

FISCAL YEAR 2022 FEDERAL INFORMATION SECURITY MODERNIZATION ACT REVIEW

Report 23-03 | December 13, 2022





EXECUTIVE SUMMARY

FISCAL YEAR 2022 FEDERAL INFORMATION SECURITY MODERNIZATION ACT REVIEW

Report 23-03

December
13, 2022

What OIG Reviewed

This report summarizes the results of our fiscal year (FY) 2022 Federal Information Security Modernization Act (FISMA) evaluation and assesses the maturity of controls used to address risks in each of the nine information security areas, called domains.

Our objectives were to determine whether the U.S. Small Business Administration (SBA) complied with FISMA and assess the maturity of controls used to address risks in each of the nine security domains.

We assessed the maturity of SBA's information security program as outlined in the FY 2022 Inspector General FISMA Reporting Metrics issued by the Office of Management and Budget. OIG contracted with KPMG LLP, an independent public accounting firm, to test a subset of systems and security controls and assess SBA's adherence to FISMA requirements.

What OIG Found

We assessed the effectiveness of information security programs on the required maturity model spectrum, which is a rating scale for information security. We rated SBA's overall program of information security as "not effective." We found SBA generally responded to previously identified vulnerabilities. The agency made progress in supply chain risk management and continues to be rated at the effective maturity level for incident response. However, the results of our tests show SBA continues to experience security control challenges in areas of configuration management, risk management, user access, security training, information security continuous monitoring, and contingency planning.

Based on tests of seven information systems, we determined the results of each domain as follows:

1. Risk management: Defined
2. Supply chain risk management: Defined
3. Configuration management: Defined
4. Identity and access management: Defined
5. Data protection and privacy: Consistently implemented
6. Security training: Ad hoc
7. Information security continuous monitoring: Consistently implemented
8. Incident response: Managed and measurable
9. Contingency planning: Consistently implemented

Ratings of defined, ad hoc, and consistently implemented are below the baseline for an effective security program.

OIG Recommendations

In addition to two open FISMA recommendations in Appendix II from prior years, we made six recommendations for improvements in six of the nine domains: risk management, supply chain risk management, identity and access management, information system continuous monitoring, security training, and contingency planning. We did not repeat outstanding recommendations in the areas of risk management and configuration management, or have recommendations in the domains of data protection and privacy and incident response.


Agency Comments

SBA management agreed with all six recommendations and outlined corrective action plans to address identified vulnerabilities. We consider these recommendations resolved.



Office of Inspector General

U.S. Small Business Administration

DATE: December 13, 2022
TO: Isabella Casillas Guzman
Administrator
FROM: Hannibal "Mike" Ware 
Inspector General
SUBJECT: Evaluation of Fiscal Year 2022 Federal Information Security Modernization Act Review

I am pleased to present the results of our evaluation on information security weaknesses, *FY 2022 Federal Information Security Modernization Act Review*. SBA Management agreed with all six of our recommendations.

We appreciate the cooperation and courtesies your staff continues to show us as we work together to combat waste, fraud, and abuse in SBA. If you have any questions or need additional information, please contact me or Andrea Deadwyler, Assistant Inspector General for Audits, at (202) 205-6586.

cc: Arthur Plews, Chief of Staff
Elias Hernandez, Acting Chief Operating Officer
Steve Kucharski, Acting Chief Information Officer
Therese Meers, General Counsel
Kate Aaby, Associate Administrator, Office of Performance, Planning, and the Chief Financial Officer
Erica Gaddy, Deputy Chief Financial Officer, Office of Performance, Planning, and the Chief Financial Officer
Patrick Kelley, Associate Administrator, Office of Capital Access
John Miller, Deputy Associate Administrator, Office of Capital Access
Bailey DeVries, Associate Administrator, Office of Investment and Innovation
Michele Schimpp, Deputy Associate Administrator, Office of Investment and Innovation
Beatrice Hidalgo, Associate Administrator, Office of Government Contracting and Business Development
Antonio Doss, Deputy Associate Administrator, Office of Government Contracting and Business Development
Michael Simmons, Attorney Advisor, Office of General Counsel
Joshua Barnes, Recovery Director, Office of Disaster Assistance
Tonia Butler, Director, Office of Internal Controls

