U.S. SMALL BUSINESS ADMINISTRATION OFFICE OF INSPECTOR GENERAL

Fiscal Year 2025 Federal Information Security Modernization Act

Evaluation Report

Report 26-10

May 19, 2026

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 USC §§ 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.

EXECUTIVE SUMMARY

Fiscal Year 2025 Federal Information Security Modernization Act (Report 26-10)

What OIG Reviewed

This report summarizes the results of our fiscal year (FY) 2025 Federal Information Security Modernization Act (FISMA) evaluation of the U.S. Small Business Administration's (SBA) information security program, which represents a point-in-time assessment of conditions observed during the review.

Our objective was to determine the effectiveness of SBA's information security program and practices. The Office of Inspector General (OIG) contracted with an independent public accounting firm of auditors to assess SBA's adherence to FISMA requirements. The auditors used federal guidance issued by the Office of Management and Budget (OMB) to evaluate the agency's security controls and test a subset of systems for compliance with the requirements.

The guidance requires OIGs to use a 5-level maturity model to determine if domains, a defined area under specific control, were ad hoc, 1; defined, 2; consistently implemented, 3; managed and measurable, 4; or optimized, 5. Per OMB, a rating of managed and measurable (4) is the baseline for effective security controls. A rating of optimized (5) is above the baseline. Ratings of ad hoc, defined, and consistently implemented (1-3) are below the baseline.

What OIG Found

The auditors found SBA made progress in 1 of the 10 domains. The incident response domain was rated as optimized, exceeding the baseline for effective security controls. SBA regressed in three domains: information security and continuous monitoring, identity and access management, and risk and asset management.

Ultimately, the agency fell below the baseline for effective controls in 9 of the 10 domains. Specifically, the following three domains were rated as consistently implemented (3):

- Cybersecurity governance,
- Data protection and privacy
- Security training

The remaining six domains were rated as defined (2):

- Cybersecurity supply chain risk management,
- Risk and asset management,
- Configuration management,
- Identity and access management,
- Contingency planning,
- Information security continuous monitoring

Therefore, SBA's overall information security program has defined policies but it has not consistently implemented them, falling short of the OMB rating for effective security controls.

What OIG Recommended

There are 17 new recommendations to improve SBA's IT security program. Additionally, the agency continues to make progress on implementing 13 open recommendations from 4 prior evaluations (see Appendix 2).

Agency Response

SBA managers agreed and proposed corrective actions that resolved all 17 recommendations. Management plans to use software tools to complete security control assessments and automate risk management, establish or update policies and procedures where necessary, and centralize processes, among other improvements.

Contents

Tables

Figures

Appendices

Introduction

The Federal Information Security Modernization Act (FISMA) of 2014 requires agencies to protect information and information systems from unauthorized access, use, destruction, or disruption at a level that makes sense for the amount of risk and possible damage. 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). The Act requires each office of inspector general, or an independent external auditor as determined by the inspector general, to independently evaluate the effectiveness of the information security program and practices of its agency.[1]

The Office of Inspector General (OIG) contracted with an independent public accounting firm of auditors for the fiscal year (FY) 2025 FISMA evaluation. The auditors tested the design and effectiveness of the agency's information security policies, procedures, and practices for a subset of its information systems. OIG monitored the auditor's work and reported SBA's progress toward achieving objectives in the FISMA CyberScope system in August 2025.

Background

The Office of Management and Budget (OMB), in coordination with the Council of the Inspectors General on Integrity and Efficiency (CIGIE), the Federal Chief Information Officer Council, the Federal Chief Information Security Officer Council, among other stakeholders, established metrics categorized under 10 domains to assess the effectiveness of an agency's information security program (see Appendix 3). The FY 2025 FISMA metrics consist of a set of 20 core questions that are evaluated every year and 5 supplemental questions that are evaluated on a 2-year cycle.[2]

OMB requires offices of inspector general to score the effectiveness of the controls using a maturity model. The maturity model uses ratings of 1 (very basic) to 5 (highly effective) to show if an area was ad hoc, 1; defined, 2; consistently implemented, 3; managed and measurable, 4; or optimized, 5 (see Table 1 for definitions of the ratings). A rating of managed and measurable (4) describes security controls that are effective, so this is the baseline for an effective security controls system. A rating of optimized (5) is above the baseline. Ratings of ad hoc, defined, and consistently implemented (1-3) are below the baseline for effective security controls.

[1] 44 U.S. Code § 3555.
[2] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (April 3, 2025).

Table 1: FISMA Maturity Levels

Maturity Levels	Policies, Procedures, and Strategies:
Level 1: Ad-hoc	Are not formalized, Are performed in an ad-hoc or reactive manner.
Level 2: Defined	Are formalized and documented but not consistently implemented.
Level 3: Consistently implemented	Are consistently implemented but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and measurable	Are assessed and refined using quantitative and qualitative measures collected across the organization.
Level 5: Optimized	Are fully institutionalized, repeatable, and self-generating, Are regularly updated based on a changing threat, the technology landscape, and agency mission needs.

Source: OIG generated based on OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, v2.0* (April 3, 2025)

Ratings in the 10 domains were determined by a calculated average across all metrics in that domain. For example, to maintain a rating of managed and measurable in a domain, the average score of all the corresponding questions must be at least a 3.5. Any metrics within a domain that scored 1 or 2 were classified as findings, even if the domain's overall average score was 3, 4, or 5.

The auditors used the 25 metrics to assess SBA's progress in achieving effective controls within the 10 domains. They performed test procedures for each of the metric questions and rated the maturity level for each metric based on the results.

