SBA INSPECTOR GENERAL EVALUATION REPORT

Fiscal Year 2021 Federal Information Security Modernization Act Review

Report 22-11 | April 28, 2022

Executive Summary

Fiscal Year 2021 Federal Information Security Modernization Act Review

Report 22-11

April 28, 2022

What OIG Reviewed

This report summarizes the results of our fiscal year (FY) 2021 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 2021 Inspector General FISMA Reporting Metrics issued by the Office of Management and Budget. We tested a subset of eight SBA systems against these metrics and evaluated them against guidance in the FISMA metrics.

What OIG Found

Inspectors General are required to assess the effectiveness of information security programs on a maturity model spectrum, which is a rating scale for information security. We rated SBA's overall program of information security as "not effective." SBA achieved the maturity level rating of "managed and measurable" in only one of the nine domains. For the security program to be rated as effective, the agency needs to earn managed and measurable ratings in a majority of the domains.

In FY 2021, SBA continued to have an unprecedented volume of loan and grant applications because of the Coronavirus Aid, Relief, and Economic Security Act and other pandemic-related legislation. As a result, the agency continued to experience security challenges. Based on tests of the eight information systems, we determined the results of each domain as follows:

- Risk management: Consistently implemented
- Supply chain risk management: Ad hoc
- Configuration management: Defined
- Identity and access management: Consistently implemented
- Data protection and privacy: Consistently implemented
- Security training: Consistently implemented
- Information security continuous monitoring: Defined
- Incident response: Managed and measurable
- Contingency planning: Consistently implemented

Managed and measurable means the security area has been rated as effective. Ratings of defined, ad hoc, or consistently implemented are below the baseline for an effective security program.

OIG Recommendations

We made a total of 10 recommendations for improvements in 5 of the 9 domains, as follows: risk management, supply chain risk management, configuration management, identity and access management, and contingency planning. We made three recommendations in risk management, configuration management, and identity and access management to address conditions identified last year. We did not have new findings for the data protection and privacy, information system continuous monitoring, security response, and incident response domains and did not report on those areas.

Agency Comments

SBA provided written responses that were considered in finalizing the report. SBA management agreed with all the recommendations in this report.

Office of Inspector General

U.S. Small Business Administration

DATE: April 28, 2022

TO: Isabella Casillas Guzman
Administrator

FROM: Hannibal "Mike" Ware
Inspector General

SUBJECT: *Fiscal Year 2021 Federal Information Security Modernization Act Review*

I am pleased to present the results of our evaluation on information security weaknesses, *FY 2021 Federal Information Security Modernization Act Review*. Management agreed with all 10 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 please contact me or Andrea Deadwyler, Assistant Inspector General for Audit, at (202) 205-6586.

cc: Antwaun Griffin, Chief of Staff
Arthur Plews, Deputy Chief of Staff
Stephen Kong, Acting Chief Operating Officer
Luis Campudoni, Acting Chief Information Officer
Peggy Delinois Hamilton, 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
Therese Meers, Deputy Associate Administrator, Office of Capital Access
Michael A. Simmons, Attorney Advisor, Office of General Counsel
Joshua Barns, Acting Director, Office of Continuous Operations and Risk Management
Tonia Butler, Director, Office of Internal Controls

Table of Contents

Introduction 1

Background 1

Objectives 2

Results 3

Domain Test Results 3

I. Risk Management 3

Recommendations 4

II. Supply Chain Risk Management 4

Recommendation 5

III. Configuration Management 5

Recommendations 6

IV. Identity and Access Management 6

Recommendations 7

V. Contingency Planning 8

Business Impact Assessment Incomplete 8

Recommendation 8

Analysis of Agency Response 9

Summary of Actions Necessary to Close the Report 9

Appendix I: Objective, Scope, and Methodology 12

Maturity Levels 12

Prior Work 12

Appendix II: Assessment Maturity Level Definitions 13

Appendix III: Management Response 14

Introduction

The Federal Information Security Modernization Act (FISMA) requires each agency Office of Inspector General or an independent external auditor to independently evaluate the effectiveness of the information security program and practices of its agency.

This report summarizes the results of our fiscal year (FY) 2021 evaluation of SBA's information technology (IT) systems. The purpose of this report is to assesses the effectiveness, or maturity, of the controls used to address risks in each of the required review areas, referred to as domains.