Table of Contents

Introduction.....	1
Background.....	1
Objectives.....	2
Results.....	3
Challenges and Improvements.....	3
Domain Test Results.....	4
I. Risk Management	4
Recommendation	5
II. Supply Chain Risk Management	5
Recommendation	5
III. Configuration Management.....	5
IV. Identity and Access Management.....	6
Recommendation	6
V. Security Training.....	7
Recommendation	7
VI. Information Security Continuous Monitoring.....	7
Recommendation	8
VII. Contingency Planning	8
Recommendation	8
Analysis of Agency Response.....	9
Recommendation 1.....	9
Recommendation 2.....	9
Recommendation 3.....	9
Recommendation 4.....	10
Recommendation 5.....	10
Recommendation 6.....	10
Appendix I: Objective, Scope, and Methodology.....	11
Maturity Levels.....	11
Prior Work.....	11
Appendix II: Open IT Security Recommendations Related to FISMA	13
Appendix III: Assessment Maturity Level Definitions.....	14
Appendix IV: Management Response.....	15

Introduction

The Federal Information Security Modernization Act (FISMA) requires each Office of Inspector General, or an independent external auditor, independently evaluate the effectiveness of the information security program and practices of its agency¹. The Act also requires agencies to report annually to the Office of Management and Budget (OMB), Congress, and the Government Accountability Office (GAO) on the adequacy and effectiveness of their information security policies, procedures, and practices².

This report summarizes the results of our fiscal year (FY) 2022 evaluation of the U.S. Small Business Administration's (SBA) information technology (IT) systems. The purpose of this report is to assess the effectiveness, or maturity, of the controls used to address risks in each of the required review areas, referred to as domains.

The Office of Inspector General (OIG) contracted with KPMG LLP, an independent public accounting firm, for our FY 2022 FISMA evaluation. KPMG tested a representative subset of SBA systems and security controls and assessed SBA's adherence to or progress in implementing minimum security standards and requirements appropriate for each system's security categorization and risk. OIG monitored KPMG's work and reported SBA's compliance with FISMA through the FISMA CyberScope submission in August 2022.

Background

In FY 2022, OMB made significant changes to the FISMA oversight and metrics collection. These changes are intended to initiate improved quality of performance data collected at the enterprise level and accelerate efforts to make more informed risk-based decisions. These revisions further required the Inspector General FISMA evaluation be completed in July rather than October and focused on a reduced core set of 20 metrics with supplemental metrics.

Each Office of Inspector General is required to assess the effectiveness of information security programs on a maturity model spectrum. The levels of this spectrum ensure sound practices, and the ratings capture the agency's proficiency with its policies and procedures.

For FY 2022, OIG is required to assess the effectiveness of the following nine domains:

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

¹ IAW 44 USC § 3555(a).

² Public Law 113-283 § 35549(c)(1)(a).

OIG contracted with KPMG LLP to perform SBA's FY 2022 FISMA evaluation. KPMG sampled and tested a representative subset of seven SBA systems.

The current benchmark for an effective program within the context of the maturity model is level 4, managed and measurable. In the maturity model, domain performance that scores below the level of managed and measurable, such as ad hoc, defined, or consistently implemented, means IT security is "not effective."

KPMG's evaluation of core metrics across the nine domains indicated that SBA continued to achieve level 4 in the area of incident response but is at level 1, ad hoc; level 2, defined; or level 3, consistently implemented in the remaining eight areas. The maturity model criteria places SBA at an overall level of "not effective."

As outlined in Appendix I, KPMG tested 20 FISMA metrics using a representative subset of SBA systems and security controls. We used the test results from this evaluation to assess SBA's adherence to and progress in implementing minimum security standards and requirements for each system's security categorization and risk.