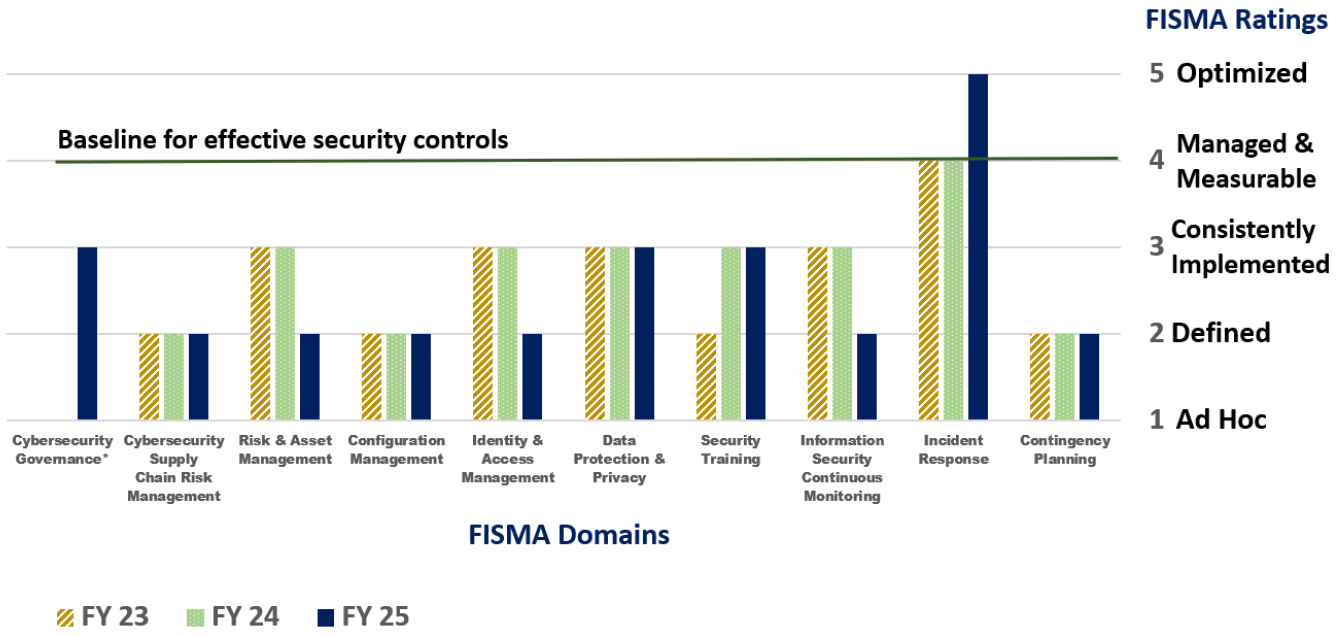
Objective

The objective was to determine the effectiveness of SBA's information security program and practices.

Results

SBA continued to improve in the area of incident response to achieve an optimized rating of 5. This means the agency's incident response policies, procedures, and strategies were fully institutionalized, repeatable, and are regularly updated based on changing threats, the technology landscape, and agency mission needs. SBA was rated as either 2, defined, or 3, consistently implemented, in the remaining nine areas, which is below the baseline for effective security controls (see Figure 1).

Figure 1: Maturity Ratings by Domain for FYs 2023-2025



*Cybersecurity Governance was added in FY 2025 and has no comparative ratings from prior years.

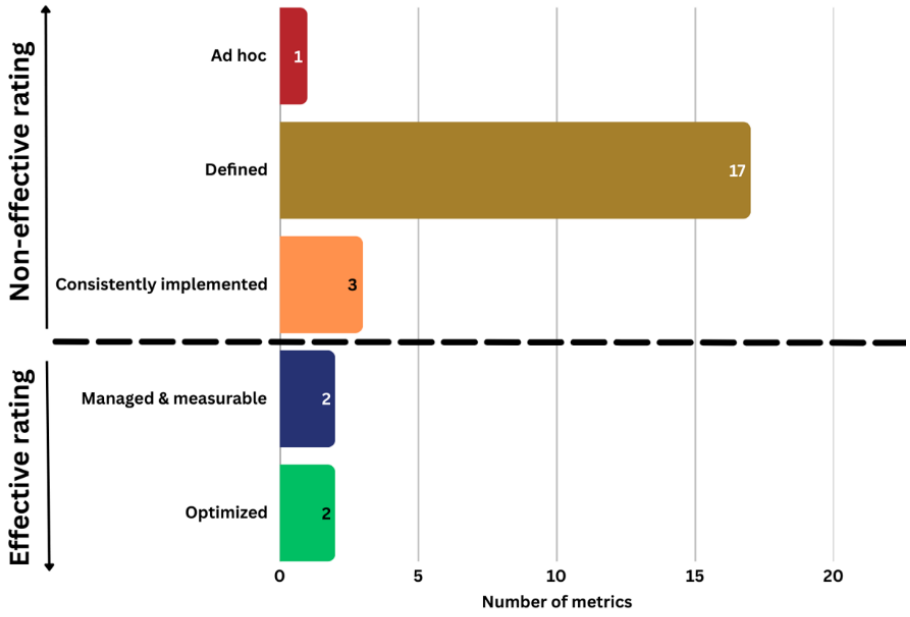
Source: OIG generated from CyberScope results

In comparison to FY 2024, SBA progressed in incident response and sustained consistently implemented ratings in security training and data protection and privacy. But SBA dropped its ratings in three areas: 1) information security and continuous monitoring, 2) identity and access management, and 3) risk and asset management. The cybersecurity governance domain was added in FY 2025 so it has no ratings from previous years.

The auditors determined that 18 metrics were rated as a maturity level of ad hoc or defined, which means the agency's policies, procedures, and strategies were far below the baseline for effectiveness (see Figure 2). Those metrics were reported as findings and the auditors and OIG

jointly made recommendations for SBA to improve these controls. Therefore, SBA's overall information security program has defined policies, but it has not consistently implemented them, falling short of the OMB rating for effective security controls.

Figure 2: The Metrics and How They Were Rated



Source: OIG generated from CyberScope results

Finding 1: Cybersecurity Governance

New to the FISMA review this year, the cybersecurity governance domain involves an agency-wide strategy that protects operations from cyber threats to reduce interruptions to deliver on SBA's mission. Features of cybersecurity governance include accountability frameworks, decision-making hierarchies, defined business objective risks, mitigation plans, and oversight processes and procedures. The auditors determined SBA's cybersecurity governance was consistently implemented, maturity level 3. SBA can improve information security by resolving the following vulnerability:

Internal Security Controls Assessments over Third Parties

Although program officials developed a risk management strategy, established risk management objectives, and lines of communication from suppliers and third parties, they did not fully approve an annual security assessment for two of the seven systems reviewed. Agency procedures require that program officials conduct and sign annual security assessments for all

third-party systems to evaluate the risk and effectiveness of controls needed to protect information systems. Ensuring that the security assessments are conducted and approved by the proper officials provides a record that all stakeholders reviewed risks and implemented acceptable risk mitigation strategies to eliminate or reduce cyber risks, such as identifying unsupported software in order to protect agency systems and data.

SBA did not consistently follow these procedures because program officials discontinued the governance, risk, and compliance system without a replacement. In one instance, one of three required signatures was missing from the security assessment. Also, for one of the two systems that did not have an annual assessment, program officials stated that the system was on a 3-year assessment cycle. However, SBA's procedures require an annual assessment.

According to OMB's guidance, to reach level 3 maturity, the agency should consistently assess and document risks across the organizational, business process, and information system levels, and update its risk management strategy based on these assessments. To progress to level 4 and achieve an effective level of security, the agency should fully integrate its security and privacy risk management into its overall enterprise risk management strategy.[3]

Recommendations

We recommend the Administrator direct the Chief Information Officer to:

Recommendation 1: Complete the implementation of a new governance risk and compliance tool to assist in the timely completion of SBA's annual security control assessments in coordination with the Office of the Chief Financial Officer.

