

U.S. SMALL BUSINESS ADMINISTRATION

OFFICE OF INSPECTOR GENERAL

# **Fiscal Year 2024 Federal Information Security Modernization Act**



**Evaluation Report**

**Report 25-13**

**April 29, 2025**



### **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 can 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](mailto: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 2024 Federal Information Security Modernization Act (Report 25-13)

---

#### What OIG Reviewed

This report summarizes the results of our fiscal year (FY) 2024 Federal Information Security Modernization Act (FISMA) evaluation and assessment of the U.S. Small Business Administration's (SBA) information security program.

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

The Office of Inspector General (OIG) contracted with 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 1 to 3 are below the baseline for an effective security program.

#### What OIG Found

We found SBA generally responded to previously identified vulnerabilities and made progress in one of the nine domains, in the area of security training. 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: consistently implemented (improved from the 2023 score)
- Information security continuous monitoring: consistently implemented
- Contingency planning: defined

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

#### What OIG Recommended

This FY there are seven new recommendations for improvement. There are 11 open recommendations from 3 prior evaluations (see Appendix 2). Repeat recommendations from prior FYs were not included in this report because they have not yet been implemented. The agency successfully closed four recommendations from FY 2023.

#### Agency Response

SBA managers agreed with six recommendations and partially agreed with one. Their corrective actions resolved all the recommendations. Management plans to implement a software tool to inventory hardware and software assets, provide anti-counterfeit training, establish policies and procedures to detect counterfeit components and devices, and ensure that all users receive cybersecurity awareness training in a timely manner.




**OFFICE OF INSPECTOR GENERAL  
U.S. SMALL BUSINESS ADMINISTRATION**

**MEMORANDUM**

---

**Date:** April 29, 2025

**To:** Kelly Loeffler  
Administrator

**From:** Sheldon Shoemaker  
Deputy Inspector General 

**Subject:** Evaluation of Fiscal Year 2024 Federal Information Security Modernization Act  
(Report 25-13)

This report summarizes the results of our fiscal year (FY) 2024 Federal Information Security Modernization Act (FISMA) evaluation and assessment of the U.S. Small Business Administration's (SBA) information security program. In this report we made seven recommendations for improvements in the areas of inventory management, external service provider risk management, vulnerability remediation, incident response management, and cybersecurity awareness training.

We considered management's comments on the draft of this report when preparing the final report. Management agreed with six recommendations and partially agreed with one recommendation. All the recommendations have been resolved.

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: Wesley Coopersmith, Chief of Staff, Office of the Administrator  
Ben Grayson, Deputy Chief of Staff, Office of the Administrator  
Robin Wright, Chief Operating Officer, Office of the Administrator  
Wendell Davis, General Counsel, Office of General Counsel  
Douglas Robertson, Acting Chief Information Officer, Office of the Chief  
Information Officer  
Nathan Davis, Chief Financial Officer and Chief Risk Officer, Office of  
Performance, Planning, and the Chief Financial Officer  
Deborah Chen, Deputy Chief Financial Officer, Office of Performance, Planning, and the  
Chief Financial Officer  
Michael Simmons, Attorney Advisor, Office of General Counsel

# Contents

---

Introduction .....	1
Background .....	1
Objective .....	3
Results .....	3
Challenges and Improvements .....	5
Improvements .....	5
Challenges .....	5
Domain Test Results .....	5
Finding 1: Risk Management .....	5
Hardware and Software System Inventory .....	6
Recommendation .....	6
Finding 2: Supply Chain Risk Management .....	6
Review of Service Providers' Supply Chain Risks .....	7
Recommendations .....	8
Finding 3: Configuration Management .....	8
Vulnerability Remediation Process .....	8
Recommendation .....	9
Finding 4: Identity and Access Management .....	9
Multi-factor Authentication for Non-privileged Users .....	10
Finding 5: Incident Response .....	10
Incident Response Documentation .....	11
Recommendation .....	11
Finding 6: Security Training .....	11
Cybersecurity Awareness Training .....	11
Recommendations .....	12

Finding 7: Contingency Planning .....	12
Continuity of Operations Plan Testing.....	12
Evaluation of Agency Response.....	13
Summary of Actions Necessary to Close the Recommendations.....	13

## Figures

1: How Security Ratings are Determined .....	2
2: Domain Ratings for FYs 2024 and 2023.....	4

## Appendices

1: Scope and Methodology .....	1-1
2: Open Recommendations.....	2-1
3: Assessment Maturity Level Definitions .....	3-1
4: Agency Response.....	4-1

# 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.<sup>1</sup>

This report summarizes the results of our fiscal year (FY) 2024 evaluation of the U.S. Small Business Administration's (SBA) information security program. 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 an independent public accounting firm for our FY 2024 FISMA evaluation. It tested a subset of SBA information technology (IT) 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 the independent public accounting firm's work and reported SBA's compliance with the Act through the FISMA CyberScope submission in July 2024.

