OFFICE OF INSPECTOR GENERAL
U.S. SMALL BUSINESS ADMINISTRATION

DATE: November 23, 2026

TO: Kelly Loeffler
Administrator

FROM: William W. Kirk
Inspector General



SUBJECT: Evaluation of Fiscal Year 2026 Federal Information Security Modernization Act (Report 27-03)

I am pleased to present the attached fiscal year (FY) 2026 report on the evaluation of the U.S. Small Business Administration's (SBA) information security program in accordance with the Federal Information Security Modernization Act (FISMA) of 2014.[1] FISMA requires agencies to provide appropriate information security protections to help them minimize harm from unauthorized access, use, disclosure, disruption, modification, or destruction of information and systems. SBA management is required to assess the adequacy and effectiveness of the agency's information security policies, procedures, and practices on a quarterly basis. The Act also 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 internal controls of its agency annually.[2]

The Office of Inspector General's (OIG) FISMA evaluation results provide management, the Office of Management and Budget (OMB), Congress, and other stakeholders with an objective view of the agency's ability to identify, prioritize, address, and continuously monitor cybersecurity risks based on six functions (see Table 1). OMB uses FISMA reporting to assess agencies' cybersecurity programs and hold them accountable for improving their security posture.

[1] Pub. L. No. 113-283.
[2] 44 U.S. Code § 3555.

Table 1: Cybersecurity Functions Framework

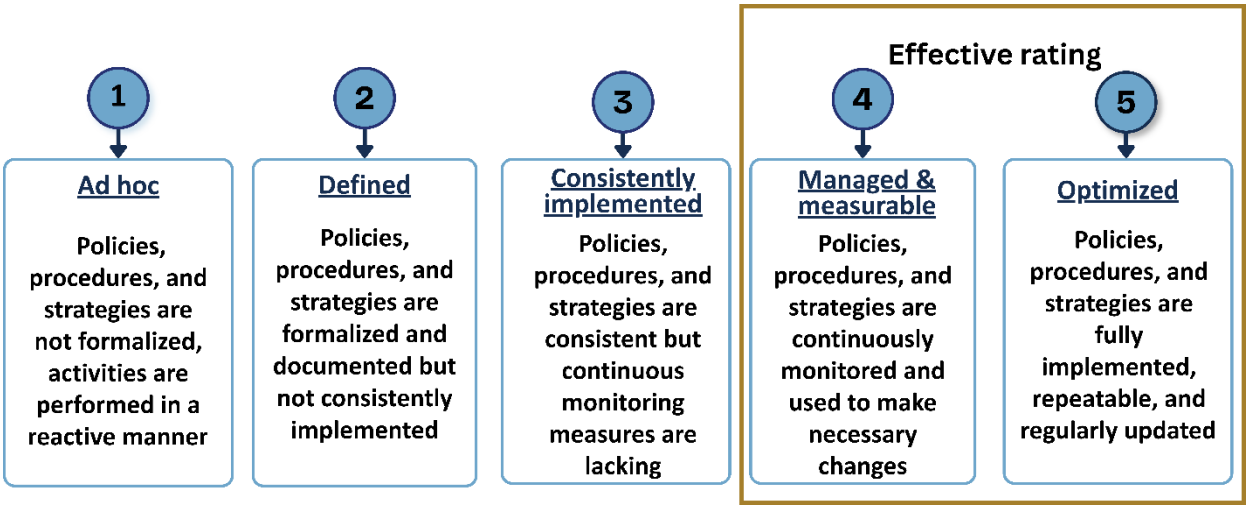
Risk Response	Function	Domains	Function Definition
Preventive	Govern	• Cybersecurity governance • Cybersecurity supply chain risk management	The agency's risk management strategy is implemented and monitored.
	Identify	• Risk and asset management	The agency's cybersecurity risks are understood.
	Protect	• Configuration management • Identity and access management • Data protection and privacy • Security training	The agency uses internal controls to manage cybersecurity risks, preventing or lowering the likelihood of a cyberattack and its adverse effects.
Reactive/manage	Detect	• Information security continuous monitoring	Possible cyberattacks and compromises are found and analyzed.
	Respond	• Incident response	Cybersecurity incidents are managed and appropriate actions taken.
	Recover	• Contingency planning	Normal operations are restored in a timely manner.

Source: OIG generated based on National Institute of Standards and Technology's *The NIST Cybersecurity Framework (CSF) 2.0*

For our FY 2026 evaluation of SBA's cybersecurity program, we contracted with independent external auditor KPMG LLP. Our contract required KPMG to conduct the evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Inspection and Evaluation* and OMB Memorandum M-25-04, "FY 2025 Guidance on Federal Information Security and Privacy Management Requirements."

The FISMA metrics assess specific aspects of an agency's information security program by asking questions under each function. Based on the evidence provided for those questions, the agency is scored on a 1 to 5 maturity scale, with scores of 4 or 5 considered an effective level of security controls (see Figure 1).

Figure 1: FISMA Maturity Levels



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

OMB strongly encourages offices of inspector general to focus on the results of the core metrics because they represent a combination of Administration priorities and align with OMB Memo M-22-09[3] and other OMB guidance. Based on the core metrics, the agency's information security program was rated a maturity level of 3, consistently implemented, meaning the agency has established and implemented cybersecurity policies and practices, but they need continuous monitoring and improvement to reach the effective cybersecurity baseline.

