risk. OIG monitored KPMG's work and reported SBA's compliance with the Act through the FISMA CyberScope submission in August 2023.

FISMA requires agencies to protect information security at a level equal to the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, modification, or destruction of information or disruption to IT systems. Each federal agency must secure its information and information systems that support its operations, including those provided or managed by other agencies and contractors (such as third-party service providers).

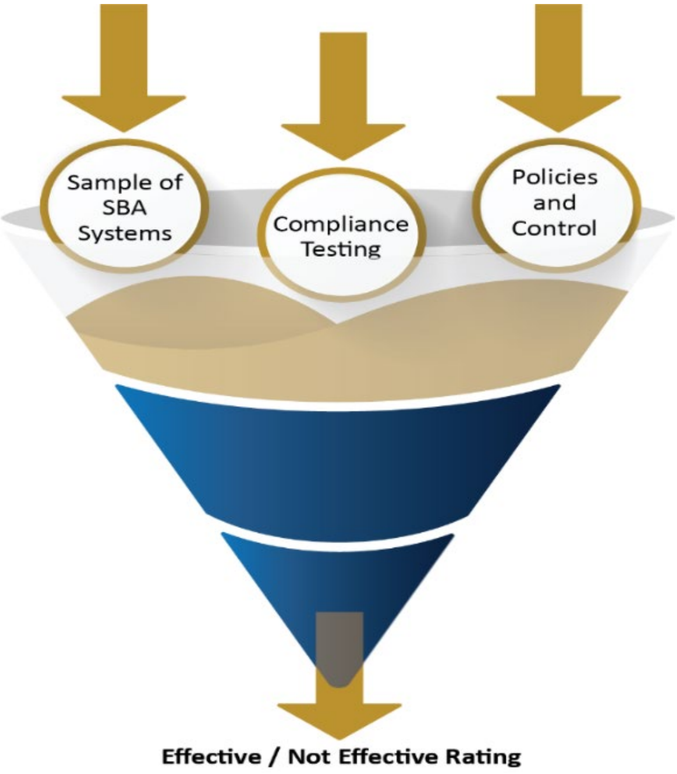
This evaluation reflects the significant changes the Office of Management and Budget (OMB) made to the FISMA oversight and metrics collection in FY 2022 and 2023. These changes are intended to rate an agency in certain high-risk areas, improve the quality of performance data collected across the whole agency, accelerate our efforts to make more informed risk-based decisions, and achieve observable security outcomes.

Background

FISMA requires federal agencies to develop and maintain an agency-wide information security program to ensure they stay current with evolving threats and reduce the risk of data breaches and other security threats. The Act also requires agencies to send an annual report to OMB, Congress, and the Government Accountability Office on the adequacy and effectiveness of their information security policies, procedures, and practices.

[1] 42 U.S. Code § 3555.

Figure 1: How Security Ratings are Determined



Source: OIG generated from SBA data

We accessed effectiveness of the following nine 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
- Contingency planning

As illustrated in Figure 1, each office of inspector general is required to assess the effectiveness of information security programs using a maturity model spectrum that has a numeric metric or rating and a corresponding label within each domain. These ratings capture the agency's proficiency with its policies and procedures and ensure sound practices.

OMB and the U.S. Department of Homeland Security issue the annual FISMA metric guidance to evaluate an agency's information security programs. FISMA metrics are a core set of 20 questions with an additional 20 supplemental questions that were introduced this fiscal year. Compliance tests are derived from the FISMA metrics. These tests are applied to a subset of SBA systems to measure compliance with policies and controls. The results of these tests indicate whether each domain is rated as effective or not effective, as illustrated in Figure 2. Rating scores of effective and not effective are determined by the calculated average of responses to questions in a domain.

KPMG sampled and tested a representative subset of seven SBA systems. The maturity model uses scores of 1 (worst) to 5 (best) to reflect a rating of ad hoc, 1; defined, 2; consistently implemented, 3; managed and measurable, 4; or optimized, 5. A rating of managed and measurable describes security controls that are effective, rated 4 out of a scale of 5, so baseline. Ratings of ad hoc, defined, and consistently implemented are below the baseline for an effective security program.

Ratings in the nine domains are determined by a calculated average across all metrics in a domain. For example, to maintain a rating of managed and measurable in a domain that has two questions, at least one of the two metric questions must earn the managed and measurable rating.

Objectives

Our objectives were to determine whether SBA complied with FISMA and assess the maturity of controls used to address risks in each of the nine 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.