Recommendation 2: Update SBA policy and procedures to clearly define the term "annual" and specify whether it refers to a period of 365 days or aligns with the fiscal year ending on September 30.

We recommend the Administrator direct the Associate Administrator for the Office of Capital Access to:

Recommendation 3: Ensure the agency follows the policy to perform security control assessments annually, either on a rolling 365-day basis or aligned with the fiscal year ending on September 30.

[3] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Metrics Evaluator's Guide*, Version 1.0 (May 5, 2025).

Finding 2: Cybersecurity Supply Chain Risk Management

The cybersecurity supply chain risk management domain covers processes used to manage and develop response strategies to risks, such as inserting malicious software and hardware, from the supplier or the supplied products and services.[4] SBA's policies, procedures, and strategies were formalized and documented but not consistently implemented. The auditors assessed the cybersecurity supply chain risk management domain as defined, maturity level 2. SBA can improve cybersecurity supply chain risk by addressing the following vulnerability:

Review of Service Providers' Supply Chain Risks

While SBA defined and communicated policies and procedures over supply chain related risks, program officials were unable to show they continuously monitored supply chain risks, such as reviewing system vulnerability scans from third-party service providers on a weekly basis. SBA's procedures require the contractor to provide deliverables to the program officials to review in order to continuously monitor the information system for effectiveness. However, the procedures did not explicitly state what evidence should be provided or how the review should be documented. When program officials do not review required third-party system documentation, there is greater chance the agency will be unaware of risks to system infrastructure. This could affect the agency's ability to make effective risk-based decisions.

Program officials stated that going forward, continuous monitoring of third-party supply chain risks will be automated and centralized through the Office of the Chief Information Officer.

The agency can achieve a maturity rating of 3 if its program officials consistently implement procedures to review the supply chain-related risks associated with contractor systems. To achieve a rating of 4, an effective level, the agency will need to incorporate cyber supply chain risks into its continuous monitoring practices.[5]

[4] National Institute of Standards and Technology, SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, at Glossary (September 2020).
[5] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 Metrics Evaluator's Guide,* Version 1.0 (May 5, 2025).

Recommendation

We recommend the Administrator direct the Chief Information Officer to:

Recommendation 4: Update the SBA Standard Operating Procedure (SOP) 20 21 4, The Small Business Administration Acquisition and Procurement Program, January 16, 2025, Appendix C — Cybersecurity and Supply Chain Risk for IT Acquisitions, to reflect the new process in which third-party supply chain risks will be continuously monitored through the Office of the Chief Information Officer.

Finding 3: Risk and Asset Management

Risk and asset management focuses on the integrity of system inventory and hardware, software, and data management. The agency's risk management policies, procedures, and strategies were formalized and documented but not consistently implemented, and the domain was assessed as defined, maturity level 2. This domain can be improved by resolving the following vulnerabilities:

Hardware and Software System Inventory

SBA program officials defined policies, procedures, and processes to develop and maintain an up-to-date inventory of hardware and software assets, such as software licenses. However, program officials did not consistently maintain hardware and software inventories, as required by SBA procedures. Program officials stated they were in the process of transitioning to a different inventory management system, and it was not fully completed at the time of the FISMA review because of the complexity involved in deploying it.

Inventory management is necessary for management to provide oversight and have visibility to all systems within the organization. Without complete inventories program officials may not be able to assess and manage cyber security threats or reduce vulnerabilities in the agency's hardware and software assets.

According to OMB guidance, an effective level of security should include an agency-wide system to track hardware and software.[6] The recommendation for this finding was previously identified in OIG Report 25-13, Recommendation 1 (see Appendix 2). SBA management continues to make progress on implementing an automated system to manage its inventory of software and hardware assets. Therefore, there are no additional recommendations for this vulnerability.

[6] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 Metrics Evaluator's Guide*, Version 1.0 (May 5, 2025).

Data Inventory

SBA has not defined or developed policies, procedures, processes, roles or responsibilities for developing a comprehensive and accurate data inventory, including data and its metadata obtained from third-party providers. Federal law requires agencies to maintain an inventory accounting for all agency data assets and ensure it is both clear and comprehensive.[7] At the time of the review, the auditors found that the effort was underway but due to staff reassignments, it was not completed.

Without policies, procedures, processes, roles and responsibilities for developing and maintaining a data inventory with corresponding metadata, SBA might not be able to address cybersecurity risks. Metadata is information that describes the characteristics of data and is critical to describe, explain, locate, or otherwise make data easier to retrieve, use, or manage and helps ensure proper data management and security. To reach an effective level of security, the agency must maintain a secure data inventory that is monitored within the agency's information security continuous monitoring strategy.[8]

Cybersecurity Risks

Program officials defined and communicated policies, procedures, processes, and requirements to manage cybersecurity risks using an automated solution. However, since December 2024, SBA has lacked an automated solution to track cybersecurity risks across the entire agency, as required by standard operating procedures. Program officials were in the process of implementing an automated system but had to put it on hold when critical issues were identified. This resulted in program officials shifting to manually tracking risks.

In the absence of an automated, agency-wide solution to track cybersecurity risks, SBA's risk-management processes may become inefficient and incomplete. An effective level of security is when the organization ensures that 1) cybersecurity risk registers are accurate and consistently monitored to prioritize operational risk response and 2) cybersecurity risk information is integrated into enterprise risk management reporting tools.[9]

System Interconnections

Several of SBA's interconnection security agreements were either expired or not available for review for one of the agency's key systems. An interconnection security agreement specifies

[7] 44 U.S. Code § 3511.
[8] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 Metrics Evaluator's Guide,* Version 1.0 (May 5, 2025).
[9] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 Metrics Evaluator's Guide*, Version 1.0 (May 5, 2025).

security requirements for connecting an agency to an external system. This occurred because staff who would normally have updated the agreements were reassigned to another task.

Without agreements reviewed and approved by officials at both organizations, the terms of the agreements may not be appropriately implemented to address all security requirements. According to OMB guidance, an effective level of security is achieved when information systems are included in the agency inventory and are subject to the information security continuous monitoring strategy.[10]

Recommendations

We recommend the Administrator direct the Chief Information Officer to:

Recommendation 5: Implement policies, procedures, and processes for developing and maintaining an accurate inventory of data and its corresponding metadata from third parties.

Recommendation 6: Improve the governance, risk, and compliance systems to track cybersecurity risks.

Recommendation 7: Develop and implement a process to monitor program offices' completion of required annual reviews of interconnection security agreements and ensure program officials review and sign the agreements prior to their expiration.