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

Background

FISMA requires federal agencies to develop and maintain an agency-wide information security program. 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 practices.

Each agency 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.

OMB and the Department of Homeland Security issue the annual FISMA metric guidance. Each Inspector General's office uses the FISMA metrics to evaluate its agency's information security programs.

SBA Office of Inspector General hired KPMG LLP, an independent public accounting firm, to perform SBA's FY 2021 FISMA evaluation. KPMG sampled and tested a representative subset of eight SBA systems.

For fiscal year 2021, the Office of Inspector General 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

In response to the Federal Acquisition Supply Chain Security Act of 2018, OMB and the Department of Homeland Security added supply chain risk management as a new domain in FY 2021. Supply chain risk management focuses on strengthening federal agencies' policies and ensuring procedures are consistent with their organization's cybersecurity and supply chain risk management requirements. For the FY 2021 FISMA metric guidance, inspectors general were instructed not to include their assessment rating score of supply chain risk management in their agency's overall information security maturity levels.

We used the test results 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: risk management, supply chain risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

Results

We rated SBA's overall cybersecurity as not effective in FY 2021 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.

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 seven questions, four of the seven metric questions must earn the high managed and measurable rating.

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

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

We did not have new findings for the data protection and privacy, information system continuous monitoring, security training, and incident response domains and did not report on those areas.

Challenges and Improvements

In FY 2021, SBA continued to face significant security challenges in carrying out the requirements of the pandemic relief programs. SBA needs to update and implement security operating procedures and address newly identified vulnerabilities in its systems. We identified that control improvements are needed in system software inventory management, patching, user recertification, and in deployment of a comprehensive supply chain risk management policy.

Domain Test Results

The following sections detail the testing results of the domains required to be monitored under FISMA. Each section outlines the scope of the review, test results, and recommendations for improvement.

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 "consistently implemented." Federal agencies are required to consistently implement their security architecture across the enterprise, business process, and system levels. SBA can improve security in this domain by resolving the following issues:

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. This issue was identified during the previous year's testing of inventory controls.

Agency management stated in response to last year's recommendation that the controls were enhanced to include an improved inventory update process. However, testing of this area showed a continued lack of documentation and support for the reported systems inventory.

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.

Testing of Continuity of Operations Plan

We found SBA did not test its continuity of operations plans for FY 2021. Federal Continuity Directive 1 requires enterprise continuity of operations plans to be tested annually and updated accordingly. The organization should document this assessment in its risk register, as stated in the FY 2021 Inspector General FISMA Reporting Metrics.

SBA did not test its continuity of operations plan for FY 2021 and may not be aware of risks such as incomplete recovery efforts. That means the agency may not be able to quickly restore operations after a disaster.

Recommendations

We recommend that 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 software inventory and contractor managed systems are maintained, as required by the National Institute of Standards and Technology (NIST) Special Publication 800-53.
2. Ensure the continuity of operations plan is tested annually, as required by Federal Continuity Directive 1.

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 "ad hoc" and requires establishment of polices.

As previously noted, we assessed but did not include supply chain risk management in the calculated metrics for the overall maturity model. Supply chain risk management domain can be improved through the resolution of the following areas:

Development of an Agency-wide Supply Chain Policy

We determined that SBA did not establish a supply-chain risk-management policy agency-wide. SBA managers stated they are in the process of determining procedures as recommended by NIST 800-53. NIST asks organizations to consider their potential supply-chain risk when establishing a methodology for managing risk.

An agency supply chain policy should consider the agency's risk management processes, high value assets, configuration management, continuous monitoring, and inventory management.

Recommendation

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

3. Implement an agency-wide policy for the management of supply-chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. This policy should address key controls outlined in NIST 800-53, such as the procurement of third-party services, high-value asset identification, and counterfeit component prevention.

Configuration Management

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

Remediation of Baseline Scans

We determined that SBA's vulnerability process does not define a timeline for resolving failed baseline and compliance scans. NIST 800-53 states that vulnerabilities should be fixed within a timeframe developed by the agency. Compliance scans are used to ensure configuration settings in a system adhere to a baseline framework agreed to by agency management.

