SBA INSPECTOR GENERAL

FY 2020 Federal Information Security Modernization Act Review

REPORT NUMBER 21-17 | July 6, 2021

Executive Summary

Weaknesses Identified During the FY 2020 Federal Information Security Modernization Act Review

What OIG Reviewed

This report summarizes the results of our fiscal year (FY) 2020 Federal Information Security Modernization Act (FISMA) evaluation and assesses the maturity of controls used to address risks in each of the information security areas, called domains.

Our objectives were to (1) determine whether the Small Business Administration (SBA) complied with FISMA and (2) assess the maturity of controls used to address risks in each of the eight security domains.

We assessed the maturity of SBA's information security program as outlined in the FY 2020 Inspector General FISMA Reporting Metrics issued by the Cybersecurity and Infrastructure Security Agency[1]. We tested a subset of eight systems against these metrics and evaluated them against guidance in the FISMA metrics.

What OIG Found

We rated SBA's overall program of information security as ”not effective” because SBA only achieved a maturity level rating of "managed and measurable" in one of the eight domains. Inspectors General are required to assess the effectiveness of information security programs on a maturity model spectrum.

In FY 2020, SBA had an unprecedented volume of loan and grant applications because of the CARES Act and other pandemic-related legislation. As a result, the agency experienced new security challenges. Based on tests of the eight information systems, we determined the results of each domain as follows:

1. Risk Management — Defined
2. Configuration Management—Defined
3. Identity and Access Management — Consistently Implemented
4. Data Protection and Privacy — Consistently Implemented
5. Security Training — Defined
6. Information Security Continuous Monitoring — Defined
7. Incident Response — Managed and Measurable
8. Contingency Planning — Consistently Implemented.

In the maturity model, the managed and measurable and optimized levels represent effective security. Performance below managed and measurable (ad hoc, defined, or consistently implemented represents ineffective security (See Appendix II)).

OIG Recommendations

We made 10 recommendations in five of the domains: three recommendations in risk management, three recommendations for configuration management, two for identity and access management, one recommendation for security training, and one for information security continuous monitoring. We did not have new findings for the data protection and privacy, contingency planning, and incident response domains and so did not discuss those areas in this report.

[1] FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0, April 17, 2020, as published by the Cybersecurity & Infrastructure Security Agency.

Agency Comments

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

Office of Inspector General

U.S. Small Business Administration

DATE: July 6, 2021

TO: Isabella Casillas Guzman
Administrator

FROM: Hannibal "Mike" Ware
Inspector General

SUBJECT: FY 2020 Federal Information Security Modernization Act Review

This report presents the results of our evaluation on weaknesses identified during the FY 2020 Federal Information Security Modernization Act Review. Our objectives were to determine whether the Small Business Administration complied with FISMA and to assess progress in each of the Cyberscope areas.

We previously furnished copies of the draft report and requested comments on the recommendations. SBA's management comments were appended and were considered in finalizing the report.

We appreciate the courtesies and cooperation extended to us during this evaluation. If you have any questions, 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
Keith Bluestein, Chief Information Officer
Luis Campudoni, Deputy Chief Information Officer
Peggy Delinois Hampton, Acting General Counsel
Erica Gaddy, Deputy Chief Financial Officer
Martin Conrey, Attorney Advisor, Legislation and Appropriation
Michael A. Simmons, Attorney Advisor, Office of General Counsel
Rafaela Monchek, Director, Office of Continuous Operations and Risk Management
Tonia Butler, Director, Office of Internal Controls

Table of Contents

Introduction

The Federal Information Security Modernization Act (FISMA) requires all federal agencies to determine the effectiveness of their information security program and practices.[2] This report summarizes the results of our fiscal year (FY) 2020 evaluation of SBA's information technology (IT) systems. The report also assesses the effectiveness, or maturity, of the controls used to address risks in each of the required review areas, referred to as domains.

We did not duplicate recommendations if the Small Business Administration (SBA) still needs to address or implement outstanding recommendations, and we have identified those areas throughout this report. However, if we identified new vulnerabilities, we made new recommendations.