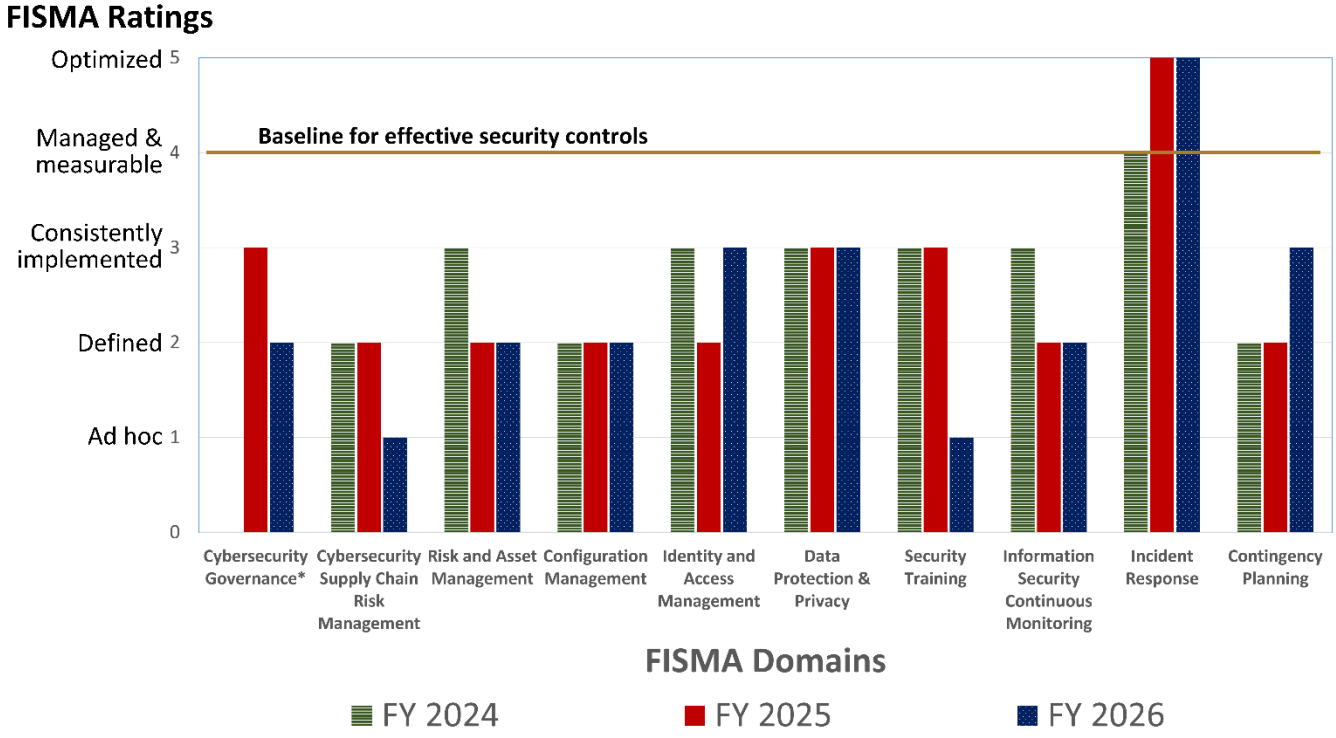
The assessment identified that SBA has the highest maturity level (5) in the incident response domain, which means SBA effectively detected cybersecurity incidents and took action. Also, the agency improved in the areas of identity and access management by consistently implementing a way to manage exceptions for users who cannot use a personal identity verification card to securely access the network. The agency also improved in contingency planning by consistently implementing exercises to restore systems to normal operations (see Figure 2).

The agency had gaps in risk and asset management, such as incomplete data inventories, an outdated risk profile, no enterprise solution for tracking cybersecurity risks, and insufficient documentation of system interconnections. The assessment also identified that security assessment and vulnerability management processes were inconsistently performed and enforced, including annual control assessments, database vulnerability scans, vulnerability tracking and remediation, and baseline compliance scans.

[3] OMB, M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles" (January 26, 2022).

SBA's Office of the Chief Information Officer also assessed its information security program and practices using the FISMA evaluation metric questions and reached similar conclusions, that most of the agency's internal controls, 84 percent, needed improvement to meet the OMB rating for effective security controls, managed and measurable maturity (level 4). Management made progress on implementing corrective actions to successfully close 10 recommendations from prior FISMA evaluations. Management continues to make progress on implementing 24 prior year recommendations (see Appendix 1). Management also plans to implement corrective actions to resolve all 11 recommendations made in the attached report (see Appendix 2).

Figure 2: Maturity Ratings by Domain for Fiscal Years 2024-2026



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

Source: OIG generated from CyberScope results

As shown in Figure 2, the ratings are calculated by averaging the responses to the questions within each domain and function. A sample of systems and a small subset of the metric questions also have changed over the years, which has caused individual metric question scores to vary. However, the agency's information security program consistently scores between 2 and 3 when averaged.

Additionally, the number of questions within a domain can have a significant effect on the resulting average. For example, the supply chain risk management and security training domains

received a score of 1 based on a single question (see Table 1 in the attached report), which lowered the govern and protect function scores to 2. A low score in one area does not necessarily indicate the entirety of the agency's govern and protect capabilities are performing at that level; it indicates the answers to the FISMA questions identified weaknesses in those functions.

The value of FISMA is in using the assessment to identify persistent weaknesses, understand their underlying causes, assign accountability, and demonstrate measurable improvement over time.

We monitored the independent external auditor's adherence with the CIGIE *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 their findings and conclusions based on the objective. We did not identify any deviation from the professional standards.

We appreciate the cooperation and assistance extended to KPMG and our office during the audit. Should you or your staff have any questions, please contact me or Andrea Deadwyler, Assistant Inspector General for Audits, at (202) 205-6586.

cc: Bill Briggs, Deputy Administrator, Office of the Administrator
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
Michelle Dawi, Senior Advisor, Office of the Administrator
Jennifer Prescott, General Counsel, Office of General Counsel
Lipika Hayet, Senior Advisor, Office of General Counsel
Tim Busler, Senior Counsel, Office of General Counsel
Michael Simmons, Attorney Advisor, Office of General Counsel
Hartley Caldwell, Chief Information Officer and Chief Super Intelligence Officer, Office of the Chief Information Officer
Doug Robertson, Deputy Chief Information Officer, Office of the Chief Information Officer
Michael Post, Chief Information Security Officer, Office of the Chief Information Officer
Nathan Davis, Chief Financial Officer and Chief Risk Officer, Office of the Chief Financial Officer
Nauman Ansari, Acting Deputy Chief Financial Officer, Office of the Chief Financial Officer
Laura Mintskovsky, Director of Financial Reporting and Quality Assurance, Office of the Chief Financial Officer
Blake Hoing, Controller, Office of the Chief Financial Officer
Thomas Kimsey, Associate Administrator, Office of Capital Access
Chris Stallings, Associate Administrator, Office of Disaster Recovery

Attachment

Fiscal Year 2026 Evaluation of the Small Business Administration (SBA) Pursuant to the Federal Information Security Modernization Act

Prepared for: SBA Office of the Inspector General

October 8, 2026

KPMG LLP
1801 K Street
Washington, D.C. 20006

TABLE OF CONTENTS

KPMG Letter 1
Background 3
Objective 3
Scope 4
Methodology 4
Findings and Recommendations 6
1. Govern Function Area 6
2. Identify Function Area 7
3. Protect Function Area 9
4. Detect Function Area 13
5. Respond Function Area 13
6. Recover Function Area 13
Conclusion 14
Appendix 1: Open Recommendations from Prior FISMA Evaluations 15
Appendix 2: SBA Management's Response 18

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

Inspector General
Small Business Administration (SBA)

This report presents the results of our work conducted to address the independent evaluation requirements of the *Federal Information Security Modernization Act (FISMA) of 2014*. Our scope period for testing was October 1, 2025, through June 30, 2026. Our work was performed during the period of May 6, 2026, through August 19, 2026 and our results are as of August 25, 2026.