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, 2023, and 2024. These changes are intended to rate an agency in certain high-risk areas, improve the quality of performance data collected across the agency, accelerate their efforts to make more informed risk-based decisions, and achieve observable security outcomes.

## Background

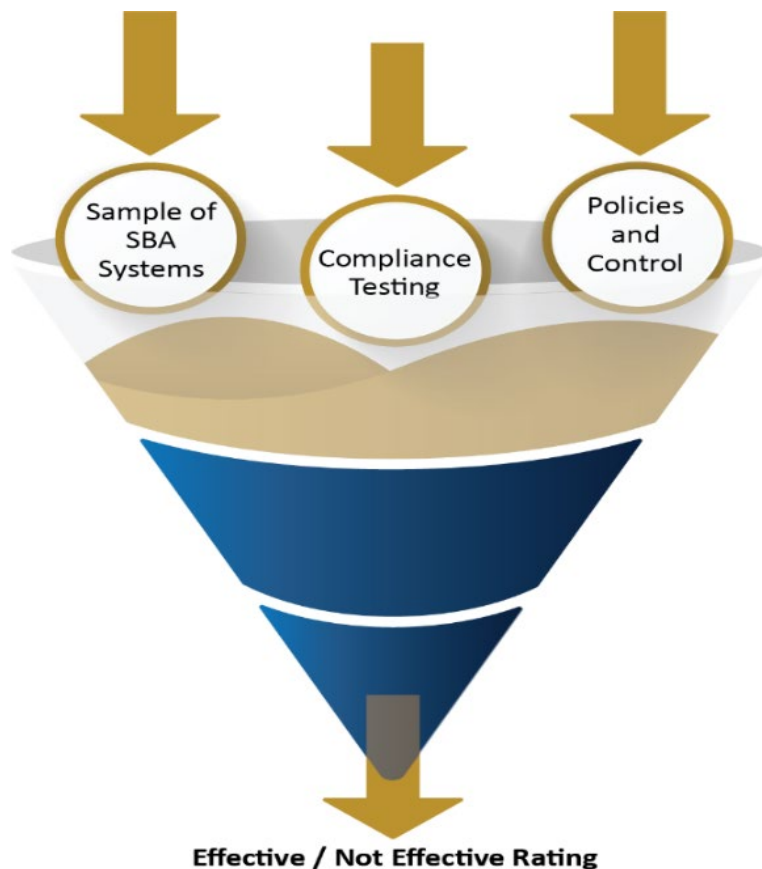
We assessed effectiveness of the following nine domains, which are the required FISMA review areas:

---

<sup>1</sup> 44 U.S. Code § 3555.

- 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

**Figure 1: How Security Ratings are Determined**



Source: OIG generated from SBA data

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 rating and a corresponding label (e.g., defined, consistently implemented, etc.) 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. For FY 2024 the FISMA metrics are a core set of 20 questions with an additional 17 supplemental questions.

Compliance tests are derived from the FISMA metrics. These tests are applied to a subset of SBA



IT 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.

The independent public accountant sampled and tested a representative subset of seven SBA IT systems. The maturity model uses scores, or levels, 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, the average score must be at least a 3.5.