Finding 4: Configuration Management

Configuration management focuses on the integrity of information systems as they change. The auditors determined the agency's configuration management policies, procedures, and strategies were formalized and documented but were not consistently implemented, so this domain was assessed as defined, maturity level 2. This domain can be improved through resolution of the following vulnerability:

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 in four out of seven systems, including a high-value asset system.

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 program officials did not follow agency procedures to

[10] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 Metrics Evaluator's Guide*, Version 1.0 (May 5, 2025).

remediate vulnerabilities. In addition, SBA managers stated that resources were reprioritized to other tasks.

Delays in making security updates increase risks that existing or new vulnerabilities could expose information systems and applications to cyberattacks, unauthorized modification, or compromised data. To obtain a maturity level that is considered effective, the agency should use automation to maintain a complete, accurate, and readily available view of security configurations.[11]

This is a recurring issue and was previously reported in OIG Report 24-07, where we made two recommendations (see Appendix 2, OIG Report 24-07, Recommendations 6 and 7). Management continues to make progress toward remediating vulnerabilities to resolve the recommendations; therefore, there are no additional recommendations for this vulnerability.

Finding 5: 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 the agency had formalized and documented policies and procedures, but they were not consistently implemented. The auditors assessed the identity and access management domain as defined, maturity level 2. Identity and access management can be improved by resolving the following vulnerabilities:

Multi-factor Authentication for Users

The auditors found multi-factor authentication for non-privileged and privileged users was not consistently enforced across the network as required by OMB.[12] 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. A privileged user is an employee or contractor authorized to perform security-relevant functions.

SBA 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. Program officials stated implementing multi-factor authentication requirements across the agency has been more challenging than initially

[11] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 Metrics Evaluator's Guide,* Version 1.0 (May 5, 2025).
[12] OMB, Memoranda 19-17, "Enabling Mission Delivery through Improved Identity, Credential, and Access Management" (May 21, 2019).

anticipated. Despite the challenges, program officials were able to transition a substantial number of users (6,094 of the 6,631 users, nearly 92 percent) onto a PIV card last fiscal year.

In addition, program officials did not define the requirements to approve, track, or manage exempted users. An exempted user is a contractor or employee who accesses the network without a PIV card.

OMB guidance states an effective level of security is achieved when all users are authenticated with multiple factors, such as passwords and PIV cards, before accessing systems and facilities. We identified this issue in a prior report and made a recommendation for management to implement a process to track and enforce compliance with PIV implementation and multi-factor requirements (see Appendix 2, OIG Report 24-07, Recommendation 8). During subsequent testing procedures performed during the audit of SBA's FY 2025 Financial Statements, the auditors determined that SBA management implemented alternative security measures for users without a PIV card. Therefore, we consider the recommendation closed.

User Access

Program officials defined user access processes, such as approving and validating privileged user accounts. However, they did not consistently perform annual user access reviews or approve access prior to granting it for privileged users. In addition, in one circumstance, access for a privileged user was granted before a valid access request was made. Agency procedure states that accounts shall only be created upon receipt of valid access requests, and they must be managed for all IT systems. This occurred because there was not a process to ensure that system administrators understood those requirements.

Granting access without prior approval and inconsistent annual reviews of privileged user accounts weakens access control safeguards and increases the agency's exposure to unauthorized access to and modification of agency data and systems. OMB guidance states for an effective level of security, the organization must use automated mechanisms to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.[13]

Recommendations

We recommend the Administrator direct the Chief Information Officer to:

Recommendation 8: Improve the existing process to manage personal identity verification exemptions.

[13] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 Metrics Evaluator's Guide*, Version 1.0 (May 5, 2025).

Recommendation 9: Ensure that system owners perform annual privileged user access reviews in accordance with SBA policies.

Recommendation 10: Provide system owners and individuals with training or other communication emphasizing requirements for approving privileged user access prior to granting access.

Finding 6: Information Security Continuous Monitoring

Information security continuous monitoring means security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect agency information. The auditors determined that SBA had formalized and documented the policies, procedures, and strategies but did not consistently implement information security continuous monitoring. They assessed this domain as defined, maturity level 2. This area can be improved by resolving the following vulnerability:

System Security Plans

Program officials did not consistently implement controls to perform annual reviews and approvals over system security plans for four of the seven systems that were tested. Agency procedure required that system security plans be reviewed and approved annually by the system owners. Program officials stated staff resources were shifted to competing priorities.

If system security plans are not kept current, they may no longer reflect actual system risks or required security controls. Outdated plans limit the ability of responsible individuals to apply appropriate safeguards or recognize emerging weaknesses. This could lead to increased risks of security breaches, potentially compromising data confidentiality, integrity, or availability. An effective level of security is when the agency develops and maintains system security plans to provide a view of the organization information security condition.[14]

Recommendation

We recommend the Administrator direct the Chief Information Officer to:

Recommendation 11: Ensure program offices review all system security plans and confirm they are updated, approved, and signed annually by the system owner, information systems security officer, and the information systems security manager.

[14] OMB and CIGIE, *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 Metrics Evaluator's Guide*, Version 1.0 (May 5, 2025).

Finding 7: Contingency Planning

Contingency planning is defined as both restoration and implementation of alternative processes when systems are compromised. The auditors determined SBA formalized and documented policies, procedures, and strategy for contingency planning, but they were not consistently implemented. The auditors assessed this domain as defined, maturity level 2. Contingency planning can be improved by resolving the following vulnerabilities:

Overall Agency Continuity of Operations Plan

The Federal Emergency Management Agency (FEMA) states an organization's continuity plan should be reviewed annually and updated as required.[15] The SBA continuity of operations plan was last updated in March 2023 and last exercised in 2021. Program officials explained that they planned to participate in the Department of Homeland Security's continuity of operations plan exercise and update SBA's plan by the end of May 2025. However, documentation to support completion of the exercise and the updated plan were not available prior to the end of this review. Inconsistent documentation and testing of the continuity of operations plan could increase the risk that sensitive and critical data and business functions could become unavailable and negatively affect business operations.

This is a recurring issue and was previously reported in OIG Report 22-11 (see Appendix 2, OIG Report 22-11, Recommendation 2). The Office of Executive Management, Installations, and Support Services is the agency program office responsible for remediating the finding and implementing the recommendation. Management continues to work toward ensuring the continuity of operations plan is tested annually. No additional recommendations for this finding were made.

Information System Contingency Plans

Program officials consistently implemented controls to review, update, and test information system contingency plans for four out of eight IT systems reviewed. For the remaining four systems the auditors noted contingency plans did not exist, or SBA program officials did not review and update the plans annually or perform annual tests (see Table 2).