Objectives

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

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

Results

We rated SBA's overall cybersecurity as "not effective" in FY 2022 because only one of the nine domains was ranked as managed and measurable. In the maturity model, domain performance scores below managed and measurable (such as ad hoc, defined, or consistently implemented) means IT security is ineffective. For a definition of each maturity level rating, see Appendix II.

Ratings in the nine domains are determined by a simple majority, where the most frequent level across the questions will serve as the domain rating. For example, to maintain a rating of managed and measurable in a domain that has two questions, at least one of the two metric questions must earn the managed and measurable rating.

Each domain is scored on a numerical scale of 1 (worst) to 5 (best). If a metric testing result identified a control area requiring improvement, we determined the impact of control deficiencies and whether a recommendation was needed. In most cases, this occurred when a policy or procedure was established but not consistently implemented.

Using the criteria in federal guidance, outlined in Appendix II, we ranked SBA's IT security domains as follows:

1. Risk management: Defined
2. Supply chain risk management: Defined
3. Configuration management: Defined
4. Identity and access management: Defined
5. Data protection and privacy: Consistently implemented
6. Security training: Ad hoc
7. Information security continuous monitoring: Consistently implemented
8. Incident response: Managed and measurable
9. Contingency planning: Consistently implemented

In our analysis of domain test results below, outstanding recommendations in risk management and configuration management are not repeated in this report (Appendix 1). We also did not have findings in the areas of data protection and privacy and incident response, and therefore do not discuss those areas in this report.

Challenges and Improvements

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

1. Configuration management
2. User access
3. Security training
4. Information security continuous monitoring
5. Contingency planning

Domain Test Results

The following section details the testing results of the domains. The data protection and privacy and incident response domains are omitted from this report because we had no findings. Each section outlines the scope of the review, test results, and recommendations for improvement.

I. Risk Management

Risk management focuses on policies and actions that manage information security risks to the organization. We determined that SBA's risk management maturity level was "defined." For a definition of the defined maturity level, see Appendix II. SBA can improve security in this domain by resolving the following vulnerabilities:

System Software Inventory

FISMA requires agencies to maintain a comprehensive and accurate inventory of its information systems to include third-party systems. SBA did not consistently maintain an up-to-date listing of software assets connected to SBA's network.

Agency management stated that a lack of resources has not allowed them to implement a process to track software inventories.

The FY 2022 Core Inspector General FISMA Reporting Metrics³ states having an agency wide software asset management capability in place is considered an effective level of security. Accurate inventory tools are needed to provide oversight and visibility to all systems. An inventory update process is also needed to maintain up-to-date software configurations and prevent unauthorized software from being installed. The recommendation for this finding was previously identified in OIG Report 22-11, *Fiscal Year 2021 Federal Information Security Modernization Act Review*, and has not been closed by the agency. Therefore, there is no recommendation for this finding in this report.

Hardware Asset Inventory

FISMA requires agencies to maintain a comprehensive and accurate inventory of its hardware assets to include third-party systems⁴. While SBA has established a process to maintain an inventory of its hardware assets connected to its network, the process does not capture a complete and accurate inventory that is necessary for tracking, reporting, and approval.

The FY 2022 Inspector General FISMA Reporting Metrics states having an agency wide hardware asset management capability in place is considered an effective level of security. Agency management stated that a lack of resources has not allowed them to implement a process to fully track hardware assets. Without a fully established process in place, SBA may not be able to assess and manage cybersecurity risks or known vulnerabilities of its hardware software assets. Thus, software and hardware assets such as databases and servers could be vulnerable to internal and external threats or attacks.

³ FY 2022 Core Inspector General FISMA Metrics Evaluation Guide (cisa.gov).

⁴ 44 USC 3505(c).

Recommendation

We recommend the Administrator direct the Office of the Chief Information Officer, in coordination with program offices, to

1. Design and implement a quality assurance program to ensure that SBA system hardware inventory is maintained as required by the National Institute of Standards and Technology (NIST) Special Publication 800-53.