## **Objective**

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**

---

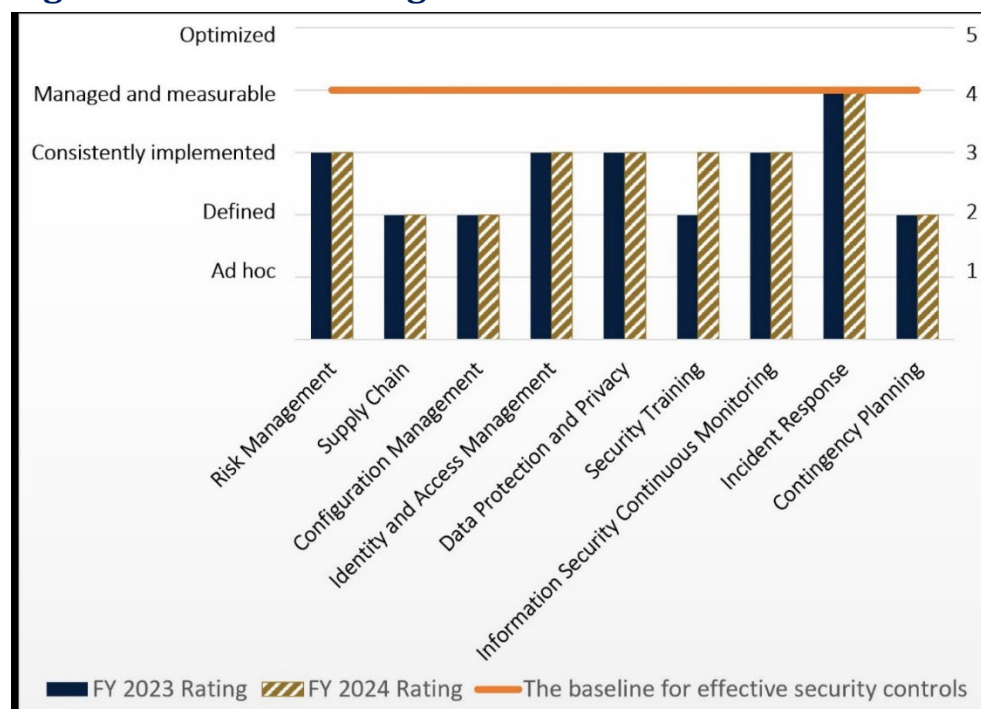
The evaluation of core metrics across the nine domains indicated SBA continued to achieve a rating of 4, managed and measurable, in incident response. SBA was rated as either 2, defined, or 3, consistently implemented, in the remaining eight domains. We rated SBA's overall cybersecurity as "not effective"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

If a domain area required improvement, we determined the effect of deficiencies and whether a recommendation was needed. Our 2024 evaluation showed that the domain scores were similar to those identified in our 2023 evaluation (see Figure 2).

Using the criteria in federal guidance, outlined in Appendix 1, we ranked and illustrated 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: consistently implemented
- Information security continuous monitoring: consistently implemented
- Incident response: managed and measurable
- Contingency planning: defined

**Figure 2: Domain Ratings for FYs 2024 and 2023**



Source: OIG generated from CyberScope results

Open recommendations from previous evaluations in supply chain risk management, configuration management, identity and access management, data protection and privacy, security training, and contingency planning are not repeated in this report (see Appendix 2).

# Challenges and Improvements

## Improvements

We found the agency's incident response continued to be rated as effective. The agency also made progress in the security training domain, although the rating remains below the baseline for an effective security program.

## Challenges

SBA maintained the same maturity level for eight of the nine domains from the previous fiscal year. SBA continues to experience security control challenges in areas of risk management, supply chain risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, and contingency planning.

## Domain Test Results

The agency's information security program is evaluated based on the 37 questions in the *FY 2023-2024 Inspector General FISMA Reporting Metrics* (metrics). The metrics are OMB's guidance for implementing the FISMA requirements. An example of a metric question in the guidance is "To what extent does the organization maintain a comprehensive and accurate inventory of its information systems?" Ratings in each of the nine domains are a calculated average of all the metric questions in that domain. As a result, although a domain average may be a 3, 4, or 5, if any of the metric questions within that domain were scored a 1, ad hoc, or 2, defined, it was considered a finding.

## 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 a 3, consistently implemented, out of a possible 5 (see Appendix 3). SBA management can improve information security in this domain by resolving the following vulnerabilities:

## Hardware and Software System Inventory

An updated listing of hardware and software assets with information necessary for tracking, reporting, and approving inventory was not consistently maintained by SBA management as required by the SBA Office of the Chief Information Officer. SBA management stated an automated IT asset inventory management tool was not completed this year as intended because of the complexity involved in deploying it. Inventory management is needed to provide oversight and visibility to all systems because hardware assets, such as servers, are vulnerable to internal and external threats or attacks. Inventory management is also necessary to maintain the latest security settings and prevent unauthorized software from being installed. Without a fully established process in place, SBA may not be able to assess and manage cybersecurity risks or vulnerabilities in its hardware and software assets.

The *FY 2024 Inspector General FISMA Metrics Evaluator's Guide* states having an agency-wide hardware and software asset management capability in place is considered an effective level of security.<sup>2</sup> FISMA requires agencies to maintain a comprehensive and accurate inventory of their information systems that includes third-party systems. In addition, hardware and software assets are a part of the agency's continuous monitoring processes.

## Recommendation

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

**Recommendation 1:** Complete the implementation of a software tool to help ensure a complete and accurate inventory of software and hardware assets that includes the detailed information necessary for tracking, reporting, and approval.

## Finding 2: Supply Chain Risk Management

Supply chain risk management is a process used to manage cyber risk vulnerabilities from the supplier or the supplied products and services. We determined that SBA's supply chain risk management maturity level scored a 2, so it is defined (see Appendix 3).

---

<sup>2</sup> Cybersecurity and Infrastructure Security Agency, *FY 2024 Inspector General Federal Information Security Modernization Act of 2014 Metrics Evaluator's Guide*, Version 4.0 (April 30, 2024).