In addition, a functional test was not performed for one of SBA's three high-value asset systems. High-value asset systems are ones in which unauthorized access could significantly affect the nation's security interests, foreign relations, or economy. An SBA standard operating procedure states high-value asset systems should be tested annually to ensure that failover testing to the

[15] FEMA, *Federal Continuity Directive 1 Federal Executive Branch National Continuity Program and Requirements*, at A-1 (January 17, 2017).

alternative backup site keeps the system operational. Program officials stated an annual test of the high-value asset system was not performed because procedures to support failover testing beyond tabletop exercises were not established. A tabletop exercise is limited to a scenario-based discussion where personnel review and validate the contingency plan by discussing their roles and responses to emergency situations. Whereas a failover test validates the capability to automatically switch to a backup or standby information system upon the failure of the previously active system.

Table 2: SBA Contingency Plan Deficiencies

SBA Systems Tested	Business Impact Analysis	Information System Contingency plan	Annual Test
System 1	✓	×	×
System 2	×	×	×
System 3	✓	×	✓
System 4 — High Value Asset	✓	✓	×

Notes: × means deficient; ✓ means the documentation was sufficient

Federal guidance and agency procedures require that information system contingency plans should be created, reviewed, and tested annually, and include a business impact assessment.[16] The noted system contingency plans were not consistently reviewed, updated, and exercised due to the lack of monitoring and enforcement with requirements.

Without regular contingency plan testing, the agency risks being unable to identify and prioritize restoration of mission-essential systems and data. Consistent testing and integration with related plans, such as the agency continuity of operations plan, are necessary to achieve an effective rating.

Recommendations

We recommend the Administrator direct the Associate Administrator for the Office of Investment and Innovation and the Chief Information Officer to:

Recommendation 12: Document procedures, roles, and responsibilities for performing an annual functional test to ensure that the alternative backup site keeps the system operational in accordance with SBA policy and procedures.

Recommendation 13: Annually perform functional testing to include failover testing in accordance with SBA policy and procedures.

[16] FEMA, *Federal Continuity Directive 1 Federal Executive Branch National Continuity Program and Requirements*, at A-1 (January 17, 2017).

We recommend the Administrator direct the Chief Information Officer to:

Recommendation 14: Establish procedures to monitor program officials' compliance with SOP 90 47 6, Cybersecurity and Privacy Policy, requirements to ensure information system contingency plans are developed, tested annually, and updated as needed.

Recommendation 15: Review and update the information system contingency plans and business impact assessments and ensure that key attributes are included.

We recommend the Administrator direct the Associate Administrator for the Office of Disaster Recovery and Resilience and the Chief Information Officer to:

Recommendation 16: Update the information system contingency plans and business impact assessments at least once a year and include the recovery priority and lessons learned.

We recommend the Administrator direct the Associate Administrator for the offices of Capital Access and the Chief Information Officer to:

Recommendation 17: Conduct the information system contingency plans to include a business impact assessment at least annually.

Evaluation of Agency Response

SBA managers provided formal written comments that are included in their entirety in Appendix 4. The managers agreed with all 17 recommendations and their planned actions are sufficient to resolve the recommendations. SBA managers provided implementation target dates for Recommendations 1-3 and 6. However, for Recommendations 4-5 and 7-17, management did not establish target dates to implement corrective actions. We will meet with management to discuss implementation target dates for monitoring progress on these 13 recommendations in accordance with our audit follow-up procedure.

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 new governance risk and compliance tool to assist in the timely completion of SBA's annual security control assessments in coordination with the Office of the Chief Financial Officer.

Status: Resolved

SBA managers agreed with the recommendation, stating they will implement a centralized, automated platform to identify, assess, and mitigate cybersecurity risks. SBA management also stated the solution will support real-time monitoring, automated assessments, and improved remediation tracking. The managers stated they plan to implement corrective action by June 1, 2026. This recommendation can be closed when SBA provides evidence it has implemented a new governance, risk, and compliance tool that supports the completion of SBA's annual security control assessments in a timely manner to minimize cybersecurity risks and vulnerabilities in its IT assets.

Recommendation 2

Update SBA policy and procedures to clearly define the term "annual" and specify whether it refers to a period of 365 days or aligns with the fiscal year ending on September 30.

Status: Resolved

SBA managers agreed with the recommendation, stating they will update the Cybersecurity and Privacy Policy to define "annual" as aligned with the fiscal year cycle ending September 30. Agency managers will update the policy by June 1, 2026. This recommendation can be closed when SBA provides evidence it updated the Cybersecurity and Privacy Policy.

Recommendation 3

Ensure the agency follows the policy to perform security control assessments annually, either on a rolling 365-day basis or aligned with the fiscal year ending on September 30.

Status: Resolved

SBA management agreed with the recommendation, stating the Office of Capital Access will coordinate with the Office of the Chief Information Officer to ensure all systems under its authority complete annual security control assessments within the defined fiscal year cycle. Additionally, SBA managers stated oversight checkpoints and automated reminders will be integrated into the new governance, risk, and compliance tool. SBA managers stated they plan to implement the corrective action by June 1, 2026.

This recommendation can be closed once SBA provides evidence security control assessments are performed within the fiscal year, in accordance with the updated Cybersecurity and Privacy Policy.

Recommendation 4

Update the SBA Standard Operating Procedure (SOP) 20 21 4, The Small Business Administration Acquisition and Procurement Program, January 16, 2025, Appendix C — Cybersecurity and

Supply Chain Risk for IT Acquisitions, to reflect the new process in which third-party supply chain risks will be continuously monitored through the Office of the Chief Information Officer.

Status: Resolved

SBA managers agreed with the recommendation and stated they documented new procedures in which third-party supply chain risks are continuously monitored through the Office of the Chief Information Officer. Managers stated this will ensure alignment with National Institute of Standards and Technology (NIST) supply chain risk management guidance and SBA's enhanced cybersecurity supply chain risk management framework. In addition, managers stated they developed a cybersecurity supply chain risk management plan and enhanced the quarterly information security continuous monitoring program to include NIST Special Publication 800-53 Rev. 5 supply chain risk management controls. Per management, these updates ensure periodic assessments and documented evidence of contractor monitoring artifacts.

This recommendation can be closed once management provides the documented procedures to reflect the new process in which third-party supply chain risks will be continuously monitored through the Office of the Chief Information Officer.

Recommendation 5

Implement policies, procedures, and processes for developing and maintaining an accurate inventory of data and its corresponding metadata from third parties.

Status: Resolved

SBA managers agreed with the recommendation, stating that SBA developed a data security plan for data labeling and tagging of all assets to maintain an accurate inventory of data and corresponding metadata from third parties. This recommendation can be closed once managers provide evidence they implemented policies, procedures, and processes to develop and maintain an accurate inventory of data and its corresponding metadata from third parties.