We conducted this evaluation in accordance with the:

- Council of Inspectors General on Integrity and Efficiency (CIGIE) *Quality Standards for Inspection and Evaluation* issued December 2020; and
- American Institute of Certified Public Accountants (AICPA) Consulting Standards.[1]

This evaluation did not constitute an audit of financial statements, or an attestation level report as defined under *Generally Accepted Government Auditing Standards* (GAGAS) and the AICPA standards for attestation engagements.

FISMA directs federal agencies to report annually to the Office of Management and Budget (OMB) Director, Comptroller General, and select congressional committees on the effectiveness of agency information security management programs and practices, and compliance with FISMA. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security management program and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency Inspector General (IG) or an independent external auditor as determined by the IG.

The objectives of our work were to determine whether SBA's overall information security management program and practices were consistent with the requirements of FISMA.[2]

We evaluated the maturity of the information security management program for 10 FISMA metric domains within the 6 Cybersecurity Framework functions: Govern (Cybersecurity Governance and Supply Chain Risk Management), Identify (Risk and Asset Management), Protect (Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training), Detect (Information Security Continuous Monitoring), Respond (Incident Response), and Recover (Contingency Planning).

[1] While KPMG conducted the SBA FISMA evaluation under CIGIE quality standards, KPMG is required to conduct services in accordance with professional standards promulgated by the AICPA or a body designated by the AICPA. Since the AICPA does not recognize CIGIE as a standard-setting body, we paired this evaluation with AICPA Consulting Standards, which has objectives closely aligned with those of an evaluation. CIGIE and AICPA Consulting Standards require that we plan and conduct the engagement to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions.

[2] The IG FISMA Reporting Metrics were developed by the OMB, the Department of Homeland Security, and CIGIE. As of the date of this report, OMB did not release new reporting metrics for FY 2026 and directed agencies to use the FY 2025 IG FISMA Reporting Metrics for the required annual Inspector General FISMA evaluation.

KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

We identified findings within the functional areas of Govern, Identify, Protect, and Recover. The findings exist because SBA management did not consistently implement and enforce information technology (IT) security policies and procedures in accordance with relevant SBA and OMB requirements. The findings identified in this report were communicated to SBA management prior to the issuance of this report.

KPMG LLP (KPMG) cautions that projecting the results of our evaluation to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

This report is intended solely for the use of the SBA OIG and SBA and is not intended to be and should not be relied upon by anyone other than these specified parties.

KPMG LLP

BACKGROUND

The Federal Information Security Modernization Act of 2014 (FISMA) was passed by Congress and signed into law by the President in 2014.[3] FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce risks to an acceptable level. The Act assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST), and OMB to strengthen information security management programs.

FISMA directs NIST to develop standards and guidelines for helping ensure the effectiveness of information security controls over information systems that support federal agencies' operations and assets. In response to this mandate, NIST has developed a risk management framework to guide agency efforts to establish effective information security management program in compliance with FISMA. Specifically, the framework provides standards and guidelines to agencies for categorizing information systems, selecting information security controls to meet minimum security requirements, performing risk and information security controls assessments, authorizing systems to operate, performing monitoring activities to continually assess the adequacy of information security controls in supporting agency operations, and developing corrective actions plans to mitigate security risks identified throughout a system's lifecycle.

Annually, agency Inspectors General are required to either perform an independent evaluation or contract an independent external auditor to perform an evaluation of the agency's information security program and practices to assess the effectiveness of the program and practices. Each evaluation must include: (1) testing the effectiveness of information security programs and practices of a representative subset of the agency's information systems; (2) an assessment (based on the result of the testing) of requirements with FISMA; and (3) separate representations, as appropriate, regarding information security related to national security systems. Additionally, we performed an evaluation of selected information security controls.

OBJECTIVE

KPMG was engaged by the SBA OIG to perform on its behalf the annual, independent evaluation of SBA's information security program and practices in accordance with FISMA. The objective of our evaluation was to assess the effectiveness of SBA's overall information security program and practices using the IG FISMA Reporting Metrics required for FY 2026. As of the date of this report, OMB did not release new reporting metrics for FY 2026 and directed agencies to use the FY 2025 IG FISMA Reporting Metrics[4], herein referred to as the IG FISMA Reporting Metrics, for the required annual IG FISMA evaluation.

Our evaluation objective was to determine whether SBA's overall information security management program and practices were consistent with the requirements of FISMA.

[3] 44. U.S.C § 3551-3558

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

SCOPE

We conducted this evaluation in accordance with the:

- Council of Inspectors General on Integrity and Efficiency (CIGIE) *Quality Standards for Inspection and Evaluation* issued December 2020; and
- American Institute of Certified Public Accountants (AICPA) Consulting Standards.[5]

The scope period for testing was October 1, 2025, through June 30, 2026.

Our work was performed during the period of May 6, 2026, through August 19, 2026, and our results are as of August 25, 2026. The test work was performed in Washington, D.C. and remotely.

KPMG conducted the evaluation based on a subset of five of SBA's information systems. The subset of systems was selected in concurrence with the SBA OIG from the total population of 55 information systems identified by SBA management. The results of this control test work were considered in our assessment of SBA's overall information security management program. Further, the evaluation of management's corrective actions associated with prior year findings is considered in scope for the evaluation.

METHODOLOGY

KPMG tested SBA management's implementation of information security controls based on criteria specified in the IG FISMA Reporting Metrics and controls within NIST Special Publication (SP) 800-53, Revision (Rev.) 5, *Security and Privacy Controls for Federal Information Systems and Organizations* referenced in the metrics. The following tables show the alignment of the IG FISMA Reporting Metric domain areas with the NIST Cybersecurity Framework Function areas (Table 1).