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

## **Review of Service Providers' Supply Chain Risks**

While SBA has policies and procedures to review supply chain related risks, our evaluation found the agency was unable to show it reviewed documents (e.g., personnel screening and security) that ensured supply chain risk management was continuously monitored as required by SBA standard operating procedure. This was not done because 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. Not reviewing required documentation for systems hosted by third parties increases the risk that the agency is unaware of the risks within the system's infrastructure, which could affect the agency's ability to make effective risk-based decisions.

The *FY 2024 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.

## **Anti-Counterfeit Components and Training**

Efforts to prevent or detect counterfeit components (e.g., data, documentation, system components) into SBA owned and managed IT environments were not required in SBA procedures. In addition, SBA managers had not designed or implemented a process to provide anti-counterfeit training to personnel. A counterfeit component is an unauthorized copy that has been identified, marked, and/or altered to look like the original.

SBA managers indicated this occurred because they relied on contractual language that required their vendors to implement procedures to verify that the supplies procured by SBA were not counterfeit. However, it is SBA's responsibility to design and implement procedures to prevent counterfeit components, in accordance with the National Institute of Standards and Technology (NIST).<sup>3</sup> It states federal agencies should develop and implement anti-counterfeit policies and procedures that include the means to detect and prevent counterfeit components from entering the system and to train personnel to detect counterfeit system components. Unclear procedures

---

<sup>3</sup> NIST, SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, at Control SR-11 (September 2020).

and undertrained personnel increase the likelihood counterfeit components could be introduced into the IT environment, which could result in the compromise of systems and data.

The *FY 2024 Inspector General FISMA Metrics Evaluator's Guide* states that for an effective level of security, the organization should monitor, analyze, and report on the qualitative and quantitative performance measures it uses to gauge the effectiveness of its policies and procedures to prevent counterfeit components. An agency that effectively handles counterfeit devices and programs also incorporates component authenticity controls into its continuous monitoring practices.

## Recommendations

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

**Recommendation 2:** Perform assessments and analysis of contractor systems to ascertain compliance with SBA's security policies and federal requirements. This includes development of procedures to obtain sufficient assurance through inspection of vulnerability assessment results, audits, test results, or other forms of evaluation to ensure the security and supply chain controls of systems or services provided is captured.

**Recommendation 3:** Establish policies and procedures for detecting counterfeit components and devices, including what risks to consider and what controls may be appropriate to mitigate those risks in SBA's supply chain. This includes the design, development, and implementation of counterfeit training requirements and configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service.

## Finding 3: Configuration Management

Configuration management focuses on the security and integrity of IT products and information systems as they change. We determined the agency's configuration management maturity level scored a 2 out of a possible 5, so it is defined (see Appendix 3). This domain can be improved through resolution of the following vulnerabilities:

### Vulnerability Remediation Process

SBA's existing vulnerability procedures prioritize criticality, timeliness, and communication to remediate issues. However, our evaluation identified unresolved vulnerabilities and

noncompliance with configuration settings for high-value asset systems as required by OMB<sup>4</sup> and SBA procedures.

Unauthorized access, disruption, or destruction to high-value assets, which are mission-critical information systems and data, could cause a significant adverse effect on agency operations. Weaknesses were not addressed because managers did not follow SBA procedures to enforce compliance with patching requirements.

The *FY 2024 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. There is an increased risk that data on the information systems will be compromised if SBA does not make prompt security updates. There also is an increased risk that existing or new vulnerabilities could expose information systems and applications to attacks, unauthorized modification, or compromised data.

Two recommendations for this finding were previously identified in OIG Report 24-07, *FY 2023 Federal Information Security Modernization Act*, and have not been closed by the agency (see Appendix 2). We also made the following recommendation to address this finding.

## Recommendation

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

**Recommendation 4:** Properly update and remediate configuration management vulnerabilities and weaknesses as specified in SBA's procedures.

## 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 IT resources. We determined that the agency's maturity level was consistently implemented, a score of 3 out of a possible 5 (see Appendix 3). This domain can be improved by resolving the following vulnerability:

---

<sup>4</sup> OMB, Memoranda 02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones" (October 17, 2001).

## Multi-factor Authentication for Non-privileged Users

SBA managers ensured that their policies and procedures for managing and reviewing privileged users were consistently implemented. A privileged user is authorized to perform security-relevant functions that ordinary users are not authorized to perform. However, we found multi-factor authentication for non-privileged users was not consistently enforced across the network as required by OMB.<sup>5</sup> A non-privileged user is part of the general user population and does not have special access privileges, such as the ability to change a user's password. However, SBA managers ensured that their policies and procedures for managing and reviewing privileged users were consistently implemented. A privileged user is authorized to perform security-relevant functions that ordinary users are not authorized to perform.

