SBA INSPECTOR GENERAL AUDIT REPORT

Weaknesses Identified During the FY 2019 Federal Information Security Modernization Act Review

REPORT NUMBER 20-10 | MARCH 30,2020

Executive Summary

Weaknesses Identified During the FY 2019 Federal Information Security Modernization Act Review

Report
Number
20-10

What OIG Reviewed

This report summarizes the results of our review of the Federal Information Security Modernization Act (FISMA) evaluation and assesses the maturity of controls used to address risks in each of the CyberScope 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 CyberScope domains: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

To determine whether SBA complied with FISMA, we assessed the maturity of SBA's information security program as outlined in the FY 2019 Inspector General FISMA Reporting Metrics as issued by the Office of Management and Budget. We tested against these metrics by selecting a subset of 10 systems and evaluating them against guidance outlined in the FISMA metrics.

What OIG Found

Control tests in each domain indicated that SBA was at the "managed and measurable level" for incident response; the "consistently implemented level" for risk management, data protection and privacy, and contingency planning; and the "defined level" for the four other domains. We evaluated the overall programs as "not effective" per the evaluation criteria set forth by the FY 2019 Inspector General FISMA Reporting Metrics. These results are summarized in the following table.

CyberScope Domain	Maturity Level
Risk Management	Consistently Implemented
Configuration Management	Defined
Identity and Access Management	Defined
Data Protection and Privacy	Consistently Implemented
Security Training	Defined
Information Security Continuous Monitoring	Defined
Incident Response	Managed and Measurable
Contingency Planning	Consistently Implemented

*SBA's CyberScope domains were not rated at the ad hoc or optimized maturity levels. Within the context of the maturity model, the managed and measurable and optimized levels represent effective security (appendix III).

OIG Recommendations

The Office of Inspector General made 11 recommendations in the following CyberScope domains: risk management (2 recommendations); configuration management (5 recommendations); and identity and access management (4 recommendations).

Agency Comments

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

U.S. SMALL BUSINESS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL
WASHINGTON, D.C. 20416

Final Report Transmittal
Report Number 20-10

DATE: March 30, 2020

TO: Jovita Carranza
Administrator

FROM: Hannibal "Mike" Ware
Inspector General

SUBJECT: Weaknesses Identified During the FY 2019 Federal Information Security Modernization Act Review

This report presents the results of our evaluation on weaknesses identified during the FY 2019 Federal Information Security Modernization Act (FISMA) 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 written comments on the recommendations. SBA management's comments are appended and were considered in finalizing the report.

We appreciate the courtesies and cooperation extended to us during this audit. If you have any questions, please contact me or Andrea Deadwyler, Assistant Inspector General of Audits at (202) 205-6586.

cc: William Manger, Chief of Staff
Christopher Gray, Deputy Chief of Staff
Maria A. Roat, Chief Information Officer
Stephen Kong, Acting Chief Operating Officer
Nina Levine, Acting General Counsel
Dorrice Roth, Acting Chief Financial Officer and Associate Administrator for Performance Management
Guy V. Cavallo, Deputy Chief Information Officer
Martin Conrey, Attorney Advisor, Legislation and Appropriation
Michael A. Simmons, Attorney Advisor

Table of Contents

Introduction

This report summarizes the results of our fiscal year (FY) 2019 Federal Information Security Modernization Act (FISMA) evaluation and assesses the maturity of controls used to address risks in each of the CyberScope domains. We made new recommendations where we identified new vulnerabilities. We did not make duplicate recommendations in instances where the Small Business Administration (SBA) needs to implement outstanding recommendations, but we have identified these control areas throughout the body of this report.

FISMA requires federal agencies to develop, implement, and report on the effectiveness of each agency's information security program. For FY 2019, the Office of Inspector General (OIG) was required to report on the following domains: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

As part of the FY 2019 FISMA evaluation, KPMG, an independent public accounting firm, tested a representative subset of 10 SBA systems and security controls. OIG monitored KPMG's work and used test results to report SBA's compliance with the FY 2019 Inspector General FISMA Reporting Metrics, as issued by the Office of Management and Budget (OMB), and reported in the CyberScope submission to the Department of Homeland Security (DHS) in October 2019.[1] OIG also used these test results to assess SBA's adherence to or progress in implementing minimum security standards and requirements commensurate with each system's security categorization and risk.