Recommendation 6

Improve the governance risk and compliance systems to track cybersecurity risks.

Status: Resolved

SBA managers agreed with the recommendation, stating they will implement a centralized, automated platform to identify, assess, and mitigate cybersecurity risks. Also, SBA managers stated this solution will support real-time monitoring, automated assessments, and improved remediation tracking. They plan to implement the corrective action by June 1, 2026. This recommendation can be closed once management provides evidence that cybersecurity risks can be identified, assessed, tracked and mitigated.

Recommendation 7

Develop and implement a process to monitor program offices' completion of required annual reviews of interconnection security agreements and ensure program officials review and sign the agreements prior to their expiration.

Status: Resolved

SBA managers agreed with the recommendation, stating they enhanced the quarterly information security continuous monitoring program to include NIST 800-53 Rev. 5 controls related to interconnection security agreement oversight, ensuring periodic assessments and timely renewal. This recommendation can be closed once SBA develops and implements processes and procedures to ensure interconnection security agreements are annually completed, reviewed, and signed by the agency program offices.

Recommendation 8

Improve the existing process to manage personal identity verification (PIV) exemptions.

Status: Resolved

SBA managers agreed with the recommendation, stating they updated and defined the PIV card exemption process. Also, management stated exemptions are now limited to new hires for 2 weeks during onboarding, with a maximum extension of 4 weeks upon approval by the Chief Information Security Officer. This recommendation can be closed once management provides evidence that the existing process to manage PIV exemptions has been implemented so multi-factor authentication is consistently enforced across the network for non-privileged and privileged users to confirm their user identity.

Recommendation 9

Ensure that system owners perform annual privileged user access reviews in accordance with SBA policies.

Status: Resolved

SBA managers agreed with the recommendation and stated they will ensure all system owners perform annual privileged user access reviews and retain documentation of completion in accordance with SBA policy. This recommendation can be closed once management provides evidence that system owners across the agency have annually performed privileged user access reviews.

Recommendation 10

Provide system owners and individuals with training or other communication emphasizing requirements for approving privileged user access prior to granting access.

Status: Resolved

SBA managers agreed with the recommendation, stating they will provide targeted training and communication to system owners and administrators that highlights the requirement to document approval prior to granting privileged access. This recommendation can be closed once management provides evidence that the agency is conducting training that includes the requirement to approve privileged user access prior to granting access. In addition, this recommendation can be closed once managers provide evidence that users' access was approved prior to receiving access to a system.

Recommendation 11

Ensure program offices review all system security plans and confirm they are updated, approved, and signed annually by the system owner, information systems security officer, and the information systems security manager.

Status: Resolved

SBA managers agreed with the recommendation, stating they will ensure all system security plans are reviewed, updated, approved, and signed annually by the system owner, information system security officer, and information system security manager. This recommendation can be closed once management provides the evidence that system security plans are updated, approved, and signed annually by the system owner, information systems security officer, and the information systems security manager.

Recommendation 12

Document procedures, roles, and responsibilities for performing an annual functional test to ensure that the alternative backup site keeps the system operational in accordance with SBA policy and procedures.

Status: Resolved

SBA managers agreed with the recommendation, stating the Office of the Chief Information Officer will work with the Office of Investment and Innovation to establish documented procedures, roles, and responsibilities to ensure annual functional testing is performed. This recommendation can be closed once management documents procedures, roles, and responsibilities for performing an annual functional test, and that the procedures ensure the alternative backup site keeps the system operational.

Recommendation 13

Annually perform functional testing to include failover testing in accordance with SBA policy and procedures.

Status: Resolved

SBA management agreed with the recommendation, stating the Office of the Chief Information Officer and Office of Investment and Innovation will ensure annual functional and failover testing is completed for all high value assets in accordance with SBA policy. This recommendation can be closed once management performs functional testing to include failover testing on an annual basis.

Recommendation 14

Establish procedures to monitor program officials' compliance with SOP 90 47 6, Cybersecurity and Privacy Policy, requirements to ensure information system contingency plans are developed, tested annually, and updated as needed.

Status: Resolved

SBA management agreed with the recommendation, stating the Office of the Chief Information Officer will coordinate with program offices to ensure compliance across all systems. This recommendation can be closed once management provides evidence of the compliance with completing annual reviews, updates, and testing of information system contingency plans.

Recommendation 15

Review and update the information system contingency plans and business impact assessments and ensure that key attributes are included.

Status: Resolved

SBA managers agreed with the recommendation, stating they will coordinate with program offices to ensure business impact assessments and information system contingency plans are reviewed and updated annually. This recommendation can be closed once management provides evidence that business impact assessments and information system contingency plans are developed, reviewed, and updated annually.

Recommendation 16

Update the information system contingency plans and business impact assessments at least once a year and include the recovery priority and lessons learned.

Status: Resolved

SBA managers agreed with the recommendation, stating they will ensure information system contingency plans and business impact assessments are updated annually and include recovery priorities and lessons learned. This recommendation can be closed once management provides evidence that recovery priorities and lessons learned are incorporated in the information system contingency plans and business impact assessments.

Recommendation 17

Conduct the information system contingency plans to include a business impact assessment at least annually.

Status: Resolved

SBA managers agreed with the recommendation, stating they will ensure business impact assessments and information system contingency plans are reviewed, updated, tested annually, and include recovery priorities and lessons learned. Also, they stated the Office of the Chief Information Officer will coordinate with the offices of Disaster Recovery and Resilience, Capital Access, and Investment and Innovation to ensure compliance across all systems. This recommendation can be closed once management provides evidence that business impact assessments and information system contingency plans are conducted annually.

Appendix 1: Scope and Methodology

Our objective was to determine the effectiveness of SBA's information security program and practices. The Office of Inspector General (OIG) contracted with an independent public accounting firm of auditors for our FY 2025 Federal Information Security Modernization Act (FISMA) of 2014 evaluation. OIG monitored the independent public accounting firm's work and reported SBA's progress toward strengthening the agency's cybersecurity program and practices through the FISMA CyberScope submission in August 2025.

As required by the Office of Management and Budget (OMB) "FY 2025 Guidance on Federal Information Security and Privacy Management Requirements" and the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, the independent public accountants assessed the effectiveness of SBA's cybersecurity program and practice across the 10 domains using the 25 metrics. OMB guidance requires the effectiveness of the metrics to be assessed using a maturity model that has five levels. The maturity levels range from 1 (very basic) to 5 (highly effective) as follows: ad hoc, 1; defined, 2; consistently implemented, 3; managed and measurable, 4; or optimized, 5 (see Table 2)

The auditors testing methodology included both 1) entity-wide test procedures to determine the effectiveness of the security policies, procedures, and practices across the agency; and 2) system-level test procedures to determine the effectiveness of the security policies, procedures, and practices for a specific system selected for the evaluation.