[5] While KPMG conducted the SBA FISMA evaluation under CIGIE quality standards, KPMG is required to conduct services in accordance with professional standards promulgated by the AICPA or a body designated by the AICPA. Since the AICPA does not recognize CIGIE as a standard-setting body, we paired this evaluation with AICPA Consulting Standards, which has objectives closely aligned with those of an evaluation. CIGIE and AICPA Consulting Standards require that we plan and conduct the engagement to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions.

Table 1
NIST Cybersecurity Framework and IG FISMA Metric Area Alignment

NIST Cybersecurity Framework Function	IG FISMA Metric Domain	Number of Metrics
Govern	Cybersecurity Governance	3
	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: FY 2025 IG FISMA Reporting Metrics[4]

KPMG's approach addressed FISMA's independent evaluation requirements for SBA to develop an effective information security management framework by evaluating the design, implementation, and operating effectiveness of SBA controls based on criteria contained in the IG FISMA Reporting Metrics.

KPMG's approach to accomplishing this evaluation was to assess the design, implementation, and operating effectiveness of controls referenced in the IG FISMA Reporting Metrics that comprise SBA's information security management program. Evaluating the design and implementation of the information security controls entailed gaining an understanding of information security related policies and guidelines established by SBA management. KPMG evaluated the policies and practices associated with controls established by SBA management against the applicable federal laws and criteria to determine their design and operating effectiveness relative to the FISMA requirements. We performed inquiry, observation, and inspection procedures in support of our evaluation. The following list clarifies those terms:

- Inquiry – Discussions with appropriate personnel and corroboration with management;
- Observation – View the application, supporting system software, or performance or existence of a control; and
- Inspection – Review documents and reports indicating performance of a control.

Specifically, KPMG inspected pertinent security and system documentation, including SBA's Information Technology (IT) security policies and procedures and security authorization documentation. We also interviewed Information Systems Security Managers, Information System Security Officers, and other individuals with significant IT responsibilities.

Furthermore, when considering the use of information furnished by SBA management in the execution of evaluation procedures, we evaluated whether the information was sufficiently reliable for the purposes of our evaluation by obtaining evidence regarding the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed.

FINDINGS AND RECOMMENDATIONS

Our evaluation of the SBA's information security management program focused on assessing the design, implementation, and operating effectiveness of information security control techniques implemented in accordance with FISMA. The following section includes the findings and recommendations identified during these assessments. Findings and recommendations are organized according to the NIST Cybersecurity Framework Functions and Domains to which they relate. Where one notification of findings and recommendation (NFR) spanned multiple domains, we separated the relevant aspects, as applicable. Further, this includes both new recommendations, and recommendations issued within previous SBA FISMA reports. Where a recommendation was reissued from the prior year, we included the prior report and recommendation number for tracking instead of issuing a new recommendation number. Please see Appendix 1 for the full list of prior year FISMA recommendations.

1. Govern Function Area

We determined SBA's maturity for the Govern function area to be a Level 2, *Defined*. The Govern function area consists of the following domains Cybersecurity Governance (CG) and Cybersecurity Supply Chain Risk Management (C-SCRM).

Cybersecurity Governance

We determined SBA's maturity for the CG domain to be a Level 2, *Defined,* and communicated the following associated notification of findings and recommendation (NFR) to management:

Risk Management Program Weaknesses **(FISMA-NFR-2026-03)**

We noted SBA management had not consistently implemented certain controls within the CG FISMA metric domain. Specifically, SBA did not have a current Risk Profile established during the period. SBA's last Risk Profile was approved November 18, 2024.

Management indicated that this condition occurred because of competing priorities with limited resources.

We identified this finding based on the following criteria:

> OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 15, 2026, B. Risk Profiles.

Without a current Risk Profile, SBA may not have reasonable assurance that emerging and existing risks are consistently identified, evaluated, prioritized, and managed across the organization.

We recommend that SBA management:

1. Approve and establish a Risk Profile so SBA can obtain reasonable assurance that emerging and existing risks are consistently identified, evaluated, prioritized, and managed across the organization.

Cybersecurity Supply Chain Risk Management

We determined SBA's maturity for the C-SCRM domain to be a Level 1, *Ad Hoc,* and communicated the following associated NFR to management:

***C-SCRM Program Weaknesses* (FISMA-NFR-2026-05)**

During the period (October 1, 2025, through June 30, 2026), SBA management did not fully define controls to evidence that external service providers adhered to their C-SCRM requirements nor were they able to evidence SBA management's assessment and review of the supply chain-related risks during the evaluation period. Specifically, KPMG was informed that SBA delegates all C-SCRM efforts to the General Services Administration (GSA). Although SBA provided an updated C-SCRM Plan on July 26, 2026, defining SBA and GSA roles and responsibilities, the plan was developed after the evaluation period and therefore does not evidence controls operating during the period under review.

On July 26, 2026, management updated SBA's *Cybersecurity Supply Chain Risk Management (C-SCRM) Plan* to define the controls noted above.

Management indicated that the condition occurred because of competing priorities with limited resources.

We identified this finding based on the following criteria:

> *SBA Cybersecurity and Privacy Policy Standard Operating Procedures (SOP) 90 47 7*, last revised May 6, 2026, 22. Supply Chain Risk Management.

The absence of enforcement controls within the C-SCRM plan increases the risk of undetected vendor vulnerabilities and supply chain compromises. Additionally, without clearly assigned ownership and formal escalation pathways, C-SCRM activities will lack consistent execution, leading to accountability gaps and unmanaged risk. In the event a vendor fails to meet security baselines, the absence of predefined enforcement mechanisms prevents timely remediation, leaving the organization vulnerable to active third-party security threats.

On July 22, 2026, SBA updated the C-SCRM plan to remediate the noted condition, as such, KPMG did not issue a recommendation.

2. Identify Function Area

We determined SBA's maturity for the Identify function area to be a Level 2, *Defined*. The Identify function area consists of one domain, Risk and Asset Management (RAM).