SBA non-privileged network accounts were missing a personal identity verification (PIV) card to authenticate users into the network. A PIV card is one way an organization can use multi-factor authentication to confirm user identity to the network. SBA managers stated implementing multi-factor authentication requirements across the agency was more challenging than initially anticipated. As of July 2024, SBA was still working to transition all employees and contractors onto PIV card access but had not yet completed the initiative.

The *FY 2024 Inspector General FISMA Metrics Evaluator's Guide* states non-privileged users who use strong authentication to access systems and facilities is considered an effective level of security. There is a greater risk of unauthorized access to SBA's systems when solely relying on usernames and passwords. The recommendation for this finding was previously identified in OIG Report 24-07 and has not been closed by the agency, so there is no recommendation for this finding in this report.

## Finding 5: Incident Response

The incident response domain requires implementation of policies and procedures to rapidly detect incidents, minimize loss and destruction, mitigate exploited weaknesses, and restore IT services. Although there was one finding in this domain, we determined that the agency's maturity level was managed and measurable, which is a score of 4 out of a possible 5 (see Appendix 3). This domain can be improved by resolving the following vulnerability:

---

<sup>5</sup> OMB, Memoranda 19-17, "Enabling Mission Delivery through Improved Identity, Credential, and Access Management" (May 21, 2019).



## Incident Response Documentation

Although SBA managers have incident response procedures, they insufficiently documented an incident involving a potential breach of personally identifiable information as required by SBA's incident response procedures and NIST SP 800-53 guidance. The incident was not fully documented because the current process did not specify analysis and actions should be documented. By not completely documenting the results of suspected incidents, all necessary preventive and remediation measures may not be taken.

The *FY 2024 Inspector General FISMA Metrics Evaluator's Guide* states that using accurate, qualitative, and quantitative performance measures to ensure privacy is considered an effective level of security.

## Recommendation

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

**Recommendation 5:** Update incident response documentation procedures, accounting for all necessary information to be included in the SBA cyber incident form.

## 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 SBA's security training program scored a 3 out of a possible 5 and is labeled consistently implemented (see Appendix 3). This domain can be improved by resolving the following vulnerability:

### Cybersecurity Awareness Training

SBA managers implemented an annual cybersecurity awareness training that provides best practices to keep information and systems secure. However, SBA managers inconsistently required and tracked role-based training for individuals with significant IT responsibilities as required by the agency's own policies.

The *FY 2024 Inspector General FISMA Metrics Evaluator's Guide* states an effective level of security is when the agency obtains feedback on its specialized security training content and uses qualitative and quantitative performance measures to gauge its security training program

effectiveness. A recommendation for one of the findings was previously identified in OIG Report 24-07 and has not been closed by the agency (see Appendix 2).

## Recommendations

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

**Recommendation 6:** Update or establish procedures to ensure that all employees and contractors receive security awareness training in a timely manner.

**Recommendation 7:** Develop and implement a process to verify remedial action has occurred if an individual fails to complete the required training within the designated timeframe.

## 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 and scored a 2 out of a possible 5. For a definition of the defined maturity level, see Appendix 3. This domain can be improved by resolving the following vulnerability:

### Continuity of Operations Plan Testing

The Federal Emergency Management Agency states an organization's continuity plan should be reviewed annually and updated as required.<sup>6</sup> The SBA continuity of operations plan was last updated 4 years ago and exercised 3 years ago. SBA managers indicated that the continuity of operations plan was not updated due to competing priorities.

By not updating its plan in a timely manner, SBA could increase risk to its systems. The agency could fail to appropriately identify essential functions and allocate appropriate resources to ensure their continuity. The recommendation for this finding was previously identified in OIG Report 22-11, *FY 2021 Federal Information Security Modernization Act Review*, and has not been closed by the agency (see Appendix 2), so there is no recommendation for this finding in this report. The Office of Executive Management, Installations and Support Services is the agency program office responsible for remediating the finding and implementing the recommendation.

---

<sup>6</sup> Federal Emergency Management Agency, *Federal Continuity Directive 1 Federal Executive Branch National Continuity Program and Requirements*, at A-1 (January 17, 2017).

The *FY 2024 Inspector General FISMA Metrics Evaluator's Guide* states an effective level of security is when the organization ensures that the results of organizational and system level business impact assessments are integrated with enterprise risk management processes.

## Evaluation of Agency Response

---

Management provided written comments that are included in Appendix 2. Additionally, management responded to the report in Integrity, SBA's audit management system, which included whether management agreed with the recommendation and the target dates for implementing the corrective actions. Management agreed with Recommendations 1, 2, 3, 4, 6, and 7, and partially agreed with Recommendation 5. Management's planned actions are sufficient to resolve all the Recommendations.