Background

Each fiscal year, the Office of Inspector General (OIG) is required to report on the following eight domains:

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

OIG hired and monitored independent public accounting firm KPMG for the FY 2020 FISMA evaluation. KPMG tested a representative subset of eight SBA systems and security to determine SBA's compliance with the FY 2020 Inspector General FISMA Reporting Metrics issued by the Office of Management and Budget (OMB).

Each domain is scored on a numerical scale of 1 (worst) to 5 (best). If a domain is scored 3 or higher, we did not make any recommendations. Three domains—incident response, data protection and privacy, and contingency planning—did not have findings and are not discussed in this report.

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.

[2] 44 USC §3555(a) and (b)(1)

Objectives

Our objectives were to 1) determine whether SBA complied with FISMA and 2) assess the maturity of controls used to address risks in each of the domains: 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 program as **not effective** in FY 2020 because only one of the eight domains' maturity level was ranked as "managed and measurable." In the maturity model, domain performance scored below managed and measurable (such as ad hoc, defined, or consistently implemented) means IT security is ineffective.

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

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

As noted earlier, the last three domains—data protection and privacy, contingency planning, and incident response, did not have findings and are not discussed in this report.

Challenges and Improvements

In FY 2020, SBA faced significant new security challenges because of the enormous increase in loan transaction volume for pandemic relief programs. Consequently, SBA needs to update and implement security operating procedures and address newly identified vulnerabilities in its systems.

We identified areas that need improvement in controls, including system inventory management, patching, user recertification, and appropriately maintaining Authority to Operate agreements.

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.

I. Risk Management

Risk Management focus on policies and actions that manage information security risks to the organization. We determined that SBA's risk management maturity level was "defined." SBA can improve security in this domain by resolving the following issues:

Cloud Information System Inventory

NIST 800-53 Revision 4 states an organization should maintain an inventory of its information systems.[3] However, SBA did not consistently update and monitor its cloud system inventory to ensure system vulnerabilities are tracked and resolved. The inventory was not updated due to

[3] National Institute of Standards and Technology, US Department of Commerce, Special Publication (NIST SP) 800-53 Revision 4, Section CM-8, April 2013.

competing priorities during the Coronavirus disease (COVID-19) pandemic. Our testing showed the central repository for information systems in SBA's Cyber Security Asset Management tool was not up to date as of September 24, 2020. The tool did not include the system used to process disaster loans under the Coronavirus Aid, Relief, and Economic Security (CARES) Act. As a result, the agency does not know how much data is stored in and subject to the inherent risks of cloud systems.

System Security Plan Documentation

SBA's SOP 90 47 5 states all system security plans should be updated at least annually.[4] However, we found that one of the systems tested was mission critical and did not have an updated security plan as required by guidance.

System security plans define security requirements under specific security criteria. Not having an updated system security plan could result in critical risk mitigation activities not being performed or security controls not being tested. Lack of security controls could result in improperly maintained hardware, incomplete patch management, or incomplete contingency plans.

Plan of Action and Milestone Remediation

NIST SP 800-53 states that plans of actions and milestones be developed for controls that have been identified as less than effective through independent assessments.[5] SBA did not consistently monitor its planned remediation dates to ensure remedial actions were on schedule. Although our tests showed planned actions were completed after the established due date, KPMG's review process showed management did not consistently amend the due date or document a justification for the delay.

Recommendations

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

1. Design and implement a quality assurance program to ensure that system inventory and system ownership for all SBA and contractor managed systems is maintained as required by NIST SP 800-53.
2. Enforce the cybersecurity and privacy policy to ensure that all system security plans are reviewed and approved at least annually, as required by SOP 90 47 5 and NIST SP 800-53.
3. Update the plan of actions and milestones to reflect progress against milestone completion dates, justification for revised milestones, and amendments to plan for action and milestones past due, as required by NIST SP 800-53 and SOP 90 47 5.

II. Configuration Management

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

[4] SOP 90 47 5, chapter 3, paragraph 2.f(2)

[5] National Institute of Standards and Technology, US Department of Commerce, Special Publication (NIST SP) 800-53 Revision 4, Section CA-5, April 2013.