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 CyberScope domains: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

[1] OMB Memorandum 19-02, Fiscal Year 2018–2019 Guidance on Federal Information Security and Privacy Management Requirements.

Results

To determine whether SBA complied with FISMA, we assessed the maturity of SBA's information security program as outlined in the FY 2019 Inspector General FISMA Reporting Metrics.

Inspectors General are required to assess the effectiveness of information security programs on a maturity model spectrum. Control tests in each domain indicated that SBA was at the "managed and measurable level" for incident response; the "consistently implemented level" for data protection and privacy, contingency planning, and risk management; and the "defined level" for the four other domains. We evaluated the overall program as "not effective per the evaluation criteria set forth by the FY 2019 Inspector General FISMA Reporting Metrics.

Notwithstanding this rating, we observed improvement in cybersecurity oversight in the domains of incident response, risk management, and contingency planning. Within the context of the maturity model domains, performance at a "managed and measurable level" represents an effective level of security. To continue to improve its FISMA effectiveness, SBA needs to proactively update and implement security operating procedures and address the new vulnerabilities identified in this report.

Summarized below are the FISMA domains testing results. Each section outlines the scope of the review, test results, and recommendations for improvement.

Risk Management

Risk management, as outlined in National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, includes the program and supporting processes to manage information security risk to organizational operations, organizational assets, individuals, other organizations, and the nation. We determined that the Agency's maturity level was "consistently implemented." This domain can be improved through resolution of the improvement areas identified below.

System Hardware Documentation Needs to Be Consistently Maintained

SBA needs to consistently maintain administration documentation for its hardware inventories to ensure only authorized hardware is on its systems. SBA's implementation procedure for the NIST Risk Management Framework states that there must be a complete listing of hardware assets for each system. Our testing identified that sufficient documentation was not maintained for all hardware inventory at SBA headquarters, data center locations, and contractor sites that process and store SBA data. The inventory was not updated due to SBA not finalizing and implementing system inventory guidance, nor defining who within SBA was responsible for maintaining a system's inventory.

Plan of Action and Milestone Remediation Dates Need to Be Monitored

SBA needs to monitor its plan of action and milestone (POA&M) remediation dates to ensure that remedial actions are on schedule. POA&Ms are established to correct weaknesses or deficiencies and to reduce or eliminate known vulnerabilities identified in information systems. NIST SP 800-53 requires that POA&Ms be updated based on findings from security controls assessments, security impact analyses, and continuous monitoring activities. Our testing identified 2 open POA&Ms out of 25 reviewed that were completed after the established due date and did not have a documented justification for the delay.

Recommendations

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

1. Develop and implement procedures to document and maintain hardware inventory and system ownership for all SBA and contractor managed systems.

2. Update the plan of action and milestones to reflect progress against milestone completion dates, justification for revised milestones, and amendments to plan for action and milestones past due.

Configuration Management

Configuration management focuses on establishing and maintaining the integrity of IT products and information systems. We determined that the Agency's maturity level was "defined." This domain can be improved through resolution of the three vulnerabilities identified below.

Change Management Process Not Followed

SBA needs to reinforce its change management process to ensure that any changes made to the system can be documented, tracked, and reversed if necessary. NIST 800 53 requires that configuration changes to a system be documented. Our testing identified that SBA was unable to provide documented evidence that the change management process was followed for two systems. Due to management oversight, SBA did not provide evidence that the change management process was appropriately followed.

SBA Needs to Improve Its Patching Process

SBA needs to reinforce patch management and configuration policies to ensure that identified systems are properly configured and vulnerabilities are remediated within specified timeframes. Vulnerability scans identified multiple configuration management and patch management weaknesses. In addition, many of these vulnerabilities were previously identified during the FY 2018 review. Due to inconsistent application of SBA IT Security Policy, SOP 90 47 4, limited or lack of authenticated vulnerability scans limiting the accuracy of vulnerability status of SBA devices and systems, and a limited discovery process to ensure which systems are production and non-production, SBA did not ensure vulnerabilities were mitigated in accordance with SBA defined timelines.