### 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 a software tool to help ensure a complete and accurate inventory of software and hardware assets that includes the detailed information necessary for tracking, reporting, and approval.

**Status:** Resolved

SBA managers agreed with the recommendation, stating that they will upload the most recent system inventories into the system used to maintain the inventory to update and improve the software management review process and procedures. Management stated they plan to implement the corrective action by July 31, 2025.

This recommendation can be closed when management provides evidence that they have captured a complete and accurate inventory of software and hardware assets and includes the detailed information necessary for tracking, reporting, and approval to minimize cybersecurity risks and vulnerabilities in its IT assets even.

## **Recommendation 2**

Perform assessments and analysis of contractor systems to ascertain compliance with SBA's security policies and federal requirements. This includes development of procedures to obtain sufficient assurance through inspection of vulnerability assessment results, audits, test results, or other forms of evaluation to ensure the security and supply chain controls of systems or services provided is captured.

**Status:** Resolved

SBA managers agreed with the recommendation, stating that they will ensure that the updated cybersecurity contract language has been added to the acquisitions standard operating procedures. Also, managers will review supply chain procedures and update to ensure compliance is met with vendors and contractor systems. Agency managers will add the cybersecurity language to the acquisition standard operating procedures and review and update supply chain procedures by June 30, 2025.

This recommendation can be closed when management provides evidence that they implemented the acquisition standard operating procedures to monitor security controls of contractor systems by reviewing documents on a regular basis to determine if the security controls continue to be effective.

## **Recommendation 3**

Establish policies and procedures for detecting counterfeit components and devices, including what risks to consider and what controls may be appropriate to mitigate those risks in SBA's supply chain. This includes the design, development, and implementation of counterfeit training requirements and configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service.

**Status:** Resolved

SBA managers agreed with the recommendation, stating that they will ensure that the updated cybersecurity contract language has been added to the acquisitions standard operating procedures. Also, managers will review and update procedures to have contracting officer representatives and program officials ensure contractor systems meet compliance requirements. Lastly, managers stated the Office of the Chief Information Officer acquired a new cybersecurity training platform and plan to research providing anti-counterfeit training. Management stated they plan to implement the corrective action by June 30, 2025.

This recommendation can be closed once managers provide evidence they updated and implemented anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system, report counterfeit system components, and train personnel to detect counterfeit system components in accordance with NIST standards.<sup>7</sup>

#### **Recommendation 4**

Properly update and remediate configuration management vulnerabilities and weaknesses as specified in SBA's procedures.

**Status:** Resolved

SBA management agreed with the recommendation, stating that the vulnerability management team will ensure findings are correctly documented. Management will implement this corrective action by June 30, 2025.

This recommendation can be closed once management demonstrates that configuration management vulnerabilities identified during our review were remediated in accordance with SBA procedures. These actions should be completed within the timeframes established for mitigating vulnerabilities depending on the severity of the weakness. Also, management must demonstrate that remediation efforts that exceeded the applicable timeframes were submitted to the SBA's Office of the Chief Information Officer for risk acceptance.<sup>8</sup>

#### **Recommendation 5**

Update incident response documentation procedures, accounting for all necessary information to be included in the SBA cyber incident form.

**Status:** Resolved

Based on management's response in the audit recommendation tracking tool, SBA managers partially agreed with the recommendation, stating that the security operations center must capture prudent information in the security incident report. Management also identified the stakeholders that collaborate to capture and communicate cyber security incidents. Managers are revising the Incident Response Procedures Manual to reflect changes and enhancements. Management plans to revise the procedures and process by June 30, 2025.

---

<sup>7</sup> NIST, SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, at Control SR-11 (September 2020).

<sup>8</sup> SBA, Standard Operating Procedure 90 47 6, Cybersecurity and Privacy Policy (2022).

This recommendation can be closed once management updates their Incident Response Procedures Manual and the security incident report is completed by the security operations center.

#### **Recommendation 6**

Update or establish procedures to ensure that all employees and contractors receive security awareness training in a timely manner.

**Status:** Resolved

SBA managers agreed with the recommendation, stating they will review and update procedures accordingly. Also, SBA managers stated a new cybersecurity training platform will track end user completion status and provide notifications for individuals who require role-based trainings. Managers stated they plan to implement the corrective action by June 30, 2025.

This recommendation can be closed once management updates their standard operating procedures and implements the new cybersecurity training system.

#### **Recommendation 7**

Develop and implement a process to verify remedial action has occurred if an individual fails to complete the required training within the designated timeframe.