II. Supply Chain Risk Management

Supply chain risk management focuses on the development, acquisition, and disposal of IT systems and services in accordance with federal security guidance. We determined the agency's supply chain risk management maturity level was "defined" and requires establishment of a process to review its supply chain risks. Definitions for the maturity levels can be found in Appendix II.

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

Review of Supply Chain Regarding Third Party Suppliers

In FY 2022, SBA established a supply chain risk management policy as required by federal criteria. However, we determined SBA did not include in this policy requirements that management review internal and third-party supply chain risks. NIST 800-53 Rev. 5 states organizations should consider their potential supply-chain risk when establishing a methodology for managing risk including that of external service providers.

The FY 2022 Core Inspector General FISMA Metrics Evaluation Guide states having qualitative and quantitative measures incorporated in policies and procedures to measure external providers as well as supplier risk assessments is considered an effective level of security. Not having a process in place to review supply chain risk management requirements increases the risk that the organization is unaware of the risks within their operating environment. This could impact the agency's ability to make decisions based on that risk.

Recommendation

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

2. Implement a process to ensure SBA reviews its external service providers for supply chain risks and ensure all assessments of supply chain risks are documented as outlined in NIST 800-53.

III. Configuration Management

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

Vulnerability Remediation Process

SBA did not reinforce its patch management guidelines to ensure that agency systems were properly configured and vulnerabilities remediated within specified timeframes, as

required by SBA Standard Operating Procedure (SOP) 90 47 6, Cybersecurity and Privacy Policy.

Software version control and vulnerability testing is a continuous process. SBA's existing remediation process should prioritize criticality, timeliness, and communication of issues to accountable parties.

The FY 2022 Core Inspector General FISMA Metrics Evaluation Guide states that an automated flaw remediation process and prioritization of flaw remediation based on risk are considered an effective level of security. If SBA does not promptly make security updates when they become available, there is an increased risk that the confidentiality, integrity, and availability of the data residing on information systems will be compromised. There is also an increased risk that existing or new vulnerabilities could expose information systems and applications to attacks, unauthorized modification, or compromised data. The recommendation for this finding was previously identified in OIG Report 22-11, *Fiscal Year 2021 Federal Information Security Modernization Act Review*, and has not been closed by the agency; therefore, there is no recommendation for this finding in this report.

IV. Identity and Access Management

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

User Accounts Authorizations and Terminations

SBA did not reauthorize users in one of its systems, a high value asset system. The last review was completed in January 2021. A high value asset is an information system that is critical to an organization's ability to perform its mission or conduct business. The reauthorization process is needed to ensure appropriate user security protections are in place or sensitive data contained within. SOP 90 47 6 requires users to be recertified annually to ensure the continued need for access to the system and to verify a user's access privileges.

The FY 2022 Core Inspector General FISMA Reporting Metrics states automated processes including the automatic removal/disabling of accounts are controls needed for an effective level of security. The agency stated that due to competing priorities, a review had not been completed annually as required. Not recertifying users could lead to inappropriate access being retained for personnel who have left the agency or no longer require access to the system.

Recommendation

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

3. Communicate and reinforce to program offices the requirement to review and remove system and user accounts in accordance with SOP 90 47 6.

V. Security Training

The security training domain requires system users have the proper IT training relevant to their IT security role and to the system. We determined that domain's maturity level was "ad hoc" because procedures are done in a reactionary manner. The definition for the ad hoc maturity level can be found in Appendix II. This domain can be improved by resolving the following vulnerability.

Formal Workforce Assessment

SBA has not updated its policies and procedures to include conducting a formal workforce assessment. This assessment reviews the skills, knowledge, and abilities of SBA's workforce to identify training needs and knowledge gaps among its IT staff.