Results

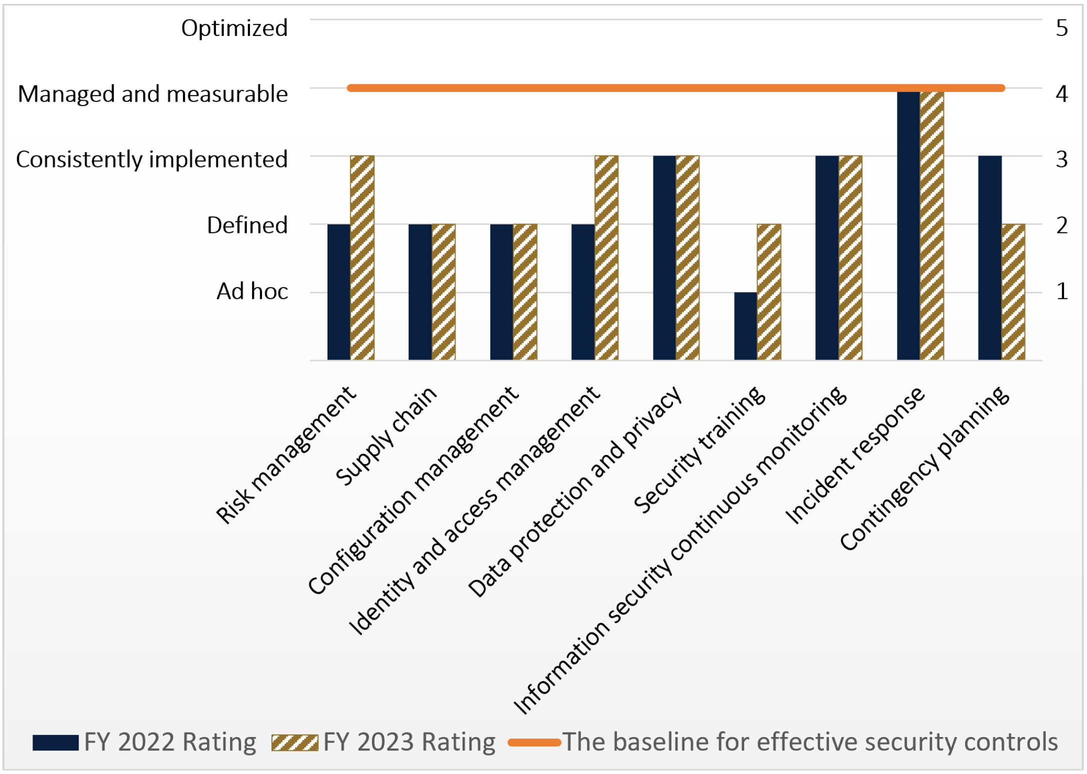
KPMG's evaluation of core metrics across the nine domains indicated that SBA continued to achieve a rating of 4, managed and measurable, in incident response. SBA was rated as either 2, defined, or 3, consistently implemented, in the remaining eight domains. We rated SBA's overall cybersecurity as "not effective" in FY 2023 because only one of the nine domains was ranked as managed and measurable, the baseline for an effective security program.

If a metric testing result identified an area requiring improvement, we determined the impact of deficiencies and whether a recommendation was needed. In most cases, this occurred when a policy or procedure was established but not consistently implemented.

Using the criteria in federal guidance, outlined in Appendix 1, we ranked and illustrated (see Figure 2) SBA's IT security domains as follows:

- Risk management: consistently implemented
- Supply chain risk management: defined
- Configuration management: defined
- Identity and access management: consistently implemented
- Data protection and privacy: consistently implemented
- Security training: defined
- Information security continuous monitoring: consistently implemented
- Incident response: managed and measurable
- Contingency planning: defined

Figure 2: Domain Ratings for FY 2023 and FY 2022



Source: OIG generated from CyberScope results

Open recommendations from previous evaluations in risk management, supply chain risk management, and contingency planning are not repeated in this report (see Appendix 2) in the domain test results below. We also did not have findings in the areas of incident response and information security continuous monitoring and therefore, do not discuss these areas in this report.

Challenges and Improvements

Within the scope of this evaluation, we found SBA generally responded to previously identified vulnerabilities. The agency made progress in risk management, identity and access management, security training, and continues to be rated at the effective maturity level for incident response. However, the results of our tests show SBA continues to experience security control challenges in areas of risk management, supply chain risk management, configuration management, identity and access management, security training, and contingency planning.

Domain Test Results

The following section details the testing results of the domains. A reportable condition occurs when an area needs improvement to achieve a consistently implemented capability. Each section outlines the scope of the review, test results, and recommendations for improvement.

Finding 1: Risk Management

Risk management focuses on policies and actions that manage information security risks to the organization. We determined that SBA's risk management maturity level scored 3 out of a possible 5 and is labeled consistently implemented. For a definition of the consistently implemented maturity level, see Appendix 3. SBA can improve security in this domain by resolving the following vulnerabilities:

Software System Inventory

The *FY 2023 Inspector General FISMA Evaluator's Guide* states having an agency-wide software asset management capability in place is considered an effective level of security. FISMA requires agencies to maintain a comprehensive and accurate inventory of its information systems to include third-party systems. SBA did not consistently maintain an up-to-date listing of software assets connected to SBA's network. Agency management stated that a lack of resources has not allowed them to implement a process to track software inventories.

Accurate inventory tools are needed to provide oversight and visibility to all systems. An inventory update process is also needed to maintain up-to-date software configurations and prevent unauthorized software from being installed.