**Status:** Resolved

SBA managers agreed with the recommendation, stating they will review and update procedures accordingly. Also, SBA managers stated a new cybersecurity training platform will track end user completion status, provide notification and reminders to users to take the cybersecurity awareness training. SBA managers stated they will develop a way to ensure action was taken for individuals who did not complete the training within the fiscal year. Management stated they plan to implement the corrective action by June 30, 2025.

This recommendation can be closed once management updates their standard operating procedures, implements the new cybersecurity training system, and implements a process to ensure action can be taken for users that do not complete the training within the fiscal year.

# Appendix 1: Scope and Methodology

---

Our objectives were to determine whether SBA complied with the Federal Information Security Modernization Act (FISMA) in 2024 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 an independent public accounting firm for our FY 2024 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.

They also performed vulnerability scanning of SBA's network environment. OIG monitored their work and reported SBA's compliance with FISMA to DHS's CyberScope application in July 2024.

## Maturity Levels

The *FY 2024 Inspector General FISMA Metrics Evaluator's Guide*, updated in April 2024, was developed as a collaborative effort among the Office of Management and Budget, DHS, Council of the Inspectors General on Integrity and Efficiency, in consultation with the Federal Chief Information Officers and Chief Information Security Officer councils.

In response to risks that threaten the technology ecosystem which continues to evolve and change at a faster pace each year, the Office of Management and Budget implemented a new

FISMA framework in FY 2022. The framework yielded two distinct groups of metrics: Core and Supplemental.

### **Core Metrics**

There are 20 core metrics. The core metrics are assessed annually and represent a combination of administration priorities, high impact security processes, and essential functions necessary to determine security program effectiveness.

### **Supplemental Metrics**

Supplemental metrics are assessed at least once every 2 years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness. FY 2024 included 17 supplemental metrics.

## **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 2023 Financial Statements*, Report 24-03, November 15, 2023; *FY 2023 Federal Information Security Modernization Act Review*, Report 24-07, March 7, 2024; and *SBA's IT Investment Governance Framework*, Report 24-10, March 29, 2024.



## Appendix 2: Open Recommendations

---

There are 11 open audit recommendations that directly affect SBA's CyberScope evaluation as it relates to FISMA compliance. The recommendations below were identified in FYs 2021, 2022, and 2023. The results were included in Report 24-07, *FY 2023 Federal Information Security Modernization Act Review*, issued March 7, 2024; Report 23-03, *FY 2022 Federal Information Security Modernization Act Review*, issued December 15, 2022; and Report 22-11, *FY 2021 Federal Information Security Modernization Act Review*, issued April 28, 2022.

### Supply Chain Risk Management

Supply chain risk management is a process used to manage cyber risk vulnerabilities from the supplier or the supplied products and services. Past audits found weaknesses in the agency's area of supply chain risk management. To address these weaknesses, we made the following recommendations 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 National Institute of Standards and Technology (NIST) 800-53.

OIG Report 24-07, 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 as outlined by the SECURE Technology Act.

### Configuration Management

Configuration management focuses on the security and integrity of IT products and information systems as they change. Past audits found weaknesses in the agency's area of configuration management. To address these weaknesses, we made these recommendations to SBA.

OIG Report 24-07, Recommendation 6: Define timeframe and remediation requirements for baseline and configuration weaknesses as outlined in NIST 800-53.

OIG Report 24-07, Recommendation 7: Properly update and remediate vulnerabilities and configuration weaknesses throughout the SBA environment as required by SBA Standard Operating Procedure.

## **Identity and Access Management**

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.<sup>9</sup> Our past audits found weaknesses in SBA’s user management. To address this weakness, we made the following recommendations 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 SBA’s Standard Operating Procedure.

OIG Report 24-07, Recommendation 8: Implement a process to track and enforce compliance with personal identity verification implementation and multi-factor requirements as required by Office of Management and Budget Memorandum 19-17, “Enabling Mission Delivery through Improved Identity, Credential, and Access Management.”

## **Data Protection and Privacy**

The data protection and privacy domain require implementation of policies and procedures for the handling of personally identifiable information and data exfiltration. Our past audits found weaknesses in SBA’s data protection and privacy program. To address this weakness, we made the following recommendation to SBA.

OIG Report 24-07, Recommendation 9: Ensure implementation procedures for data loss prevention are updated at least on a biannual basis to reflect new processes and new requirements as outlined in NIST 800-53.

---

<sup>9</sup> Cybersecurity and Infrastructure Security Agency, *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, (February 10, 2023).

## 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. Our past audits found weaknesses in SBA's security training program. To address this weakness, we made the following recommendation to SBA.

OIG Report 24-07, 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 in accordance with NIST 800-53 and SBA's procedures.