Approvals for System Changes

NIST 800 53 states that organizations implement approved configuration changes to a system, but SBA did not ensure changes made to information systems were approved by system owners.[6] Our testing showed changes were not approved for three of eight systems. Approvals for system changes reduce the risk that unauthorized modifications could affect the confidentiality, integrity, or availability of sensitive data.

Vulnerability Remediation Process

As required by SOP 90 47 5, SBA did not reinforce its patch management and configuration policies to ensure that identified systems were properly configured and vulnerabilities remediated within specified timeframes.[7] Vulnerability scans identified multiple configuration management and patch management weaknesses.

In addition, SBA did not document or issue a formal risk acceptance waiver required by SOP 90 47 5 for the vulnerability weaknesses identified through the scans.[8] We identified a number of the vulnerabilities during our FY 2020 review.

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.

Security Patches Require Approval

NIST 800 53 states that organizations implement tested and approved configuration changes to a system.[9] However, SBA did not enforce its patch management process to ensure that patches were tested and approved. SBA should require evidence for tests and approvals of security patches to reduce the risk of unauthorized modifications.

Baseline Configuration Deviations Require Approval

NIST SP 800 53 states that an organization should identify, document, and approve exceptions from established configuration settings.[10] SBA did not approve the baseline deviations for information systems because of competing priorities during the Coronavirus disease 2019 (COVID-19) pandemic.

[6] National Institute of Standards and Technology, US Department of Commerce, Special Publication (NIST SP) 800-53 Revision 4, Section SA-10, April 2013.

[7] SOP 90 47 5, chapter 5, paragraph 2.f(1)

[8] SOP 90 47 5, chapter 5, paragraph 2.f(2)

[9] National Institute of Standards and Technology, US Department of Commerce, Special Publication (NIST SP) 800-53 Revision 4, Section CM-3, Enhancement 2, April 2013.

[10] National Institute of Standards and Technology, US Department of Commerce, Special Publication (NIST SP) 800-53 Revision 4, Section CM-6, April 2013.

SBA also did not issue a risk acceptance waiver in a timely manner. SBA should require approvals for baseline configuration deviations to reduce the risk that unauthorized modifications could affect the confidentiality, integrity, or availability of sensitive data.

Recommendations

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

4. Improve the existing application change management process to ensure changes are correctly documented and approved and an audit trail established before implementation, as required by NIST SP 800 53.
5. Address identified vulnerabilities in systems during the assessment process and ensure patches are documented, tested, approved, and applied to all systems as required by SOP 90 47 5.
6. Require all system owners to approve and provide justification for deviations from the baseline configuration, as required by NIST SP 800 53.

III. 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 two vulnerabilities:

User Accounts Authorizations

SOP 90 47 5 requires that information system accounts must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing accounts.[11] SBA did not correctly execute its new and existing user access review process to reduce the risk that improper access is approved and not identified. We identified 11 of 13 new users of two systems for whom SBA could not provide evidence that access had been properly authorized.

SOP 90 47 5 also requires separation of duties among multiple staff whose responsibilities have a security impact; no individual should entirely control a critical process.[12]

We also found that during the COVID-19 pandemic, new and existing user accounts were not always authorized due to competing priorities and lack of management oversight.

Recommendations

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

7. Appropriately track, approve, and validate access to new and existing user accounts to ensure the appropriate assigned access is granted in accordance with SOP 90 47 5.
8. Communicate and reinforce to program offices their respective system owner responsibilities to approve, establish, activate, modify, review, disable, and remove accounts in accordance with SOP 90 47 5.

[11] SOP 90 47 5, chapter 5, paragraph 2.b(3)

[12] SOP 90 47 5, chapter 4, paragraph 2.r(1)

IV. Security Training

System users should have proper IT security training relevant to the system and the applicable IT security role. We determined that the Agency's maturity level is defined. Our testing identified that SBA has not consistently implemented user awareness training. The effectiveness of security training can be improved through resolution of recommendations in the CyberScope domain of Identity and Access Management.