They judgmentally selected seven systems to perform system-level testing procedures. The auditors considered the following factors to identify a representative set of systems for testing:

- A mix of general support, high-value assets, and mission-critical systems;
- A mix of contractor-managed and SBA-owned systems;
- A mix of systems across multiple program offices to assess consistency of processes and procedures throughout the agency;
- For the non-financial systems, consideration of systems selected in the five prior FISMA evaluations were excluded; and
- A mix of systems that contained personally identifiable information to determine the maturity level of each metric.

Also, for the Contingency Planning domain the auditors selected an additional high-value asset system testing a total of eight for this domain.

As required by OMB's guidance, the auditors used the FY 2025 FISMA metrics, which consisted of a set of 20 core questions that are evaluated every year and 5 supplemental questions that are evaluated on a 2-year cycle to assess the effectiveness of SBA's cybersecurity program and practices. Based on the results of their testing, they provided the final maturity level determination for each metric question. Ultimately, the results of the test procedures indicate whether the domains are effective or not effective, as illustrated in Figure 1. Any metric that was rated as ad hoc, 1, or defined, 2, resulted in an area of improvement for the agency and a corresponding recommendation was made.

We monitored the contracted independent public accounting firm's adherence with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. These standards require that the auditors adequately plan and perform this evaluation to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objective. They are required to ensure the evidence obtained provides a reasonable basis for our findings and conclusions based on our objective. We did not identify any deviation from the professional standards.

Prior Audit Coverage

The following lists OIG's previous audit coverage related to this report:

Report Number	Report Title	Report Date
22-11	*FY 2021 Federal Information Security Modernization Act Review*	April 28, 2022
23-03	*FY 2022 Federal Information Security Modernization Act Review*	December 13, 2022
24-07	*FY 2023 Federal Information Security Modernization Act*	March 7, 2024
25-13	*FY 2024 Federal Information Security Modernization Act*	April 29, 2025

Appendix 2: Open Recommendations

There are 13 open audit recommendations from prior Federal Information Security Modernization Act evaluations that directly affected the maturity levels of the domains. The recommendations shown below were identified in fiscal years (FY) 2021, 2022, 2023, and 2024. The results were included in Report 25-13, *FY 2024 Federal Information Security Modernization Act Review,* issued April 29, 2025; 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.

Cybersecurity Supply Chain Risk Management

Agency policies and procedures require managers to continuously monitor security controls of the contractor's system and its environment of operation. Prior reviews found weaknesses in monitoring security controls over third-party contractors. To improve the maturity of this domain, SBA management should continue to make progress on implementing the following recommendations:

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) SP 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 required by federal law.

OIG Report 25-13, 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.

OIG Report 25-13, 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 as required by NIST SP 800-53.[17]

Risk and Asset Management

Federal guidance and agency procedures require that managers maintain a complete and up-to-date inventory of all components within the system boundary.[18] A prior review found a weakness in the completeness and accuracy of software and hardware asset inventory. To improve the maturity of this domain, SBA management should implement the following recommendation:

OIG Report 25-13, 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 as required by agency procedures.

Configuration Management

Federal guidance and agency procedures require that IT systems must be securely configured before being put into operation and while in operation.[19] A prior review found weaknesses in securely configured systems. To improve the maturity of this domain, SBA management should continue to make progress on implementing the following recommendations:

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.

OIG Report 25-13, Recommendation 4: Properly update and remediate configuration management vulnerabilities and weaknesses as specified in SBA's procedures.

[17] NIST, SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, at Control SR-11 (September 2020).
[18] NIST, SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, at Control CM-8 (September 2020).
[19] NIST, SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, at Control CM-6 (September 2020).

Identity and Access Management

FISMA requires that organizations identify and authenticate system users and limit system users to the information, functions, and systems those users are authorized to operate.[20] A prior review found weaknesses in SBA's user management. To improve the maturity of this domain, SBA management should continue to make progress on implementing the following recommendation:

> 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.

Data Protection and Privacy

Data protection and privacy procedures are required to be updated at least biannually. Our past audit found a weakness in policy updates. To address this weakness, we made the following recommendation to SBA:

> OIG Report 24-07, 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.

Incident Response

Agency procedures require that key agency officials identify incidents and analyze the risk of harm. A prior review found a weakness in policy updates. To improve the maturity of this domain, SBA management should continue to make progress on implementing the following recommendation:

> OIG Report 25-13, Recommendation 5: Update incident response documentation procedures, accounting for all necessary information to be included in the SBA cyber incident form.

Contingency Planning

National Institute of Standards and Technology Special Publication 800-53 states that contingency planning for information systems is part of an overall organizational program for achieving continuity for mission or business functions.[21] Prior reviews found weaknesses in SBA's

[20] NIST, SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, at Control AC-2 (September 2020).
[21] NIST, SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, at Control CP-2 (September 2020).

test of contingency plans. To improve the maturity of this domain, SBA management should continue to make progress on implementing the following recommendations:

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.

Appendix 3: FISMA Performance Metrics Overview

The Office of Management and Budget, in coordination with the Council of the Inspectors General on Integrity and Efficiency, the Federal Chief Information Officer, and the Federal Chief Information Security Officer Council, established metrics to standardize Office of Inspector General assessments of their agency's cybersecurity program and practices. The metrics are aligned with the six function areas in *The National Institute of Standards and Technology Cybersecurity Framework 2.0* resource and overview guide: govern, identify, protect, detect, respond, and recover. These metrics are then categorized by domains within the functions. A domain is a group of related cybersecurity outcomes that collectively comprise a function (see Table 3).

Table 3: FISMA Functions, Domains, and Number of Metrics for FY 2025 Assessment

Function	Domain	Number of Metrics
Govern	Cybersecurity governance	3
	Cybersecurity supply chain risk management	1
Identify	Risk and asset management	6
Protect	Configuration management	2
	Identity and access management	3
	Data protection and privacy	2
	Security training	1
Detect	Information security continuous monitoring	3
Respond	Incident response	2
Recover	Contingency planning	2

Source: OIG generated based on Cybersecurity and Infrastructure Security Agency reporting metrics

Appendix 4: Agency Response

U.S. Small Business Administration
Response to Draft Report

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

To: Office of Inspector General (OIG)

From: Michael T. Post
Chief Information Security Officer

Date: April 22, 2026

Subject: Response to Fiscal Year 2025 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.

This memorandum provides SBA's management response to the audit findings regarding annual security control assessments and governance requirements. The Office of the Chief Information Officer (OCIO) concurs with each recommendation, and the following sections outline actions OCIO has taken as well as planned corrective actions and milestones in order to satisfy all of the recommendations.