To improve this area, SBA needs to implement the provisions of 800-53 that require specific timeframes for remediation of the vulnerability. When systems owners don't prioritize such vulnerabilities and commit to timeframes for correction, they risk potential compromise of sensitive information.

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 5 Cybersecurity and Privacy Policy. SBA also did not ensure one system was regularly scanned for vulnerabilities as required by SBA 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.

We had identified patch management as a weakness during testing of vulnerability remediation controls last year. Officials in the Office of the Chief Information Officer stated in their response to last year's recommendation that steps were taken to improve patch and vulnerability management process. The officials said the agency used several risk-response techniques, continuous monitoring and measurement, risk mitigation, risk acceptance, and consideration of compensating controls.

The FY 2021 Inspector General FISMA Reporting Metrics states that a centrally managed remediation process for patch management is considered an effective level of security. If SBA does not promptly make security updates when they become available, there is an increased risk the confidentiality, integrity, and availability of the data residing on information systems could 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.

Recommendations

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

4. Ensure timelines are incorporated into policies requiring baseline scan vulnerabilities be remediated in a timely manner. Also, ensure these vulnerabilities are tracked appropriately through the Plan of Action and Milestones process as required by NIST 800-53.

In addition, we recommend that the Administrator direct the Office of Capital Access along with the Office of the Chief Information Officer to

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.

Identity and Access Management

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

User Accounts Authorizations and Terminations

Management could not provide evidence that new user access had been properly authorized for three systems we reviewed. We found management had not terminated the account of an administrator for one system within 30 days of the person leaving the agency.

We also identified this issue of ineffective user-account controls during our testing of access controls last year. The agency stated in response to last year's recommendation that the controls were enhanced to improve the access authorization process and continuous monitoring of authorized accounts.

SOP 90 47 5 states that information security must be managed properly for all activities, such as activating, modifying, reviewing, disabling, and removing accounts. In addition, the use of automated mechanisms to manage and review user access is considered an effective level of security, as stated in the FY 2021 Inspector General FISMA Reporting Metrics.

SBA was not able to provide evidence that new user access was authorized, nor that access was terminated for users who had left the agency. Not managing the account access process for new and terminated users could lead SBA to potential loss or inappropriate disclosure of crucial data.

Audit logs of Administrator Activity

The two systems under contract by Office of Capital Access did not log administrator activity as required. SBA SOP 90 47 5 requires systems administrator activity to be recorded through software when an administrative account is used.

This information is used to ensure suspicious activity or violations can be investigated. This control also prevents undetected and unauthorized activity within administrator accounts. Use of automated processes to manage privileged accounts establishes an effective level of security based on FISMA guidance.

System Use Notification

We found the two systems did not show a warning banner to users before allowing access. SOP 90 47 5 requires all systems show an approved warning banner before users are allowed access, notifying them that the system is subject to monitoring and any unauthorized access is prohibited and may be subject to law enforcement action.

Employee Risk Designation

We found one user with administrative system privileges was initially assigned the wrong job position risk designation. As a result, the employee's background investigation was not appropriate for the position. The position-risk designation is a rating based on how sensitive the position is and determines the level of the background check required for the employee or contractor.

SBA policy 90 47 5 requires all SBA employees and contractors to undergo a background investigation based on the position risk designation before being allowed access to SBA facilities and systems. In addition, an effective security level in this area requires the use of automation to centrally manage and share risk designations with necessary parties.

Recommendations

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

6. Communicate and reinforce to program offices required system owner responsibilities to approve, establish, activate, modify, review, disable, and remove accounts in accordance with SOP 90 47 5.

We recommend that the Administrator direct the Office of Capital Access to

7. Require audit logging of administrator activity so an independent reviewer can monitor and mitigate risks, as required by SOP 90 47 5.
8. Establish warning banners for systems that lack them to communicate user responsibilities and prevent unauthorized disclosure, as required by SOP 90 47 5.

We recommend that the Administrator direct the Office of Personnel Security to

9. Perform periodic reviews of users with administrator privileges to ensure risk designation of their position aligns with their duties, as required by SOP 90 47 5.

Contingency Planning

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

Business Impact Assessment Incomplete

We found one system was missing required components in the business impact assessment, including

- documentation of all system components
- mission essential functions that require those system components
- documentation of recovery criticality
- identification of resource requirements; and
- recovery priority of the system.