Baseline Configuration Deviations Require Approval

SBA should require approvals for baseline configuration deviations to reduce the risk that deviations in baseline configurations are not remediated. NIST SP 800 53 states that an organization should identify, document, and approve exceptions from established configuration settings. SBA did not ensure identified deviations from the baseline were mitigated or approved.

Recommendations

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

3. Establish a process for tracking and documenting change management documents to establish an audit trail, as well as to aid in resolving any change management issues that may arise.

4. Address identified vulnerabilities in systems during assessment process and enforce policy to ensure patches are applied to all systems as required by SBA IT Security Policy 90 47 4.

5. Reevaluate the vulnerability management process for discovery to ensure that scans accurately identify production and non-production environments.

6. Require all system owners to adhere to SBA policy allowing personnel to perform administrative level authenticated scans.

7. Establish a process for providing approval and justification for deviations from the baseline configuration as required by NIST SP 800 53.

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 resources. We determined that the Agency's maturity level was "defined." This domain can be improved through the remediation of the four vulnerabilities identified below.

Identify, Credential, and Access Management Strategy Not Finalized

SBA needs to finalize its entity-wide Identify, Credential, and Access Management (ICAM) policy for Access Control. The current policy is still in draft and is not complete. Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors requires agencies to develop and issue policy for the use of personal identification verification (PIV) implementation. SBA has not formalized or implemented this policy agency wide due to resource limitations. Without a formal ICAM strategy, SBA is unable to implement federal ICAM requirements; therefore, there is increased risk that management may not sufficiently identify and mitigate security risks.

New User Accounts Require Documentation That Access Granted Was Appropriate

To reduce the risk that improper access is approved and not identified, SBA must strengthen its process of review for user access. SBA IT Security Policy, SOP 90 47 4, states that it is the data owner's responsibility to review and determine appropriate access at least annually. Our testing identified that SBA could not provide evidence that access granted to new users added in FY 2019 was appropriate for two systems.

Personal Identification Verification Enforcement Exemptions Require Approvals

SBA needs to improve its processes for PIV enforcement to reduce risk that a non-PIV-enforced machine could be used for unauthorized access to SBA systems. SBA IT Security Policy, SOP 90 47 4, states that all users on government workstations must authenticate using a PIV card, unless they are exempt from the requirement. Examples of the listed exemptions include if the employee is temporary, has forgotten their PIV for the day, or is being issued a new PIV. Our testing identified that SBA could not provide approvals for these exemptions for 1 out of 40 selected workstations.

Session Lockout Settings Need to Be Implemented

SBA needs to implement its session lockout policies to reduce the risk of unauthorized access to its systems and the data they contain. SBA IT Security Policy, SOP 90 47 4, states that failed logins must automatically lock out an account for 30 minutes, unless the account is unlocked by an administrator. Our testing identified that one system had a lockout setting that did not adhere to SBA policy. Lockout settings were initially set by a third-party vendor and were not subsequently changed to reflect SBA policy.

Recommendations

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

8. Continue to develop its entity-wide Identify, Credential, and Access Management implementation strategy for Access Control.

9. Develop a process to ensure timely retrieval of access authorizations for users.

10. Strengthen the process for maintaining approvals for removing personal identification enforcement on SBA workstations as required by SBA IT Security Policy 90 47 4.

11. Ensure lockout settings meet SBA policy as required by SBA IT Security Policy, SOP 90 47 4.

Security Training

System users should have proper IT security training relevant to their IT security role and to the system. We determined that the Agency's maturity level is "defined." Our testing identified that SBA has not consistently implemented user awareness training due to a weakness identified with user access agreements. The effectiveness of security training can be improved through resolution of recommendations identified above in the CyberScope domain of identity and access management.

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 "defined." Our testing identified that SBA was not enforcing the configuration and patch management processes to remediate vulnerabilities found within required timeframes. The effectiveness of information security continuous monitoring oversight can be improved through resolution of identified recommendations above in the CyberScope domain of configuration management.

Analysis of Agency Response

SBA Management provided informal comments and concurred with the 11 recommendations in the draft report.

Summary of Actions Necessary to Close the Recommendations

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

1. **Resolved**. SBA agreed to develop and implement procedures to document and maintain hardware inventory and system ownership for all SBA and contractor managed systems. This recommendation can be closed when management provides evidence that hardware inventories procedures are consistently maintained.