Recommendation 1 – Direct the Chief Information Officer to complete the implementation of a new Governance, Risk, and Compliance (GRC) tool to support timely completion of annual security control assessments in coordination with the Office of the Chief Financial Officer.

SBA Response – OCIO concurs. SBA will implement a centralized, automated platform to identify, assess, and mitigate cybersecurity risks. This solution will support real-time monitoring, automated assessments, and improved remediation tracking. The estimated IOC is June 1, 2026.

Recommendation 2 – Update SBA policy and procedures to clearly define the term "annual" and specify whether it refers to a 365-day period or the fiscal year ending September 30.

SBA Response – OCIO concurs. SBA has updated the Cybersecurity and Privacy Policy to define "annual" as aligned with the **fiscal year cycle** ending September 30, 2026. This clarification ensures consistent interpretation and implementation across all SBA systems. The estimated completion date is June 1, 2026.

Recommendation 3 – Direct the Associate Administrator for the Office of Capital Access (OCA) to ensure the agency follows policy to perform required security control assessments for all applicable systems.

SBA Response – OCIO concurs. OCA will coordinate with OCIO to ensure all systems under its authority complete annual security control assessments within the defined fiscal-year cycle. Additional oversight checkpoints and automated reminders will be integrated into the new GRC tool to ensure compliance. The estimated completion date is June 1, 2026.

Recommendation 4 – Update the SBA Standard Operating Procedure (SOP) 20 21 4, The Small Business Administration Acquisition and Procurement Program, January 16, 2025, Appendix C – Cybersecurity and Supply Chain Risk for IT Acquisitions to reflect the new process in which third-party supply chain risks will be continuously monitored through the Office of Chief Information Officer.

SBA Response – OCIO concurs. SBA developed documented new procedures in which third-party supply chain risks are continuously monitored through OCIO. This update will ensure alignment with NIST supply chain risk management expectations and SBA's enhanced Cybersecurity Supply Chain Risk Management (CSCRM) framework.

SBA has also developed a CSCRM Plan and enhanced the quarterly Information Security Continuous Monitoring (ISCM) Program to include NIST 800-53 Rev. 5 SCRM controls. These updates ensure periodic assessments and documented evidence of contractor monitoring artifacts.

Recommendation 5 – Implement policies, procedures, and processes for developing and maintaining an accurate inventory of data and its corresponding metadata from third parties.

SBA Response – OCIO concurs. SBA has developed a Data Security Plan for data labeling and tagging of all assets to maintain an accurate inventory of data and corresponding metadata from third parties.

Recommendation 6 – Improve governance, risk, and compliance systems to track cybersecurity risks.

SBA Response – OCIO concurs. SBA will implement a centralized, automated platform to identify, assess, and mitigate cybersecurity risks. This solution will support real-time monitoring, automated assessments, and improved remediation tracking. The estimated IOC is June 1, 2026.

Recommendation 7 – Develop and implement a process to monitor program offices' completion of required annual reviews of interconnection security agreements and ensure program officials review and sign the agreements prior to their expiration.

SBA Response – OCIO concurs. SBA has enhanced the quarterly ISCM Program to include NIST 800-53 Rev. 5 controls related to Interconnection Security Agreement (ISA) oversight, ensuring periodic assessments and timely renewal.

Recommendation 8 – Improve the existing process to manage PIV exemptions.

SBA Response – OCIO concurs. SBA has updated and defined the PIV exemption process. Exemptions are now limited to new hires for two weeks during onboarding, with a maximum extension of four weeks upon CISO approval.

Recommendation 9 - Ensure that system owners perform annual privileged user access reviews in accordance with SBA policies.

SBA Response – OCIO concurs. SBA will ensure all system owners perform annual privileged user access reviews in accordance with SBA policy and retain documentation of completion.

Recommendation 10 – Provide system owners and individuals with training or other communication emphasizing requirements for approving privileged user access prior to granting access.

SBA Response – OCIO concurs. SBA will provide targeted training and communication to system owners and administrators emphasizing the requirement to document approval prior to granting privileged access.

Recommendation 11 – Ensure program offices review all system security plans and confirm they are updated, approved, and signed annually by the system owner, information systems security officer, and the information systems security manager.

SBA Response – OCIO concurs. SBA will ensure all System Security Plans (SSPs) are reviewed, updated, approved, and signed annually by the system owner, Information System Security Officer (ISSO), and Information System Security Manager (ISSM).

Recommendation 12 – Document procedures, roles, and responsibilities for performing an annual functional test to ensure that the alternative backup site keeps the system operational in accordance with SBA policy and procedures.

SBA Response – OCIO concurs. OCIO will work with the Office of Investment and Innovation (OII) to establish documented procedures, roles, and responsibilities to ensure annual functional testing is performed.

Recommendation 13 - Annually perform functional testing to include failover testing in accordance with SBA policy and procedures.

SBA Response – OCIO concurs. OCIO and OII will ensure annual functional and failover testing is completed for all High Value Assets (HVAs) in accordance with SBA policy.

Recommendations 14 – Establish procedures to monitor program officials' compliance with Standard Operating Procedure 90 47 6, Cybersecurity and Privacy Policy requirements, to ensure information system contingency plans are developed, tested annually, and updated as needed.

Recommendation 15 – Review and update the information system contingency plans and business impact assessments and ensure that key attributes are included.

Recommendation 16 – Update the information system contingency plans and business impact assessments at least once a year and to include the recovery priority and lessons learned.

Recommendation 17 – Conduct the information system contingency plans to include a business impact assessment at least annually.

SBA Response: OCIO concurs with Recommendations 14-17. SBA will ensure Business Impact Assessments (BIAs) and Information System Contingency Plans (ISCPs) are reviewed, updated, tested annually, and include recovery priorities and lessons learned. OCIO will coordinate with ODRR, OCA, and OII to ensure compliance across all systems.

Conclusion

OCIO remains committed to strengthening SBA's cybersecurity governance, improving documentation and oversight, and ensuring full compliance with federal requirements. The corrective actions outlined above demonstrate SBA's proactive approach to addressing audit findings and enhancing enterprise-wide security resilience.

SBA concurs with the audit recommendations and is actively implementing corrective actions to strengthen governance, improve assessment timeliness, and ensure consistent policy interpretation. Deployment of the new GRC tool and updated policy guidance will significantly enhance SBA's ability to maintain continuous monitoring and meet federal cybersecurity requirements.

MICHAEL POST

Digitally signed by MICHAEL POST
Date: 2026.04.30 10:17:52 -04'00'

Michael T. Post

Chief Information Security Officer