Hardware Asset Inventory

FISMA requires agencies to maintain a comprehensive and accurate inventory of its hardware assets to include third-party systems. While SBA has established a process to maintain an inventory of its hardware assets connected to its network, the process does not capture a complete and accurate inventory that is necessary for tracking, reporting, and approval.

The *FY 2023 Inspector General FISMA Evaluator's Guide* states having an agency-wide hardware asset management capability in place is considered an effective level of security. Agency management stated that a lack of resources has not allowed them to implement a process to fully track hardware assets. Without a fully established process in place, SBA may not be able to assess and manage cybersecurity risks or known vulnerabilities in its hardware assets. So, hardware assets such as servers could be vulnerable to internal and external threats or attacks.

The recommendation for this finding was previously identified in OIG Report 23-03, *Fiscal Year 2022 Federal Information Security Modernization Act Review*, and has not been closed by the agency. Therefore, there is no recommendation for this finding in this report.

System Inventory

FISMA requires agencies to maintain a comprehensive and accurate inventory of information systems. While SBA has policies and procedures for maintaining its information systems, our evaluation determined SBA's inventory was not accurate. We identified one system that had been approved and was deployed for production; however, the system was identified in the inventory as under development.

The *FY 2023 Inspector General FISMA Evaluator's Guide* states information systems included in the inventory that are subjected to continuous monitoring are considered an effective level of security. Currently, SBA does not have a defined frequency for reviewing its official system inventory, although agency management did state they were separately tracking and reporting the system as one that is in production. By not maintaining an accurate inventory, management may not be aware of risks that could be introduced.

Plans of Action and Milestones

The *FY 2023 Inspector General FISMA Metrics Evaluator's Guide* states that measuring the effectiveness of the organization's plans of action and milestones process and using that information to make adjustments is considered an effective level of security. FISMA requires that an organization use plans and milestones to mitigate security weaknesses, and OMB Memorandum 02-01 requires them to only be closed when a weakness has been fully resolved and the corrective action tested. We found SBA's policy does not require the closure of plans and milestones based on completion. Instead, a replacement plan is created if the weakness is not remediated within a year of creation. SBA has reported that because of a lack of resources, its managers have focused on closing plans and milestones instead of correcting the underlying cause of the issue.

By prematurely closing plans and milestones and reissuing new ones before they are corrected, identified risks are not resolved. Specifically, there is reduced visibility to track weaknesses over time because closed plans and milestones do not provide assurances that planned corrective actions and milestones were implemented.

Update to Enterprise Risk Management Framework Guide

SBA policy requires the *Enterprise Risk Management Framework Guide* to be reviewed on an annual basis. Our review found the framework guide had not been reviewed since 2019. Due to a lack of resources as well as personnel changes, the guide has not been reviewed annually to make necessary updates. By not ensuring the framework guide is reviewed on an annual basis, program and support offices may not receive any changes or updates to existing responsibilities within the framework. Additionally, failure to update the framework guide increases the risk that SBA management may not be aware of the actual security posture of the agency, and risks may not be identified or sufficiently mitigated.

Recommendations

We recommend the Administrator direct the Office of the Chief Information Officer to:

Recommendation 1: Complete the implementation of an automated solution to help ensure a complete and accurate inventory of software assets.

Recommendation 2: Define a required frequency for updating the system inventory and implement a quality control process to validate that system inventories are updated in a timely manner.

Recommendation 3: Update existing policy and procedures to ensure plans of action and milestones are closed only after the planned corrective actions and milestones have been implemented.

We recommend the Administrator direct the Office of Continuous Operations and Risk Management to:

Recommendation 4: Review the *Enterprise Risk Management Framework Guide* annually and update if needed.

Finding 2: Supply Chain Risk Management

Supply chain risk management focuses on the development, acquisition, and disposal of IT systems and services in accordance with federal security guidance. We determined the agency’s supply chain risk management maturity level was defined. Definitions for the defined maturity level are found in Appendix 3.

Supply chain risk management domain can be improved through the resolution of the following vulnerabilities:

Development of a Supply Chain Risk Management Strategy

While we determined that SBA has developed a supply chain risk management assessment plan, the results have not been finalized or integrated into SBA's strategy for managing supply chain risks nor integrated into SBA's enterprise risk management framework. This integration includes the development of goals and a formal process to consistently capture and share lessons learned on the effectiveness of its supply chain strategy and program. The Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act of December 2018 requires agencies to develop an overall supply chain strategy and implementation plan to guide and govern these activities.[2]

The *FY 2023 Inspector General FISMA Metrics Evaluator's Guide* states that using performance measures on the effectiveness of its supply chain and making updates accordingly is considered an effective level of security. SBA management indicated a lack of resources and recent personnel changes prevented the development and finalization of a supply chain strategy and a process to consistently capture and share lessons learned. Without an effective supply chain strategy, SBA may not adequately consider security and privacy risks associated with the development, acquisition, maintenance, and disposal of its systems.