Risk and Asset Management

We determined SBA's maturity for the RAM domain to be a Level 2, *Defined,* and communicated the following associated NFR to management:

Risk Management Program Weaknesses **(FISMA-NFR-2026-03)**

We noted SBA management did not consistently implement certain controls within RAM and Information Systems Continuous Monitoring (ISCM) FISMA metric domains. Specifically:

1. Since December 2024, SBA lacks an automated enterprise-wide solution for tracking its information systems' cybersecurity risk information.
2. For one of five in-scope systems, SBA management did not consistently implement controls to perform annual security control assessments for the system. While SBA completed the most recent security control assessment on June 30, 2026, the prior security control assessment was completed on March 1, 2022, which did meet the required annual frequency.
3. For one of five in-scope systems, SBA management did not consistently implement controls to authorize the system. Specifically, although the Authorization to Operate (ATO) was extended on March 17, 2026, through September 30, 2026, the prior ATO expired on January 6, 2025, resulting in a 15-month time period in which the system was not authorized.
4. SBA management did not consistently document Interconnection Security Agreements (ISAs) for four of the five in-scope systems.

The conditions occurred because the planned Governance, Risk, and Compliance (GRC) tool, which was intended to provide an automated enterprise-wide solution for tracking cybersecurity risk information, was discontinued. As a result, SBA continues to rely on manual processes to manage and track cybersecurity risk information across its information systems. This reliance on manual processes contributed to delays or gaps in monitoring system security status, including the timely completion of annual security assessments, maintenance of valid ATOs, and support the completion of ISAs.

We identified this finding based on the following criteria:

> *SBA Cybersecurity and Privacy Policy Standard Operating Procedures (SOP) 90 47 7*, last revised May 6, 2026, *Chapter 2: Roles and Responsibilities and Chapter 7: Assessment, Authorization, and Monitoring.*
>
> NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organization*, control CA-2 *CONTROL ASSESSMENTS.*

The lack of an automated GRC tool results in reliance on manual processes to track and manage cybersecurity risks, increasing the likelihood of delays, errors, and incomplete oversight. Additionally, incompletion of annual security assessments may allow security vulnerabilities, control deficiencies, and compliance gaps to remain unidentified and unaddressed, increasing cybersecurity risk. Further, incompletion or renewal of ATOs may result in security controls not being adequately reviewed and validated, increasing the risk that unresolved weaknesses affect the confidentiality, integrity, and availability of organizational systems and data. The purpose of an ISA is to provide a technical framework for agreed upon security controls and outline responsibilities for data shared between the two systems. Without having final documented agreements reviewed and approved by both parties, the risk exists that the terms of the agreements may not be understood or appropriately implemented to address all security requirements.

We recommend that SBA management:

2. Implement a centralized process for tracking ATO milestones, renewal dates, and required documentation to ensure timely completion and reauthorization activities.

Additionally, the following recommendations were reissued from prior reports:

Report 26-10, FY 2025 Federal Information Security Modernization Act, issued May 19, 2026

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 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.

Data Inventory Weakness (FISMA-NFR-2026-04)

SBA did not consistently implement its procedures and processes to maintain a comprehensive and accurate inventory of its data and corresponding metadata.

Management indicated that due to competing priorities with limited resources, management was still in the process of identifying and collecting information on all data assets necessary to develop a complete enterprise-wide data inventory and is working to secure the resources needed to support this effort.

We identified this finding based on the following criteria:

44 United States (U.S.) Code Section 3511 – Data Inventory and Federal Data Catalogue

Without consistently implementing the developed policies, procedures, processes, and roles and responsibilities for developing and maintaining comprehensive and accurate data inventory and corresponding metadata, SBA may not be able to assess, manage, monitor, and/or mitigate cybersecurity risks.

We recommend that SBA management:

3. Implement the defined policies, procedures, and processes to develop, maintain, and regularly update a comprehensive and accurate inventory of organizational data and its corresponding metadata. This should include, but not be limited to, identifying and documenting data types, assigning data owners, maintaining records of data repositories and data flows, applying data classifications through appropriate tags or labels, and tracking key metadata attributes such as data ownership, provenance, geolocation, and information location. Additionally, periodic reviews should be performed to validate the completeness, accuracy, and currency of the data inventory and associated metadata.

3. Protect Function Area

We determined SBA's maturity for the Protect function area to be a Level 2, *Defined*. The Protect function area consists of four following domains: Configuration management (CM), Identity and Access management (IDAM), Data Protection and Privacy (DPP), and Security Training (ST).

Configuration Management

We determined SBA's maturity for the CM domain to be a Level 2, *Defined,* and communicated the following associated NFR to management:

Configuration, Patch and Vulnerability Management Program Weaknesses **(FISMA-NFR-2026-07)**

SBA management did not consistently implement certain controls within the SBA vulnerability management program. Specifically, KPMG identified the following:

1. Management did not perform required database vulnerability scanning for one in-scope system.
2. Although the Office of the Chief Information Officer (OCIO) established collaborative vulnerability management processes, to include automated scanning, OCIO management did not consistently remediate, track the remediation of, or fully document Plans of Action and Milestones (POA&Ms) for critical, high, medium, and low-risk vulnerabilities for two in-scope systems.
3. Although the OCIO utilized tools within its security pipelines (such as Center for Internet Security (CIS) benchmarks and Ansible playbooks) to enforce baselines compliance across components of the IS environment, management did not consistently enforce baseline compliance configuration settings across one in-scope system. Specifically, we noted noncompliance with configuration baseline settings through baseline configuration scans within the system.

The conditions occurred because:

- SBA management did not establish continuous automated database vulnerability scanning for the noted system because of an oversight by management in which the noted database was not included in enterprise scanning processes.
- Management did not consistently remediate noted vulnerabilities timely, nor document associated POA&M records with the detailed information required by SBA policy throughout the fiscal year because of the high volume of vulnerabilities and a reliance on interim manual tracking while the agency's primary GRC tool remained under development.
- OCIO management did not continuously implement and monitor the enforcement of baseline compliance requirements because of management oversight.

We identified this finding based on the following criteria:

> NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organization*, controls: RA-05, *Vulnerability Monitoring and Scanning;* CM-6, *Configuration Settings*; and SI-02, *Flaw Remediation.*

Lack of untimely patch management and improper system configurations increases the risk that known vulnerabilities could be exploited, exposing the system to unauthorized access, malicious attacks, and potentially compromise the confidentiality, integrity, and availability of the data residing within the information system. Additionally, not performing an annual security assessment can lead to vulnerabilities that may go unnoticed, increasing the system's risk. Without this assessment, responsible individuals may not be able to properly understand and apply controls to the information system or identify necessary changes that are required to be implemented. This can lead to a failure in security controls, potentially compromising data confidentiality, integrity or availability. Further, failure to perform and maintain security compliance scans may lead to increased vulnerability to security threats and non-compliance with established regulations, potentially resulting in unauthorized access, data breaches, and compromised system integrity.