The Federal Cybersecurity Workforce Assessment Act⁵ requires agencies develop procedures to identify the personnel with IT or cybersecurity responsibilities and create a strategy to resolve any identified knowledge or training gaps identified. SBA management decided to perform alternate procedures instead of conducting a formal workforce assessment.

The FY 2022 Inspector General FISMA Reporting Metrics defines an effective level of security as the agency providing documentary evidence that it has made progress in addressing workforce assessment gaps. By not including a formal workforce assessment as required, SBA risks not updating its security awareness and training strategy to enhance its personnel's knowledge to security threats.

Recommendation

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

4. Update the policies and procedures to conduct a formal workforce assessment as required under the Federal Cybersecurity Workforce Assessment Act of 2015.

VI. Information Security Continuous Monitoring

Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. We determined that the agency's maturity level was "consistently implemented." For the definition of consistently implemented, see Appendix II. This domain can be improved by resolving the following vulnerability.

Process of Information Security Continuous Monitoring Incomplete

SBA has not been able to show evidence that it has established processes to continuously monitor information security, nor a process to report findings based on a review. Specifically, we identified that while SBA has policies that require management to review its processes to ensure its ongoing authorization process is effective, the policy does not have specific requirements on how management is to review data and report findings. NIST 800-53 states organizations should establish a process for monitoring and reporting

⁵ Federal Cybersecurity Workforce Assessment Act of 2015.

control effectiveness, as well as addressing any results of this control monitoring assessment.

The FY 2022 Inspector General FISMA Reporting Metrics states the use of performance metrics, as well as the use of ongoing authorizations, are considered an effective level of security. SBA management may not be able identify and respond to information security threats, exposing SBA's information systems to compromise.

Recommendation

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

5. Develop, document, and implement a process that requires management review of information security data and report information security threats.

VII. Contingency Planning

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

Contingency Test Performed Not Appropriate for System

We found SBA had completed a tabletop exercise instead of a functional test for one of its systems, which is a high value asset.

SOP 90 47 6 states a high value asset system must have a functional test conducted, including failover testing, for contingency planning purposes. A functional test of a contingency plan requires assigned personnel to test simulations or scenarios to determine how effective the plan was in restoring operations. A tabletop exercise only requires personnel to meet and discuss how a contingency plan would be conducted.

The FY 2022 Inspector General FISMA Reporting Metrics states the use of automated processes to test contingency plans are considered an effective level of security. Due to the criticality of a high value asset, a properly documented contingency plan is important so that the system can be restored in an efficient and timely manner.

Recommendation

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

6. Ensure owners of high value asset systems carry out functional testing of contingency plans on an annual basis and initiate corrective actions as required by SOP 90 47 6.

Analysis of Agency Response

Summary of Actions Necessary to Close the Report

SBA management concurred with the six recommendations in the draft report. The status of our recommendations and actions necessary to close them are as follows:

Recommendation 1

Design and implement a quality assurance program to ensure that SBA system hardware inventory is maintained as required by the National Institute of Standards and Technology (NIST) Special Publication 800-53.

Status: Resolved

SBA management agreed with this recommendation and stated they will improve their capability to track hardware inventory more accurately and comprehensively. In subsequent correspondence, management further stated the agency plans to implement a software platform in FY 2023 that will provide compliance automation with updates for SBA's FISMA systems. SBA managers intend to complete final action on this recommendation by August 11, 2023. This recommendation can be closed when SBA management provides evidence that the agency has established a quality assurance program that effectively ensures system hardware inventory is maintained as required by the NIST Special Publication 800-53.

Recommendation 2

Implement a process to ensure SBA reviews its external service providers for supply chain risks and ensure all assessments of supply chain risks are documented as outlined in NIST 800-53.

Status: Resolved

SBA management agreed with this recommendation and stated they will provide the acquisitions organization with standardized cyber language for IT investments that can be incorporated into acquisition requirement documents. Management intends to complete final action on this recommendation by May 26, 2023. This recommendation can be closed when SBA management provides evidence SBA reviews its external service providers for supply chain risks and ensures assessments of supply chain risks are documented as outlined in NIST 800-53.