Review of Supply Chain Regarding Third-Party Suppliers

In FY 2022, SBA established a supply chain risk management policy as required by SBA policy 90 47 6.[3] However, we determined SBA did not include policy requirements that management review internal and third-party supply chain risks, including reviews done internally as well as by third-party service providers. National Institute of Standards and Technology (NIST) 800-53 Rev. 5 states organizations should consider their potential supply-chain risk when establishing a methodology for managing risk including that of external service providers.[4]

The *FY 2023 Inspector General FISMA Metrics Evaluator's Guide* states having qualitative and quantitative measures incorporated in policies and procedures to measure external providers as well as supplier risk assessments is considered an effective level of security. Not having a process in place to review supply chain risk management requirements could mean that the organization is unaware of the risks within their operating environment, and this affects the agency's ability to make decisions based on that risk. The recommendation for this finding was previously identified

[2] Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology Act. Pub. L. No. 115-390, (December 21, 2018).

[3] SBA, Standard Operating Procedure 90 47 6, Cybersecurity and Privacy Policy, (March 28, 2022).

[4] NIST, SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, at Control SR-7, Supply Chain Operations Security (September 2020).

in OIG Report 23-03, *Fiscal Year 2022 Federal Information Security Modernization Act Review*, and has not been closed by the agency. Therefore, there is no recommendation for this finding in this report.

Recommendation

We recommend the Administrator direct the Office of the Chief Information Officer to:

Recommendation 5: Develop a strategy to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements.

Finding 3: Configuration Management

Configuration management focuses on the integrity of IT products and information systems as they change. We determined the agency's configuration management maturity level was defined. This domain can be improved through resolution of the following vulnerabilities:

Baseline Configuration Changes

NIST 800-53 states agencies should monitor and control configuration settings in accordance with its own policies and procedures. Our evaluation identified that SBA has not defined a timeframe for remediation of configuration weaknesses identified during baseline and configuration scans.

The *FY 2023 Inspector General FISMA Metrics Evaluator's Guide* states using automated mechanisms to detect unauthorized changes is considered an effective level of security. Without a consistent process for remediating baseline configuration changes, there is a risk that flaws in the IT environment could expose information systems and applications to unauthorized modification or data being compromised.

Vulnerability Remediation Process

SBA did not reinforce its patch management guidelines to ensure that agency systems were properly configured, and vulnerabilities remediated within specified timeframes, as required by SBA Standard Operating Procedure (SOP) 90 47 6, Cybersecurity and Privacy Policy. Software version control and vulnerability testing is a continuous process. SBA's existing remediation process should prioritize criticality, timeliness, and communication of issues to accountable parties.

The *FY 2023 Inspector General FISMA Metrics Evaluator's Guide* states that an automated flaw remediation process and prioritization of flaw remediation based on risk are considered an effective level of security. If SBA does not make security updates promptly, there is an increased risk that the confidentiality, integrity, and availability of the data residing on information systems will be compromised. There also is an increased risk that existing or new vulnerabilities could expose information systems and applications to attacks, unauthorized modification, or compromised data.

Recommendations

We recommend the Administrator direct the Office of the Chief Information Officer to:

Recommendation 6: Define timeframe and remediation requirements for baseline and configuration weaknesses.

We recommend the Administrator direct the Office of the Chief Information Officer and Office of Capital Access to:

Recommendation 7: Properly update and remediate vulnerabilities and configuration weaknesses throughout the SBA environment.

Finding 4: Identity and Access Management

The identity and access management domain requires implementation of policies and procedures to ensure that only authorized users can access SBA IT resources. We determined that the agency's maturity level was consistently implemented. This domain can be improved by resolving the following vulnerability:

Multi-factor Authentication for Non-privileged Users

Our evaluation identified that SBA did not enforce multi-factor authentication for non-privileged users across its network. Of the 15,109 total network accounts, 11,323 did not require the use of a personal identity verification (PIV) card. A PIV card is one way an organization can authenticate users to the network through multi-factor authentication.

The *FY 2023 Inspector General FISMA Metrics Evaluator's Guide* states non-privileged users that use strong authentication to authenticate to systems and facilities is considered an effective level of security. Due to the Coronavirus 2019 (COVID-19) pandemic, SBA management initiated a waiver for PIV authentication. This waiver expired on September 30, 2022 and was not renewed; however, the practice of not requiring users to authenticate using a PIV continued.

There is a greater risk of unauthorized access to SBA's systems when solely relying on usernames and passwords.

Recommendation

We recommend the Administrator direct the Office of the Chief Information Officer to:

Recommendation 8: Implement a process to track and enforce compliance with PIV implementation and multi-factor requirements.

Finding 5: Data Prevention and Privacy

The data protection and privacy domain requires implementation of policies and procedures for the handling of personally identifiable information and data exfiltration. We determined that the agency's maturity level was consistently implemented. This domain can be improved by resolving the following vulnerability:

Biannual Update of Polices

Our evaluation determined that SBA did not update its implementation procedures for data loss prevention on a biannual basis. The latest version of this policy is dated July 15, 2020. This document has a requirement to be updated at least biannually. SBA management stated due to recent personnel changes and limited resources, the update was not done.