We recommend that SBA management:

4. Implement database vulnerability scanning in accordance with SBA and NIST requirements and maintain documentation to evidence the scans.
5. Continue to implement procedures to remediate all existing configuration baseline failures within SBA systems. Ensure ongoing enforcement by continuous monitoring to detect drift from authorized baselines, while regularly reviewing and maintaining historical remediation documentation to ensure adherence to NIST Risk Management Framework controls.
6. Implement a formalized root cause analysis process for identified deficiencies. Establish and continuously enforce strict remediation milestones to track, manage, and definitively resolve the underlying systemic failures leading to findings.

Additionally, the following recommendations were reissued from prior reports:

Report 24-07, FY 2023 Federal Information Security Modernization Act Review, issued March 7, 2024

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

Identity and Access Management

We determined SBA's maturity for the IDAM domain to be a Level 3, *Consistently Implemented,* and communicated the following associated NFR to management:

***Identity and Access Management Program Weaknesses* (FISMA-NFR-2026-06)**

KPMG identified the following weaknesses with SBA controls and processes that align to the IDAM FISMA metric domain:

1. For two of the five in-scope systems, management did not configure the system to implement session termination after 30 minutes of inactivity, according to SBA policy.
2. For two of the five in-scope systems, management did not provide evidence supporting the approval and provisioning of the sampled newly assigned privileged users.
3. For three of the five in-scope systems, management was unable to provide documentation evidencing the completion of the annual privileged user recertification process.
4. For one of the five in-scope systems, management did not consistently implement controls to perform annual privileged user access recertifications.

Management indicated that the condition occurred because of competing priorities with limited resources.

We identified this finding based on the following criteria:

SBA Cybersecurity and Privacy Policy Standard Operating Procedures (SOP) 90 47 7, last revised May 6, 2026, Chapter 4: Policy on Access Controls.

Non-compliant session termination settings may allow inactive sessions to remain open longer than intended, increasing the risk of misuse of system access. Additionally, the lack of documented and retained access requests for newly added privileged users increases the risk that privileged access is granted without adequate authorization or oversight, potentially resulting in unauthorized access to production systems, data, and computing resources. Further, the lack of establishing a formal

privileged user access recertification process and performing periodic access recertifications increases the risk that unauthorized, inappropriate, or excessive privileged access may not be identified and removed in a timely manner, potentially resulting in unauthorized access to or modification of production systems, data, and computing resources.

We recommend that SBA management:

7. Review and remediate session termination configurations for all information systems to ensure inactivity timeout settings comply with SBA policies.
8. Implement and enforce a process to document, approve, and retain evidence of privileged user access requests prior to granting system access, ensuring privileged access is appropriately authorized, traceable, and supported by management oversight.

Additionally, the following recommendations were reissued from prior reports:

Report 26-10, FY 2025 Federal Information Security Modernization Act, issued May 19, 2026

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.

Data Protection and Privacy

We determined SBA's maturity for the DPP domain to be a Level 3, *Consistently Implemented,* and communicated the following associated NFR to management:

Security Training

We determined SBA's maturity for the ST domain to be a Level 1, *Ad Hoc,* and communicated the following associated NFR to management:

***Workforce Assessment Program Weaknesses* (FISMA-NFR-2026-02)**

SBA management did not fully define or implement workforce assessments to determine the skills, knowledge, and abilities of its workforce. Specifically, SBA conducts the IT Specialist 2210 Series Competency Assessment (CA) every two years to analyze the workforce skills and knowledge across the agency; however, the last one was conducted in June of 2023. The assessment conducted in June 2023 had expired in June 2025; therefore, SBA did not complete the required assessment during our current scope period.

Management indicated that the condition occurred because the assessment administration is currently on hold due to an upcoming reorganization and change in risk environment.

We identified this finding based on the following criteria:

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organization*, released August 2022, control PM-13, *SECURITY AND PRIVACY WORKFORCE.*

Not defining and implementing a process to assess the skills, knowledge, and abilities of its workforce and aligning them with specialized security training increases the risk of an unclear understanding of workforce capabilities and an undertrained workforce.

We recommend that SBA management:

9. Define a process to implement a workforce assessment program to determine the skills, knowledge, and abilities of SBA's workforce to provide specialized security training within the functional areas of govern, identify, protect, detect, respond, and recover.

4. Detect Function Area

We determined SBA's maturity for the Detect function area to be a Level 2, *Defined*. The Detect function area consists of one domain, Information Security Continuous Monitoring (ISCM). Findings related to this domain were communicated in conjunction with those for the RAM domain as documented within the ***Risk Management Program Weaknesses*** **(FISMA-NFR-2026-03)** in the Protect domain.

5. Respond Function Area

We determined SBA's maturity for the Respond function area to be a Level 5, *Optimized*. The Respond function area consists of one domain, Incident Response (IR), for which we had no related findings and recommendations.

6. Recover Function Area

We determined SBA's maturity for the Recover function area to be a Level 2, *Defined*. The Recover function area consists of one domain, Contingency Planning (CP).

Contingency Planning

We determined SBA's maturity for the CP domain to be a Level 3, *Consistently Implemented,* and communicated the following associated NFR to management:

Contingency Planning Program Weaknesses **(FISMA-NFR-2026-01)**

The SBA Continuity of Operations Plan (COOP), which contains the SBA organizational Business Impact Assessment (BIA), was not updated annually. Further, management did not fully complete the annual exercise. Specifically, the COOP was last updated in June 2023 and although a Disaster Tabletop Exercise was performed within the last year, disaster recovery exercise responses were not provided for 4 of 8 Mission Essential Functions (MEFs) during the FY 2025 Disaster Tabletop Exercise (DPRP), dated June 24, 2025.

Management indicated that the condition occurred because of a recent SBA reorganization which impacted the program offices responsible.

We identified this finding based on the following criteria:

> Federal Continuity Directive, *Federal Executive Branch Continuity Program Management Requirements*, FEMA Office of National Continuity Programs, dated August 2024, section *7.1.2. CONTINUITY PLANNING and* 7.1.4. CONTINUITY EVALUATION.

Inconsistent documentation and testing of the SBA's COOP could increase the risk that SBA sensitive data and business functions could become unavailable and impact business operations. This may consequently decrease SBA's ability to adequately protect and recover critical information systems. Further, the lack of a current agency level BIA increases the risk that SBA will fail to appropriately identify essential functions and allocate appropriate resources to ensure their continuity.