SOP 90 47 5 requires system owners to develop and maintain a contingency plan for each system that includes an acceptable business impact assessment. FY 2021 Inspector General FISMA Reporting Metrics states that incorporating a system-level business impact assessment into the enterprise risk management process is an effective level of security.

A business impact analysis determines the effect on the agency if the system is disrupted or unavailable. SBA may not be able to determine contingency planning priorities including those functions that are mission essential without a proper business impact analysis.

Recommendation

We recommend that the Administrator direct the Office of Capital Access to:

10. Create a business impact analysis incorporating all elements SOP 90 47 5 requires.

Analysis of Agency Response

SBA management concurred with the 10 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 software inventory and contractor managed systems are maintained, as required by the National Institute of Standards and Technology (NIST) Special Publication 800-53.

Status: Resolved

SBA Management agreed with this recommendation has begun implementing solutions to better maintain an inventory of software and contractor managed systems. Management intends to complete final action on this recommendation by March 23, 2023. This recommendation can be closed when SBA management provides evidence that they have established a quality assurance program that effectively ensures system inventory and system ownership for agency and contractor systems is managed and maintained as required by NIST 800-53.

Recommendation 2

Ensure the continuity of operations plan is tested annually, as required by Federal Continuity Directive 1.

Status: Resolved

SBA Management agreed with this recommendation and stated they will ensure the annual exercise is completed and updated annually. Management intends to complete final action on this recommendation by August 1, 2022. This recommendation can be closed when SBA management provides documentation that the continuity of operations plan has been tested as required by Federal Continuity Directive 1.

Recommendation 3

Implement an agency-wide policy for the management of supply-chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. This policy should address key controls outlined in NIST 800-53, such as the procurement of third-party services, high-value asset identification, and counterfeit component prevention.

Status: Resolved

SBA Management agreed with this recommendation and stated they are in the process of formalizing a supply chain risk policy. Management intends to complete final action on this recommendation by June 1, 2022. This recommendation can be closed when SBA management provides documentation that a supply chain risk policy has been implemented.

Recommendation 4

Ensure timelines are incorporated into policies requiring baseline scan vulnerabilities be remediated in a timely manner. Also, ensure these vulnerabilities are tracked appropriately through the Plan of Action and Milestones process as required by NIST 800-53.

Status: Resolved

SBA management agreed with this recommendation and stated they will begin the process by defining and communicating baselines for major operating system components, and then monitor deviations within those applicable assets. Management intends to complete final action by September 1, 2022. This recommendation can be closed when SBA management provides documentation that timelines have been implemented for remediating baseline scan vulnerabilities and evidence that those timelines are being monitored and tracked.

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.

Status: Resolved

SBA management agreed with this recommendation and stated they are correcting identified gaps in their vulnerability process for contractor operated services. Management intends to complete for final action by June 1, 2022. This recommendation can be closed when SBA management provides documentation that systems have undergone scans, and vulnerabilities have been identified and addressed as required by SOP 90 47 5.

Recommendation 6

Communicate and reinforce to program offices required system owner responsibilities to approve, establish, activate, modify, review, disable, and remove accounts in accordance with SOP 90 47 5.

Status: Resolved

SBA management agreed with this recommendation and stated they will increase their monitoring and oversight over account approval and termination. Management intends to complete for final action by July 1, 2022. This recommendation can be closed when SBA management provides documentation that it has communicated, and reinforced account management responsibilities as required in SOP 90 47 5.

Recommendation 7

Require audit logging of administrator activity so an independent reviewer can monitor and mitigate risks, as required by SOP 90 47 5.

Status: Resolved

SBA management agreed with the recommendation and stated they are taking action to ensure privileged user activity is logged. Management intends to complete for final action by May 1, 2022. This recommendation can be closed when SBA management provides documentation that privileged accounts are being logged as required by SOP 90 47 5.

Recommendation 8

Establish warning banners for systems that lack them to communicate user responsibilities and prevent unauthorized disclosure, as required by SOP 90 47 5.

Status: Resolved

SBA Management agreed with the recommendation and stated they are working with system owners to ensure authentication points incorporate SBA-approved system notifications. Management intends to complete final action by May 1, 2022. This recommendation can be closed when SBA management provides documentation that warning banners have been implemented as required by SOP 90 47 5.