The *FY 2023 Inspector General FISMA Metrics Evaluator's Guide* states that using qualitative and quantitative performance measures on the effectiveness of its privacy program and adjusting as needed is considered an effective level of security. If SBA policies and procedures are not reviewed and updated, there is an increased risk that sufficient controls are not implemented, which may then increase the risk of data exfiltration of information or compromise of personally identifiable information.

Recommendation

We recommend the Administrator direct the Office of the Chief Information Officer to:

Recommendation 9: Ensure implementation procedures for data loss prevention are updated at least on a biannual basis to reflect new processes and new requirements.

Finding 6: Security Training

The security training domain requires system users to have the proper IT training relevant to their IT security role and to the system. We determined that this domain's maturity level was defined. This domain can be improved by resolving the following vulnerability:

Role Based Training

SBA management did not enforce controls consistently to require and track role-based training for individuals with significant IT responsibilities. In order to evaluate this requirement, we examined the training records of 25 SBA IT employees. Specifically, while 11 of 25 individuals with privileged access were properly identified, they were not required to complete the annual role-based security training. SBA's Awareness and Training Implementation Procedures outlines that personnel with significant security responsibilities must take role-based training annually. The 11 individuals were not required to complete annual role-based training because even though SBA's training policy specifies which positions are required to have role-based training, the process of identifying users with significant security responsibilities is manually intensive and does not capture everyone with privileged access.

The *FY 2023 Inspector General FISMA Metrics Evaluator's Guide* states the use of qualitative and quantitative measures of its security training program to gauge its effectiveness is considered an effective level of security.

Recommendation

We recommend the Administrator direct the Office of the Chief Information Officer to:

Recommendation 10: Update existing procedures that identify the roles of individuals with significant IT responsibilities who require role-based training and ensure such training is provided and tracked.

Finding 7: Contingency Planning

Contingency planning is defined as both restoration and implementation of alternative processes when systems are compromised. We determined this domain's maturity level was defined. This domain can be improved by resolving the following vulnerability:

Contingency Planning Training

Our evaluation determined that SBA management did not provide contingency planning training to system users consistent with their assigned roles and responsibilities within the first year of assuming a contingency role or responsibility, as well as annually afterward. SBA's Contingency Planning Implementation Procedure states the Chief Information Officer provides contingency training annually to system owners, information system security owners, and other relevant stakeholders.

The *FY 2023 Inspector General FISMA Metrics Evaluator's Guide* states that using automated mechanisms to test contingency plans and coordinate plan testing with external stakeholders is considered an effective level of security. SBA management indicated that they are aware of the weakness and are tracking it through the plan of action and milestones process.

Recommendation

We recommend the Administrator direct the Office of the Chief Information Officer to:

Recommendation 11: Provide training to individuals with contingency planning roles and responsibilities.

Testing of the Continuity of Operations Plan

Our evaluation revealed that SBA's continuity of operations plan and the accompanying business impact assessment were not tested nor updated as required. The continuity of operations plan was last updated in 2020 and was last tested in 2021 during the U.S. Department of Homeland Security's (DHS) Eagle Horizon exercise. SBA officials indicated that because of the COVID-19 pandemic, as well as competing priorities, the continuity of operations plan and business impact assessment were not tested annually. The DHS Federal Emergency Management Agency's Federal Continuity Directive 1 states that the business impact assessment must be updated at least every 2 years, and the continuity of operations plan must be tested annually. A business impact analysis determines the effect on the agency in case the system is disrupted or unavailable.

The *FY 2023 Inspector General FISMA Metrics Evaluator's Guide* states having metrics on the effectiveness of recovery activities that are obtained accurately and consistently is considered an effective level of security. Inconsistent documentation and testing of the continuity of operations plan increases the risk that SBA mission critical functions could become unavailable and impact business operations. This can consequently decrease SBA's ability to adequately protect and recover critical information systems. The recommendation for this finding was previously identified in OIG Report 22-11, *Fiscal Year 2021 Federal Information Security Modernization Act Review*, and has not been closed by the agency; therefore, there is no recommendation for this finding in this report.

Evaluation of Agency Response

The agency agreed with all 11 recommendations. To address these recommendations, the agency is planning to implement corrective measures to include inventory software, PIV card compliance, and updating applicable policies and procedures. See Appendix 4 for management's comments in their entirety.

Summary of Actions Necessary to Close the Recommendations

The following section summarizes the status of our recommendations and the actions necessary to close them.

Recommendation 1

Complete the implementation of an automated solution to help ensure a complete and accurate inventory of software assets.

Status: Resolved

SBA management agreed with the recommendation and has implemented ServiceNow for software management. SBA stated it implemented ServiceNow on September 10, 2023. SBA intends to complete final action by providing documentation by April 30, 2024. This recommendation can be closed when SBA management provides documentation that an automated solution for inventory of software assets has been established.