We recommend that SBA management:

10. Review and update the SBA COOP, which includes the organizational BIA, on an annual basis.
11. Fully exercise the COOP to include all MEFs, in accordance with Federal requirements.

CONCLUSION

We identified findings in 6 of the 10 metric domains of SBA's information security management program pertaining to 4 of the 6 Cybersecurity Framework functions. Specifically, we identified control findings in the functional areas of Govern, Identify, Protect, Detect and Recover. Without effective controls in place, these control findings could increase the risk in the information security management program and impact the cybersecurity risk maturity across the organization. These findings exist because SBA management did not consistently implement and enforce IT security policies and procedures in accordance with relevant SBA and OMB requirements. The findings identified in this report were communicated to SBA management prior to the issuance of this report. SBA management should also consider whether any specific recommendation in this report apply to other information systems maintained in the organization's FISMA system inventory and implement remedial action as needed.

APPENDIX 1: OPEN RECOMMENDATIONS FROM PRIOR FISMA EVALUATIONS

The following table provides the status of open recommendations from prior FISMA evaluations, as of the date of this report. Recommendations reissued in the current year are referenced within the body of the report.

OIG Report	#	Recommendation
Report 23-03, *FY 2022 Federal Information Security Modernization Act Review*, issued December 15, 2022		
23-03	02	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.
23-03	03	Communicate and reinforce to program offices the requirement to review and remove system and user accounts in accordance with SBA's Standard Operating Procedure.
23-03	05	Develop, document, and implement a process that requires management review of information security data and report information security threats.
Report 24-07, *FY 2023 Federal Information Security Modernization Act Review*, issued March 7, 2024		
24-07	05	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.
24-07	06	Define timeframe and remediation requirements for baseline and configuration weaknesses as outlined in NIST 800-53.
24-07	07	Properly update and remediate vulnerabilities and configuration weaknesses throughout the SBA environment as required by SBA Standard Operating Procedure.
24-07	10	Update existing procedures that identify the roles of individuals with signification IT responsibilities who require role-based training and ensure such training is provided and tracked.
24-07	11	Provide training to individuals with contingency planning roles and responsibilities.
Report 25-13, *FY 2024 Federal Information Security Modernization Act Review,* issued April 29, 2025		
25-13	02	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	#	Recommendation
25-13	03	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.
25-13	04	Properly update and remediate configuration management vulnerabilities and weaknesses as specified in SBA's procedures.
25-13	06	Update or establish procedures to ensure that all employees and contractors receive security awareness training in a timely manner.
25-13	07	Develop and implement a process to verify remedial action has occurred if an individual fails to complete the required training within the designated timeframe.
Report 26-10, *FY 2025 Federal Information Security Modernization Act,* issued May 19, 2026		
26-10	01	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.
26-10	02	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.
26-10	03	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.
26-10	04	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 16 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.
26-10	06	Improve the governance risk and compliance systems to track cybersecurity risks.
26-10	07	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.
26-10	09	Ensure that system owners perform annual privileged user access reviews in accordance with SBA policies.
26-10	10	Provide system owners and individuals with training or other communication emphasizing requirements for approving privileged user access prior to granting access.
26-10	15	Review and update the information system contingency plans and business impact assessments and ensure that key attributes are included.

OIG Report	#	Recommendation
26-10	16	Update the information system contingency plans and business impact assessments at least once a year and include the recovery priority and lessons learned.
26-10	17	Conduct the information system contingency plans to include a business impact assessment at least annually.

APPENDIX 2: SBA MANAGEMENT'S RESPONSE

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

To: William W. Kirk
Inspector General

From: Douglas Robertson
Deputy Chief Information Officer

Date: October 8, 2026

Subject: Response to Fiscal Year 2026 Evaluation of the Small Business Administration (SBA) Pursuant to the Federal Information Security Modernization Act

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.

Here are OCIO's plans and actions with the goal of satisfying the eleven (11) recommendations documented in the draft report:

Recommendation 1 - Approve and establish a Risk Profile so SBA can obtain reasonable assurance that emerging and existing risks are consistently identified, evaluated, prioritized, and managed across the organization

SBA Response – SBA concurs. SBA will finalize, approve, and publish an enterprise cybersecurity Risk Profile aligned with the NIST Cybersecurity Framework 2.0 Govern function and NIST SP 800-37 and SP 800-39. The Risk Profile will define risk appetite, tolerance, categories, and ownership, and will be approved through CIO and CISO governance.

SBA will maintain the risk register in ServiceNow Integrated Risk Management (IRM), populated with exposure data from Tenable, Wiz, Rapid7, and SentinelOne through ServiceNow Unified Security Exposure Management (USEM) so emerging and existing risks are identified, evaluated, and prioritized consistently. Enterprise risk posture will be reported to leadership through the ServiceNow CISO Dashboard and reviewed at least quarterly.

Recommendation 2 – Implement a centralized process for tracking ATO milestones, renewal dates, and required documentation to ensure timely completion and reauthorization activities.

SBA Response – SBA concurs. SBA will use ServiceNow Continuous Authorization and Monitoring (CAM) as the centralized, authoritative record for all system authorizations, including ATO milestones, expiration and renewal dates, and required artifacts such as the SSP, SAR, POA&Ms, contingency plans, and PTA/PIA documentation. Authorization data currently

maintained in SharePoint will be migrated into CAM through a governed ServiceNow Integration Hub SharePoint integration, beginning with POA&M data and expanding to all authorization data types. CAM will generate automated notifications to system owners and ISSOs in advance of upcoming milestones and expirations, and ATO status will be reported through the CISO Dashboard.

Recommendation 3 - Implement the defined policies, procedures, and processes to develop, maintain, and regularly update a comprehensive and accurate inventory of organizational data and its corresponding metadata. This should include, but not be limited to, identifying and documenting data types, assigning data owners, maintaining records of data repositories and data flows, applying data classifications through appropriate tags or labels, and tracking key metadata attributes such as data ownership, provenance, geolocation, and information location. Additionally, periodic reviews should be performed to validate the completeness, accuracy, and currency of the data inventory and associated metadata.