Security Training Program

SBA's SOP 90 47 5 states all SBA authorized users, employees, and contractors must complete the mandatory CSAT course annually as well as within 30 days of beginning employment.[13] SOP 90 47 5 also states individuals with significant security responsibilities should have appropriate security and privacy awareness training needed to carry out their duties.[14] We found that SBA did not ensure that users consistently completed required Computer Security Awareness Training (CSAT).

Mandatory security awareness training was incomplete. Management was unable to enforce security training completion requirements in FY 2020 because of the record increase in new users processing pandemic-related loans. We identified 6,455 of 21,499 users who did not complete the required annual training.

Mandatory specialized security awareness training was incomplete. Management also did not enforce requirements for IT personnel to complete the required training. We identified 43 of 290 users who were identified as IT personnel with significant information security and privacy responsibilities who had not completed the specialized training.

An incomplete security training program introduces weaknesses into the IT environment. SBA personnel not fully trained on computer security awareness and privacy protocols may not know how to respond to internal and external threats. Consequently, undetected security vulnerabilities could compromise the confidentiality, integrity, and availability of SBA data.

Recommendations

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

9. Design and implement mechanisms to ensure that all new and existing users and IT personnel with significant security and privacy responsibilities complete the required training in the timeframe required by SOP 90 47 5.

V. 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 the domain's maturity level was "defined". SBA can improve the effectiveness of information security continuous monitoring by resolving the following:

[13] SOP 90 47 5, chapter 4, paragraph 2.h(2)

[14] SOP 90 47 5, chapter 2, paragraph 6.x

System Authority to Operate Controls

SBA's SOP 90 47 5 states that all SBA IT systems must have a current authorization.[15] We determined SBA did not ensure all systems audited for this FISMA review had an Authorization to Operate for the entire fiscal year.

SBA managers said they were unable to follow up on proper documentation, tracking, and authorization procedures because of increased strain caused by CARES Act and other COVID-19 legislation requirements and juggling multiple priorities.

However, agency management cannot be sure of the effectiveness of a system's security controls if a system's authorization is not up to date. Authorization packages include critical information such as security plans, security assessment reports, etc.

In an unauthorized system, those critical components may not be current. Potential risks could include exposing the network to malware and potentially compromising sensitive data or program objectives.

Recommendation

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

10. Ensure all SBA systems have a current Authorization to Operate, as required by SOP 90 47 5.

[15] SOP 90 47 5, chapter 3, paragraph 2.b(2)

Analysis of Agency Response

SBA management concurred with the 10 recommendations in the draft report.

Summary of Actions Necessary to Close the Report

The following provides the status of recommendations and actions necessary to close them.

1. Design and implement a quality assurance program to ensure that system inventory and system ownership for all SBA and contractor managed systems is maintained as required by NIST SP 800-53.

   Resolved. SBA management agreed with this recommendation and stated they have implemented corrective actions. 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.

2. Enforce the cybersecurity and privacy policy to ensure that all system security plans are reviewed and approved at least annually, as required by SOP 90 47 5 and NIST SP 800-53.

   Resolved. SBA management agreed with this recommendation and stated they have implemented corrective actions. The recommendation can be closed when SBA management provides evidence demonstrating they are enforcing the cybersecurity and privacy policy to ensure that all system security plans are reviewed and approved at least annually.

3. Update the plan of actions and milestones (POA&Ms) to reflect progress against milestone completion dates, justification for revised milestones, and amendments to plan for action and milestones past due, as required by NIST SP 800-53 and SOP 90 47 5.

   Resolved. SBA management agreed to implement the recommendation and stated they will complete corrective actions by August 2021. This recommendation can be closed when management provides evidence that POA&Ms are updated accordingly.

4. Improve the existing application change management process to ensure changes are correctly documented and approved and an audit trail established before implementation, as required by NIST SP 800 53.

   Resolved. SBA management agreed with this recommendation and stated they have implemented corrective actions. The recommendation can be closed when management provides evidence they have improved the existing application change management process to ensure changes are correctly documented and approved and an audit trail has been established as required.