Recommendation 9

Perform periodic reviews of users with administrator privileges to ensure risk designation of their position aligns with their duties, as required by SOP 90 47 5.

Status: Resolved

SBA management agreed with our recommendation and stated they are improving quality control mechanisms to ensure privileged users' risk determination is accurate. Management intends to complete for final action by June 1, 2022. This recommendation can be closed when SBA management provides documentation that periodic reviews of privileged users' risk designations align with their duties as required by SOP 90 47 5.

Recommendation 10

Create a business impact analysis that incorporates all elements required by SOP 90 47 5.

Status: Resolved

SBA management agreed with our recommendation and stated they are working to correct irregulates identified in the review of the business impact analyses and recovery objectives. Management intends to complete for final action by May 1, 2022. This recommendation can be closed when SBA management provides documentation that all elements that are required by SOP 90 47 5, have been incorporated in the business impact analysis.

Appendix I: Objective, Scope, and Methodology

Our objectives were to determine whether SBA complied with FISMA in 2021 and assess the maturity of controls used to address risks in each of the nine domains reported to the Department of Homeland Security 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

We hired KPMG LLP, an independent public accounting firm, for our FY 2021 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' CyberScope application in October 2021.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) *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.

Prior Work

OIG reviews IT security through the annual financial statement audit, as well as the annual FISMA evaluation. Our recent reports include

- Independent Auditors' Report on SBA's FY 2021 Financial Statements, Report 22-05 (November 15, 2021)
- FY 2020 Federal Information Security Modernization Act Review, Report 21-17, (July 6, 2021)

Appendix II: Assessment Maturity Level Definitions

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

The FY 2021 FISMA reporting metrics, issued in May 2021, were developed as a collaborative effort among OMB, DHS, and the Council of Inspector General for Integrity and Efficiency in consultation with the Federal Chief Information Officer Council.

The current 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.

Maturity Level	Description	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 Federal Information Security Modernization Act 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 eight domains are calculated based on a simple majority, where the most frequent level across the questions serves as the domain rating.

Appendix III: Management Response

SBA Management Comments Follow

U.S. Small Business Administration

Office of the Chief Information Officer

Memo for: Hannibal Ware
Inspector General

From: Luis A. Campudoni
Acting Chief Information Officer

Subject: Management Response:
Draft FY 2021 Federal Information Security Modernization Act Review, Project 21014

Date: March 15, 2022

We appreciate the opportunity to review the draft report entitled "FY 2021 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 and the Executive Order (EO) 14028 initiatives, 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 more accurately and comprehensively track its software inventory, enabling automation to the greatest extent possible, for internal and contractor-operated systems and services.

Recommendation 2: The SBA agrees. The SBA will ensure that the agency Continuity of Operations Plan (COOP) is updated and exercised annually.

Recommendation 3: The SBA agrees. The SBA is in the process of formalizing its supply chain risk management program. This includes formalization of enterprise wide policy, procedures, acquisition language, supplier reviews and notifications, training, and methods to ensure component authenticity.

Recommendation 4: The SBA agrees. The SBA plans to first define and communicate agency wide baseline configurations for major operating system components. Once defined, applicable assets will be continuously monitored for deviations, in conjunction with Recommendation 1. In addition, the SBA is improving its vulnerability tracking process.

Recommendation 5: The SBA agrees. The SBA is correcting identified gaps in its vulnerability scanning process for contractor-operated services, utilizing a hybrid of on-premises and cloud-based capabilities, to ensure visibility and remediation tracking across the enterprise.

Recommendation 6: The SBA agrees. The SBA continues to increase its monitoring and oversight for account approval and termination.

Recommendation 7: The SBA agrees. The SBA is taking corrective action to ensure privileged user activity is logged and monitored through its enterprise capability.

Recommendation 8: The SBA agrees. The SBA is working with system owners to ensure that all system- and application-level authentication points include SBA-approved use notifications.

Recommendation 9: The SBA agrees. The SBA is improving its quality controls mechanisms to ensure that privileged users' position risk determination is accurate and aligns with their assigned responsibilities.

Recommendation 10: The SBA agrees. The SBA is correcting irregularities identified in its review of system business impact analyses and recovery objectives.