Recommendation 3

Communicate and reinforce to program offices the requirement to review and remove system and user accounts in accordance with SOP 90 47 6.

Status: Resolved

SBA management agreed with this recommendation and stated they plan to procure and implement a software platform that will provide automated communication to stakeholders with approval workflows for the user recertifications process for FISMA systems. Management intends to complete final action on this recommendation by August 11, 2023. This recommendation can be closed when SBA management provides evidence

the automated communication is working and that they have communicated and reinforced to program offices the requirement to review and remove system and user accounts in accordance with SOP 90 47 6.

Recommendation 4

Update the policies and procedures to conduct a formal workforce assessment as required under the Federal Cybersecurity Workforce Assessment Act of 2015.

Status: Resolved

SBA management agreed with this recommendation and stated they plan to conduct a formal cybersecurity workforce assessment in FY23 to identify any gaps in skills and/or training for any IT personnel with a role in cybersecurity. Management intends to complete final action on this recommendation by July 28, 2023. This recommendation can be closed when SBA management provides evidence that they have updated the policies and procedures to conduct a formal workforce assessment as required under the Federal Cybersecurity Workforce Assessment Act of 2015.

Recommendation 5

Develop, document, and implement a process that requires management review of information security data and report information security threats.

Status: Resolved

SBA management agreed with this recommendation and stated they plan to purchase and implement a risk management software that will provide automated continuous monitoring capability of information security threats and compliance statuses for FISMA systems. Management intends to complete final action on this recommendation by August 11, 2023. This recommendation can be closed when SBA management provides evidence that the agency has developed, documented, and implemented a process that requires management review of information security data and report information security threats.

Recommendation 6

Ensure owners of high value asset systems carry out functional testing of contingency plans on an annual basis and initiate corrective actions as required by SOP 90 47 6.

Status: Resolved

SBA management agreed with this recommendation and stated they will ensure owners of high value assets carry out functional testing of their contingency plan on an annual basis and initiate corrective actions if required. Management intends to complete final action on this recommendation by August 25, 2023. This recommendation can be closed when SBA management provides evidence that the agency is ensuring high value asset system owners carry out annual contingency plan functional testing and initiate corrective actions as required by SOP 90 47 6.

Appendix I: Objective, Scope, and Methodology

Our objectives were to determine whether SBA complied with FISMA in 2022 and assess the maturity of controls used to address risks in each of the nine domains reported to the U.S. Department of Homeland Security (DHS) CyberScope system, as follows:

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

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

We hired KPMG LLP, an independent public accounting firm, for our FY 2022 FISMA evaluation. KPMG tested a representative subset of SBA systems and security controls and assessed SBA's adherence to or progress in implementing minimum security standards and requirements appropriate for each system's security categorization and risk.

KPMG also performed vulnerability scanning of SBA's network environment. OIG monitored KPMG's work and reported SBA's compliance with FISMA to DHS's CyberScope application in August 2022.

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

Maturity Levels

The FY 2022 Core Inspector General FISMA Metrics Evaluation Guide, issued in May 2022, was developed as a collaborative effort among the Office of Management and Budget, DHS, and the Council of the Inspectors General on Integrity and Efficiency in consultation with the Federal Chief Information Officer Council.

The metrics are a continuation of work begun in FY 2016, when the metrics were aligned with the five function areas in the NIST Cybersecurity Framework: identify, protect, detect, respond, and recover.

Prior Work

OIG reviews information technology security through the annual financial statement audit as well as the annual FISMA evaluation. Our recent reports include the *Independent Auditors' Report on SBA's FY 2021 Financial Statements*, Report 22-05, November 15, 2021;

and *FY 2020 Federal Information Security Modernization Act Review*, Report 21-17, July 6, 2021. We also issued *COVID-19 and Disaster Assistance Information Systems Security Controls*, Report 22-19, September 27, 2022.