5. Address identified vulnerabilities in systems during the assessment process and ensure patches are documented, tested, approved, and applied to all systems as required by SOP 90 47 5.

   Resolved. SBA management agreed with the recommendation and stated they will implement corrective actions by August 2021. This recommendation can be closed when management provides evidence that vulnerabilities are identified and applied in a consistent and timely manner.

6. Require all system owners to approve and provide justification for deviations from the baseline configuration, as required by NIST SP 800 53.

   Resolved. SBA management agreed to implement the recommendation and stated they will complete corrective actions by August 2021. This recommendation can be closed when management provides evidence that baseline deviations are approved and justified.

7. Appropriately track, approve, and validate access to new and existing user accounts to ensure the appropriate assigned access is granted in accordance with SOP 90 47 5.

   Resolved. SBA management agreed with this recommendation and stated they have implemented corrective actions. The recommendation can be closed when management provides evidence they are tracking, approving, and validating access to new and existing user accounts as required.

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

   Resolved. SBA management agreed with this recommendation and stated they have implemented corrective actions. The recommendation can be closed when management provides evidence they have communicated to program offices reinforcing the requirements for approving, establishing, activating, modifying, reviewing, disabling, and removing accounts.

9. Design and implement mechanisms to ensure that all new and existing users and IT personnel with significant security and privacy responsibilities complete the required training in the timeframe required by SOP 90 47 5.

   Resolved. SBA management agreed with the recommendation and stated they have implemented corrective actions. The recommendation can be closed when management provides evidence they have established a process to ensure that all new and existing users and IT personnel with significant security and privacy responsibilities complete training as required.

10. Ensure all SBA systems have a current Authorization to Operate, as required by SOP 90 47 5.

Resolved. SBA management agreed with this recommendation and stated they have implemented corrective actions. The recommendation can be closed when management provides evidence all SBA systems have a current Authorization to Operate.

Appendix I: Objective, Scope, and Methodology

Our objectives were to (1) determine whether SBA complied with FISMA in 2020 and (2) assess the maturity of controls used to address risks in each of the eight domains reported to the DHS CyberScope system:

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

We hired KPMG, an independent public accounting firm for our FY 2020 FISMA evaluation. KPMG tested a representative subset of eight SBA systems and security controls and assessed SBA's adherence to or progress in implementing minimum security standards and requirements commensurate with 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 November 2020.

We conducted this evaluation in accordance with the CIGIE'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 2020 FISMA reporting metrics, issued in April 2020, were developed as a collaborative effort among OMB, DHS, and the Council of Inspectors General on Integrity and Efficiency (CIGIE) in consultation with the Federal Chief Information Officer Council.

The metrics continue 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 IT security through the annual financial statement audit as well as the annual FISMA evaluation.

Our recent reports include:

1. ***Independent Auditor's Report on SBA's FY 2020 Financial Statements***, Report 21-04, December 18, 2020.
2 ***Weaknesses Identified During the FY 2019 Federal Information Security Modernization Act Review*, **Report 20-10, March 30, 2020.

Appendix II: Assessment Maturity Level Definitions

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

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/mission needs.

Source: FY 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, Version 4.0, April 17, 2020

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

Agency Comments

U.S. Small Business Administration

Office of the Chief Information Officer

Memo for:
Hannibal Ware
Inspector General
U.S. Small Business Administration

From:
Keith A. Bluestein
Chief Information Officer
U.S. Small Business Administration

Subject:
Management Response:
Draft FY 2020 Federal Information Security
Modernization Act Review, Project 20011

Date:
May 12, 2021

We appreciate the opportunity to review the draft report entitled "FY 2020 Federal Information Security Modernization Act Review." We are equally satisfied with the Inspector General's understanding and consideration of the unusual and new challenges the organization encountered during our support of pandemic-related legislation. We concur with recommendations in the draft report.

The Office of the Chief Information Officer will diligently pursue robust and adaptive cybersecurity visibility, defense, detection, and response capabilities across the enterprise.

Sincerely,

// signed //

Keith A. Bluestein
Chief Information Officer