SBA Response – SBA concurs. SBA will implement its data inventory policies and procedures using ServiceNow CMDB as the system of record for data repositories, data owners, data types, and data flows, using CMDB service relationships to document how data moves between applications and systems. Microsoft Purview and Fortra will support automated data discovery, classification, and sensitivity labeling, and Wiz will identify sensitive data in cloud data stores. Responsibilities will be shared among the Data Office (governance and stewardship), Records Management (retention and disposition), and Cyber Security (control enforcement), with privacy determinations linked through the PTA/PIA process. The inventory will be reviewed and updated on a recurring basis.

Recommendation 4 - Implement database vulnerability scanning in accordance with SBA and NIST requirements and maintain documentation to evidence the scans.

SBA Response – SBA concurs. SBA will implement credentialed database vulnerability and configuration scanning with Tenable for on-premises and cloud-hosted databases and will use Wiz to assess cloud-managed database services for vulnerabilities and misconfigurations. Scan results will be ingested into ServiceNow USEM and associated with database configuration items in the CMDB to assign ownership and track remediation against SBA timelines. Scan schedules, results, and remediation evidence will be retained in ServiceNow and linked to each system's authorization record in CAM to show compliance with SBA policy and NIST SP 800-53 RA-5.

Recommendation 5 - Continue to implement procedures to remediate all existing configuration baseline failures within SBA systems. Ensure ongoing enforcement by continuous monitoring to detect drift from authorized baselines, while regularly reviewing and maintaining historical remediation documentation to ensure adherence to NIST Risk Management Framework controls.

SBA Response – SBA concurs. SBA will continue to remediate existing configuration baseline failures and will enforce approved baselines using Tenable compliance audits against CIS and DISA STIG benchmarks for servers and databases, Wiz for cloud configuration posture, and Microsoft Intune for endpoint configuration enforcement. ServiceNow CMDB, Discovery, and Change Management will be used to maintain authorized baselines and detect unauthorized drift in

line with NIST SP 800-128. Baseline failures will be tracked to closure in ServiceNow USEM, with historical remediation records retained as evidence in CAM to support continuous monitoring under the NIST Risk Management Framework.

Recommendation 6 - Implement a formalized root cause analysis process for identified deficiencies. Establish and continuously enforce strict remediation milestones to track, manage, and definitively resolve the underlying systemic failures leading to findings.

SBA Response – SBA concurs. SBA will establish a formal root cause analysis procedure in ServiceNow so that deficiencies identified through OIG audits, security assessments, penetration testing, and Horizon3.ai validation testing are analyzed for underlying systemic causes. Each finding will be linked to a POA&M in ServiceNow CAM with defined milestones, owners, and due dates, and remediation will be tracked in ServiceNow USEM. Progress will be enforced through weekly remediation burndown reviews, monthly performance metrics, and quarterly executive governance, with recurring systemic issues escalated through the CISO Dashboard.

Recommendation 7 - Review and remediate session termination configurations for all information systems to ensure inactivity timeout settings comply with SBA policies..

SBA Response – SBA concurs. SBA will review session termination settings across all information systems, beginning with IS, UCP, NEXUS, and RelOneGov, and remediate any settings that do not meet SBA policy. Inactivity timeouts will be enforced centrally where possible through Ping Identity and Microsoft Entra ID session policies and Conditional Access, Microsoft Intune device lock policies, and Delinea session controls for privileged access. Compliance will be verified through Tenable and Wiz configuration checks, and any noncompliant systems will be documented and tracked to closure as POA&Ms in ServiceNow CAM.

Recommendation 8 - Implement and enforce a process to document, approve, and retain evidence of privileged user access requests prior to granting system access, ensuring privileged access is appropriately authorized, traceable, and supported by management oversight.

SBA Response – SBA concurs. SBA will implement a standardized privileged access request workflow in ServiceNow that requires documented business justification and approval by the supervisor, system owner, and ISSO before access is provisioned. Approved privileged access will be granted through IdAM, which provides credential vaulting, just-in-time elevation, and session recording, with role assignments managed through Ping Identity and Microsoft Entra ID groups. Request, approval, and provisioning records will be retained in ServiceNow as audit evidence, and privileged accounts will be recertified on a recurring basis.

Recommendation 9 - Define a process to implement a workforce assessment program to determine the skills, knowledge, and abilities of SBA's workforce to provide specialized security training within the functional areas of govern, identify, protect, detect, respond, and recover.

SBA Response – SBA concurs. SBA will define and implement a cybersecurity workforce assessment process aligned with the NICE Workforce Framework for Cybersecurity (NIST SP 800-181) to assess the knowledge, skills, and abilities of personnel with significant security

responsibilities across the govern, identify, protect, detect, respond, and recover functions. Results from the assessment, along with lessons learned from Purple Team exercises, penetration testing, and incident response activities, will be used to identify skill gaps and assign role-based training. Specialized training will include vendor training for SBA's security tools (including SentinelOne, Wiz, Tenable, Zscaler, and ServiceNow) and CISA-provided resources, with completion tracked and reported annually.

Recommendation 10 - Review and update the SBA COOP, which includes the organizational BIA, on an annual basis.

SBA Response – SBA concurs. Through the Enterprise IT Continuity of Operations (IT COOP) program, SBA will review and update the COOP plan and organizational Business Impact Analysis (BIA) at least annually and after significant changes. The BIA will map each Mission Essential Function (MEF) to its supporting systems, data, personnel, vendors, and recovery time and recovery point objectives, using ServiceNow CMDB service relationships to identify system dependencies. Updates will be coordinated with ISSOs and the CFO continuity office, aligned with system contingency plans, and the approved versions will be retained as evidence in ServiceNow CAM.

Recommendation 11 - Fully exercise the COOP to include all MEFs, in accordance with Federal requirements.

SBA Response – SBA concurs. SBA will conduct an annual COOP exercise that covers all MEFs in accordance with Federal Continuity Directives 1 and 2, including the FY2026 assessment of the AWS migration as an exercise event.

Exercises will validate recovery of critical systems and supporting capabilities, including identity services (Ping Identity, Microsoft Entra ID, and Delinea), security monitoring through SentinelOne, and secure remote access through Zscaler. Each exercise will produce an after-action report, and corrective actions will be tracked to closure as POA&Ms in ServiceNow.

DOUGLAS ROBERTSON

Digitally signed by DOUGLAS ROBERTSON
Date: 2026.10.08 18:04:48 -04'00'

Douglas Robertson
Alternate Authorizing Official
Deputy Chief Information Officer
Small Business Administration (SBA)