Recommendation 2

Define a required frequency for updating the system inventory and implement a quality control process to validate that system inventories are updated in a timely manner.

Status: Resolved

SBA managers agreed with the finding and stated that they are planning to implement ServiceNow to provide real time updates to Office of the Chief Information Officer personnel to ensure all systems are valid, as well as add continuous monitoring capabilities for unauthorized systems. SBA plans to have ServiceNow in place and this recommendation closed by September 30, 2024. This recommendation can be closed when SBA provides evidence that an established frequency for system inventory updates and a quality control process to update system inventories in a timely manner, have been developed and implemented.

Recommendation 3

Update existing policy and procedures to ensure plans of action and milestones are closed only after the planned corrective actions and milestones have been implemented.

Status: Resolved

SBA management agreed with the finding. SBA plans to update the policy to ensure plans of action and milestones are closed only after corrective actions have been taken. SBA plans to have this policy updated for closure of final action by September 30, 2024. This recommendation can be closed when SBA managers provide evidence that their plans of action and milestones policy has been updated to reflect closure only when the issues have been corrected.

Recommendation 4

Review the *Enterprise Risk Management Framework Guide* annually and update if needed.

Status: Resolved

SBA management agreed to update the *Enterprise Risk Management Framework Guide* on an annual basis. SBA intends to complete final action on September 30, 2024. This recommendation can be closed when SBA management provides documentation that the *Enterprise Risk Management Framework Guide* has been updated at least annually.

Recommendation 5

Develop a strategy to ensure that products, system components, systems, and services of external providers are consistent with the organization’s cybersecurity and supply chain requirements.

Status: Resolved

SBA management agreed to develop strategy for external providers. The Office of the Chief Information Officer has updated its policy for cybersecurity and supply chain risk for IT acquisitions and will work with other program offices to incorporate this policy into SBA’s acquisition program. SBA intends to complete final action by September 30, 2024. This recommendation can be closed when SBA provides documentation that policies regarding external providers have been updated to reflect cybersecurity and supply chain requirements.

Recommendation 6

Define timeframe and remediation requirements for baseline and configuration weaknesses.

Status: Resolved

SBA management agreed with the recommendation and stated the agency will review and update processes and procedures for defining baseline deviation remediation. SBA intends to complete final action by September 30, 2024. This recommendation can be closed when SBA provides documentation that remediation for baseline and configuration deviations have been defined.

Recommendation 7

Properly update and remediate vulnerabilities and configuration weaknesses throughout the SBA environment.

Status: Resolved

SBA management agreed with the recommendation and will work with system owners and information system security owners to ensure vulnerabilities are remediated according to policy. SBA intends to complete final action by September 30, 2024. This recommendation can be closed when SBA management provides documentation that vulnerabilities and configuration weaknesses are remediated according to agency policies.

Recommendation 8

Implement a process to track and enforce compliance with PIV implementation and multi-factor requirements.

Status: Resolved

SBA management agreed with the recommendation and will establish a process to monitor PIV compliance that will include a waiver process for those employees that are exempt. SBA intends to complete final action by September 30, 2024. This recommendation can be closed when SBA management provides documentation that a process has been established to track and enforce PIV implementation.

Recommendation 9

Ensure implementation procedures for data loss prevention are updated at least on a biannual basis to reflect new processes and new requirements.

Status: Resolved

SBA management agreed with the recommendation and will ensure policies and procedures are updated to reflect new processes and requirements. SBA intends to complete final action by September 30, 2024. This recommendation can be closed when SBA management provides documentation that the implementation procedures for data loss prevention have been updated at least biannually.

Recommendation 10

Update existing procedures that identify the roles of individuals with significant IT responsibilities who require role-based training and ensure such training is provided and tracked.

Status: Resolved

SBA management agreed with the recommendation and will update policies and procedures to identify roles with significant IT responsibilities and ensure that those users take role-based training. SBA intends to complete final action by September 30, 2024. This recommendation can be closed when SBA management provides documentation that procedures have been updated to identify roles with significant IT responsibilities and role-based training is provided and tracked.

Recommendation 11

Provide training to individuals with contingency planning roles and responsibilities.

Status: Resolved

SBA management agreed with the recommendation and will provide annual training to individuals with contingency planning responsibilities. SBA will also ensure that this training is tracked accordingly. SBA intends to complete final action by September 30, 2024. This recommendation can be closed when SBA management provides documentation that training has been provided to individuals with contingency planning responsibilities and that this training is tracked.

Appendix 1: Scope and Methodology

Our objectives were to determine whether SBA complied with Federal Information Security Modernization Act (FISMA) in 2023 and assess the maturity of controls used to address risks in each of the nine domains reported to the U.S. Department of Homeland Security's (DHS) CyberScope system, as follows:

1. Risk management
2. Supply chain risk management
3. Configuration management
4. Identity and access management
5. Data protection and privacy
6. Security training
7. Information security continuous monitoring
8. Incident Response
9. Contingency planning

CyberScope is the reporting tool used by DHS to collect FISMA results from across the government.