Appendix II: Open IT Security Recommendations Related to FISMA

There are two open audit recommendations that directly affect SBA's CyberScope evaluation as it relates to Federal Information Security Modernization Act (FISMA) compliance. The recommendations below were identified in fiscal year 2021. FISMA results were included in Report 22-11 issued April 28, 2022.

Risk Management

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

OIG Report 22-11, Recommendation 1: Design and implement a quality assurance program to ensure that SBA system software inventory and contractor managed systems are maintained, as required by the National Institute of Standards and Technology (NIST) Special Publication 800-53.

Configuration Management

FISMA requires that organizations develop minimally acceptable system configuration requirements to ensure a baseline level of security for information technology operations and assets. Our past audits and reviews identified weaknesses in the development of baseline configurations and other configuration-related controls. To address these weaknesses, we made this recommendation to SBA:

OIG Report 22-11, Recommendation 5: Ensure systems under control undergo vulnerability scans and address identified vulnerabilities as part of the patch management process, as required by SOP 90 47 5.

Appendix III: Assessment Maturity Level Definitions

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

Maturity Level	Rating	Definition
Level 1	Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad hoc, reactive manner
Level 2	Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented
Level 3	Consistently implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking
Level 4	Managed and measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes
Level 5	Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business or mission needs

Source: FY 2021 Inspector General FISMA of 2014 Reporting Metrics, Version 1.1, May 12, 2021

Level 4, managed and measurable, is considered to be an effective level of security at the domain, function, and overall program level. Ratings throughout the nine domains are calculated based on a simple majority, where the most frequent level across the questions serves as the domain rating.

Appendix IV: Management Response

SBA Response to Evaluation Report



U.S. Small Business
Administration

Office of the Chief Information Officer

Memo for: Hannibal Ware
Inspector General

From: Kelvin Moore
Chief Information Security
Officer (CISO)

Subject: Management Response:
Evaluation FY 2022 Federal Information Security
Modernization Act Review, Project 22014

Date: December 2, 2022

We appreciate the opportunity to review the draft report entitled “Evaluation FY 2022 Federal Information Security Modernization Act Review.” The SBA built, delivers, and continues to mature resilient and robust Enterprise Cybersecurity Service (ECS) capabilities that can be consistently implemented, maintained, and leveraged throughout the agency. These ECS capabilities ensure the SBA is well-positioned to align to executive branch goals such as the FY2022 Chief Information Officer (CIO) Metrics, Zero Trust initiatives and the Executive Order (EO) 14028 priorities, as well as enabling the SBA to rapidly respond to recent well-publicized global cyber events with minimal impact and no indications of compromise.

The Office of the CIO has the following comments with respect to the recommendations:

Recommendation 1: The SBA agrees. The SBA will improve its capability to track its hardware inventory more accurately and comprehensively, enabling automation to the greatest extent possible, for internal and contractor-operated systems and services for FISMA systems.

Recommendation 2: The SBA agrees. The SBA will provide the acquisitions organization with standardized cyber language for IT investments that can be incorporated into acquisition requirement documents. This language includes requirements to offerors for pre-award attestation of supply chain risk management, transparency of downstream supply chain dependencies, and notification of potential supply chain compromises.

Recommendation 3: The SBA agrees. The SBA plans to procure and implement a Cyber Risk Management Platform that will provide automation, communication to stakeholders with approval workflows for the user re-certifications process for FISMA systems.

Recommendation 4: The SBA agrees. The SBA plans to conduct a formal cybersecurity workforce assessment in FY23 to identify any gaps in skills and/or training for any IT personnel with a role in cybersecurity.

Recommendation 5: The SBA agrees. The SBA plans to purchase and implement a Cyber Risk Management Tool in FY23. The CRM tool will provide automation for the agency and a continuous monitoring capability that will provide information security threats and compliance status for FISMA systems.

Recommendation 6: The SBA agrees. The SBA will ensure owners of High Value Assets (HVA) carry out functional testing of their contingency plan on an annual basis and initiate corrective actions if required.