## 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.<sup>10</sup> 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 as outlined in NIST 800-53.

## 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 recommendations to SBA.

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

OIG Report 24-07, Recommendation 11: Provide training to individuals with contingency planning roles and responsibilities as outlined by SBA's procedures.

---

<sup>10</sup> NIST, SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, at Control CA-7 (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, a score of 4 out of 5, is considered to be an effective level of security at the domain, function, and overall program level.<sup>11</sup> Ratings in each of the nine domains are a calculated average of all the metric questions in that domain.

---

<sup>11</sup> 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 Draft Report



U.S. SMALL BUSINESS ADMINISTRATION  
WASHINGTON, D.C. 20416

**To:** Sheldon Shoemaker  
Deputy Inspector General

**From:** Douglas Robertson  
Chief Information Officer (Acting)

**Date:** March 18, 2025

**Subject:** Response to Fiscal Year 2024 Federal Information Security Modernization Act  
Review Project

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 ArchAngel which is our new cybersecurity and compliance management platform which improves operational efficiency, enhancing user experience, and strengthening our cybersecurity posture. Also, OCIO has procured KnowBe4 a new platform for Cyber Security Awareness Training (CSAT) and is comprised of KnowBe4 Security Awareness Training (KMSAT) and Anti-Phishing & Phishing Incident Response Management (PhishER+).

**Recommendation 1** - Complete the implementation of a software tool to help ensure a complete and accurate inventory of software and hardware assets that includes the detailed information necessary for tracking, reporting, and approval.

**SBA Response** - The P&C team will work with the SO/ISSOs and SNOW team to get the most recent system inventories uploaded into the SNOW. We will coordinate with the CMDB developers and provide requirements to ingest the inventories into SNOW for automation. P&C will work with the SAM and SNOW teams to update and improve the software management review process and procedures.

**Recommendation 2** - Perform assessments and analysis of contractor systems to ascertain compliance with SBA's security policies and federal requirements. This includes development of procedures to obtain sufficient assurance through inspection of vulnerability assessment results, audits, test results, or other forms of evaluation to ensure the security and supply chain controls of systems or services provided is captured.

**SBA Response** - The ISD P&C team will ensure that the updated Cybersecurity Contract Language has been added to the Acquisitions SOP. Also, P&C will review supply chain procedures and update to ensure compliance is met with vendors/contractor systems through CORs/SOs/ISSOs.

**Recommendation 3** - Establish policies and procedures for detecting counterfeit components and

devices, including what risks to consider and what controls may be appropriate to mitigate those risks in SBA's supply chain. This includes the design, development, and implementation of counterfeit training requirements and configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service.

**SBA Response** - The ISD P&C team will ensure that the updated Cybersecurity Contract Language has been added to the Acquisitions SOP. Also, P&C will review supply chain procedures and update to ensure compliance is met with vendors/contractor systems through CORs/SOs/ISSOs. ISD has acquired a new Cybersecurity Training Platform and will investigate providing Anti-Counterfeit training.

**Recommendation 4** - Properly update and remediate configuration management vulnerabilities and weaknesses as specified in SBA's procedures.

**SBA Response** - The Vulnerability management team will work with SOs/ISSOs to ensure that all findings are documented correctly. This will include properly drafting AoRs for vulnerabilities that fall outside SBA's criticality mitigation timeframes.

**Recommendation 5** - Update incident response documentation procedures, accounting for all necessary information to be included in the SBA cyber incident form.

**SBA Response** - The Security Incident Report has been appended to the process for Security Operations Center to capture prudent information involving the initial reporting of the incident. Playbooks have been revised to include the PII Playbook. Collaborations between Cybersecurity Operations, Cyber Threat Intel – Forensics, Privacy Officer, and stakeholder's communication were via emails, Teams, and telephone communications. SBA OCIO-ISD is working on revising the Incident Response Procedures Manual to reflect changes that were operating in the background, transparent to the process as well as enhancements.

**Recommendation 6** - Update or establish procedures to ensure that all employees and contractors receive security awareness training in a timely manner.

**SBA Response** - The P&C team will review current procedures and update accordingly. Also, ISD has purchased a new Cybersecurity Training Platform which will track end user completion status and provide notification for individuals who require role-based trainings.

**Recommendation 7** - Develop and implement a process to verify remedial action has occurred if an individual fails to complete the required training within the designated timeframe.

**SBA Response** - The P&C team will review current procedures and update accordingly. Also, ISD has purchased a new Cybersecurity Training Platform which will track end user completion status and provide notification and reminders to take training. ISD will develop a way to track compliance to ensure action was taken for individuals who did not complete the training within the fiscal year.

Douglas Robertson

Chief Information Officer (Acting)