We hired KPMG LLP, an independent public accounting firm, for our FY 2023 FISMA evaluation. KPMG tested a representative subset of SBA systems and security controls and assessed SBA's adherence to our progress in implementing minimum security standards and requirements appropriate for each system's security categorization and risk.

KPMG also performed vulnerability scanning of SBA's network environment. OIG monitored KPMG's work and reported SBA's compliance with FISMA to DHS's CyberScope application in August 2023.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. These standards require that we adequately plan inspections; present all factual data accurately, fairly, and objectively; and present findings, conclusions, and recommendations in a persuasive manner. We believe the evidence we obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

Maturity Levels

The *FY 2023 Inspector General FISMA Metrics Evaluator's Guide*, updated in April 2023, was developed as a collaborative effort among the Office of Management and Budget, DHS, and the Council of the Inspectors General on Integrity and Efficiency in consultation with the Federal Chief Information Security Officer Council.

The metrics are a continuation of work that began in FY 2016, when the metrics were aligned with the five function areas in the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*: identify, protect, detect, respond, and recover.

Prior Work

OIG reviews information technology security through the annual financial statement audit as well as the annual FISMA evaluation. Our recent reports include the *Independent Auditors' Report on SBA's FY 2022 Financial Statements*, Report 23-02, November 15, 2022; and *FY 2022 Federal Information Security Modernization Act Review*, Report 23-03, December 13, 2022. We also issued *COVID-19 and Disaster Assistance Information Systems Security Controls*, Report 22-19, September 27, 2022.

Appendix 2: Open Recommendations

There are four open audit recommendations that directly affect SBA's CyberScope evaluation as it relates to FISMA compliance. The recommendations below were identified in fiscal years 2022 and 2021 FISMA results and were included in Report 23-03, *Fiscal Year 2022 Federal Information Security Modernization Act Review*, issued December 15, 2022; and Report 22-11, *Fiscal Year 2021 Federal Information Security Modernization Act Review*, issued April 28, 2022.

Risk Management

Identifying information system risk ensures that SBA minimizes vulnerabilities. Risk management includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. Past audits found weaknesses in the agency's risk management. To address these weaknesses, we made this recommendation to SBA.

> OIG Report 23-03, Recommendation 1: Design and implement a quality assurance program to ensure that SBA system software inventory and contractor managed systems are maintained, as required by the National Institute of Standards and Technology (NIST) Special Publication 800-53.

Supply Chain Risk Management

Supply chain risk management includes assessing the risks with the acquisition, maintenance, and disposal of systems as well as assessing risks for external service providers. Past audits found weaknesses in the agency's supply chain risk management. To address these weaknesses, we made this recommendation to SBA.

> OIG Report 23-03, Recommendation 2: Implement a process to ensure SBA reviews its external service providers for supply chain risks and ensure all assessments of supply chain risks are documented as outlined in NIST 800-53.

Identification and Authentication

FISMA requires that organizations identify and authenticate system users and limit system users to the information, functions, and information systems those users are authorized to operate.[5]

[5] Cybersecurity and Infrastructure Security Agency, *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, (February 10, 2023).

Our past audits found weaknesses in SBA's account management. To address this weakness, we made the following recommendation to SBA.

> OIG Report 23-03, Recommendation 3: Communicate and reinforce to program offices the requirement to review and remove system and user accounts in accordance with Standard Operating Procedure 90 47 6.

Information Security Continuous Monitoring

NIST 800-53 requires that organizations monitor and test the controls of its information systems and maintain ongoing awareness of information security, vulnerabilities, and threats. Our past audits found weaknesses in SBA's ongoing authorization process.[6] To address this weakness, we made the following recommendation to SBA.

> OIG Report 23-03, Recommendation 5: Develop, document, and implement a process that requires management review of information security data and report information security threats.

Contingency Planning

NIST 800-53 states that contingency planning for information systems is part of an overall organizational program for achieving continuity for mission or business functions. Our past audits found weaknesses in SBA's test of contingency plans. To address this weakness, we made the following recommendation to SBA.

> OIG Report 22-11, Recommendation 2: Ensure the continuity of operations plan is tested annually, as required by Federal Continuity Directive 1.

[6] NIST, SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, at Control CA-2, Control Assessments (September 2020).

Appendix 3: Assessment Maturity Level Definitions

Inspectors General are required to assess the effectiveness of information security programs on a maturity model spectrum.

Maturity Level	Rating	Definition
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.
Level 3	Consistently implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4	Managed and measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5	Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business or mission needs.

Managed and Measurable, level 4 out of a scale of 5, is considered to be an effective level of security at the domain, function, and overall program level.[7] Ratings throughout the nine domains are calculated based on a simple majority, where the most frequent level across the questions serves as the domain rating.

[7] Cybersecurity and Infrastructure Security Agency, *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, (February 10, 2023).

Appendix 4: Agency Response

U.S. Small Business Administration

Response to Report

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, DC 20416

To: Hannibal “Mike” Ware
Inspector General
U.S. Small Business Administration

From: Stephen Kucharski SK
Chief Information Officer (Acting)

Date: February 8, 2024

Subject: Response to Fiscal Year 2023 Federal Information Security Modernization Act Review Project 23009

We appreciate the Office of Inspector General’s (OIG) role in providing guidance to SBA management to help ensure that our programs are effectively managed, and for the feedback provided in this draft report.

OCIO has procured ServiceNow (SNOW) to handle hardware and software inventories. The software inventory has been implemented and the hardware inventory is underway. OCIO has also, created a dashboard to track Personal Identity Verification (PIV) compliance and effective February 19, 2024, OCIO will heighten the enforcement of its PIV policy by discontinuing the "indefinite unenforced PIV" list.

The Information Security Division has updated the POA&M policy which is currently under OCIO management review.

Recommendation 1 - Complete the implementation of an automated solution to help ensure a complete and accurate inventory of software assets**.**

SBA Response: SBA agrees with this recommendation. ServiceNow (SNOW) is now being used as a repository for software asset management. The associated finding from the previous year was official closed on 9/10/23. Documentation will be provided to support the closure.

Recommendation 2 - Define a required frequency for updating the system inventory and implement a quality control process to validate that system inventories are updated in a timely manner.

SBA Response: SBA agrees with this recommendation. The Office of the Chief Information Officer agrees with the recommendation to implement a quality assurance program to ensure the SBA system hardware inventory remains updated. OCIO is currently implementing ServiceNow (SNOW) to provide compliance automation with updates for the SBA's FISMA systems. The OCIO has a requirement that system owners provide updates on their inventories on a quarterly basis. The new platform will not only validate the system inventory is in alignment with the systems SSP but will pull real time logs from the agency's discovery tool and provide reports on rogue system increasing the agency continuous compliance monitoring capability.

Recommendation 3 - Update existing policy and procedures to ensure plans of action and milestones are closed only after the planned corrective actions and milestones have been implemented.

SBA Response: SBA agrees with this recommendation. OCIO will update the Agency's POA&M policy to ensure corrective actions are met prior to closure of POA&M. Also, procedures will be produced for SOs and ISSOs to meet requirements in updated POA&M policy.

Recommendation 4 - Review the Enterprise Risk Management Framework Guide annually and update if needed.

SBA Response: SBA agrees with this recommendation. SBA has reviewed and updated the Enterprise Risk Management (ERM) Framework Guide since last reported. SBA will continue to review it annually and update it as needed. The Document Revision History section (Appendix D) has been added to the Guide to better monitor and manage this process.

Recommendation 5 - Develop a strategy to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements.

SBA Response: SBA agrees with this recommendation. The Small Business Administration Acquisition Program owned by Office of Performance, Planning, and the Chief Financial Officer (OPP/CFO) and Office of Financial Operations and Acquisition Management (OFOAM) contain Cybersecurity and Supply Chain Risk for IT Acquisitions. OCIO has recently updated the Cybersecurity and Supply Chain Risk for IT Acquisitions and we will work with OPP/CFO and OFOAM to update their existing policy with the new language.

Recommendation 6 - Define timeframe and remediation requirements for baseline and configuration weaknesses.

SBA Response: SBA agrees with this recommendation. OCIO will review and update current processes and procedures defining the timeframe remediate baseline and configuration deviations not covered by an Acceptance of Risk/approved system deviation list.

Recommendation 7- Properly update and remediate vulnerabilities and configuration weaknesses throughout the SBA environment.

SBA Response: SBA agrees with this recommendation. OCIO will work with Agency system owners and ISSOs to ensure system vulnerabilities and configuration weakness are remediate in accordance with Agency policy.

Recommendation 8- Implement a process to track and enforce compliance with PIV implementation and multi-factor requirements.

SBA Response: SBA agrees with this recommendation. OCIO will establish procedures for monitoring PIV compliance including establishing a waiver process for employees who cannot utilize PIV ensuring compliance for MFA and are categorized as exempt.

Recommendation 9- Ensure the Implementation Procedures for Data Loss Prevention is updated at least on a biannual basis to reflect new processes and new requirements.

SBA Response: SBA agrees with this recommendation. OCIO will ensure policy and procedures are updated to meet frequency requirements ensuring new processes and requirements are met.

Recommendation 10- Update existing procedures that identify the roles of individuals with significant IT responsibilities who require role-based training and ensure such training is provided and tracked.

SBA Response: SBA agrees with this recommendation. OCIO will update policy and procedures are to identify roles with significant IT responsibilities and their requirement to take role-based training. The Information Security Division will track and monitor role-based training results to ensure compliance is met.

Recommendation 11- Provide training to individuals with contingency planning roles and responsibilities.

SBA Response: SBA agrees with this recommendation. OCIO will provide annual contingency planning training to individuals with contingency roles and responsibilities. The Information Security Division will track and monitor role-based training results to ensure compliance is met.