2. **Resolved**. SBA agreed to update the plan of action and milestones to reflect progress against milestone completion dates, justification for revised milestones, and amendments to plan for action and milestones past due. This recommendation can be closed when management provides evidence that POA&Ms are updated accordingly.

3. **Resolved**. SBA agreed to establish a process for tracking and documenting change management documents to establish an audit trail, as well as to aid in resolving any change management issues that may arise. This recommendation can be closed when management provides evidence that change management processes are followed accordingly.

4. **Resolved.** SBA agreed to identify vulnerabilities in systems during assessment process and enforce policy to ensure patches are applied in a timeframe required by SBA IT Security Policy 90 47 4. This recommendation can be closed when management provides evidence that vulnerabilities are identified, and patches are applied in a timely manner.

5. **Resolved**. SBA agreed to reevaluate the vulnerability management process for discovery to ensure that scans accurately identify production and non-production environments, such as testing and development systems. This recommendation can be closed when management provides evidence that their scans are identifying production and non-production environments.

6. **Resolved**. SBA agreed with our recommendation to address vulnerabilities in systems during the assessment process and ensure patches are applied according to policy. This recommendation can be closed when management provides evidence that vulnerabilities are identified, and patches are applied in a timely manner.

7. **Resolved**. SBA agreed to establish a process for providing approval and justification for deviations from the baseline configuration as required by NIST SP 800 53. This recommendation can be closed when management provides evidence of justifications and approvals for baseline deviations.

8. **Resolved.** SBA agreed to continue to develop its entity-wide ICAM strategy for access control. This recommendation can be closed when management provides evidence that an access control ICAM strategy has been developed.

9. **Resolved.** Develop a process to ensure timely retrieval of access authorizations for users.

This recommendation can be closed when management provides evidence that access authorizations for users are available.

10. **Resolved**. SBA agreed with our recommendation to strengthen the process for approvals for PIV removal on workstations. This recommendation can be closed when management provides evidence that approvals for PIV removal are available.

11. **Resolved**. SBA agreed with our recommendation to ensure lockout settings match SBA policy. This recommendation can be closed when management provides evidence that they have updated lockout settings to conform to SBA policy.

Appendix I: Objective, Scope, and Methodology

Our objectives were to (1) determine whether the Small Business Administration (SBA) complied with the Federal Information Security Modernization Act (FISMA) of 2014 and (2) assess the maturity of controls used to address risks in each of the eight CyberScope domains: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

FISMA is an amendment to the Federal Information Security Management Act of 2002. FISMA updates include requiring agencies to use automated tools in security programs, revise OMB Circular A-130 to eliminate inefficient or wasteful reporting, change reporting guidelines for threats, and ensure that all agency personnel are responsible for complying with agency security programs.

On April 9, 2019, the FY 2019 Inspector General FISMA Reporting Metrics were issued to provide instructions for agencies to meet their FY 2019 reporting requirements. The metrics required an assessment of agencies' information security programs. The reporting metrics were developed as a collaborative effort among OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in consultation with the Federal Chief Information Officer Council.

As part of the FY 2019 FISMA evaluation, KPMG, an independent public accounting firm, with agreement from OIG, tested a representative subset of SBA systems and security controls. KPMG performed testing to assess SBA's adherence to or progress in implementing minimum security standards and requirements commensurate with each system's security categorization and risk. OIG monitored KPMG's work and reported SBA's compliance with FISMA in the CyberScope submission to DHS in October 2019.

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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

Maturity Levels

The FY 2019 Inspector General FISMA Reporting Metrics were developed as a collaborative effort between OMB, DHS, and CIGIE, in consultation with the Federal Chief Information Officer Council. The FY 2019 metrics represent a continuation of work begun in FY 2016, when the metrics were aligned with the five function areas in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risk.

Prior Work

OIG reviews IT security through the annual financial statement audit as well as its annual FISMA evaluation. The most recent reports include the following:

> Report 20-04, Independent Auditor's Report on SBA's FY 2019 Financial Statements (November 15, 2019).

Report 19-09, Weaknesses Identified During the FY 2018 Federal Information Security Management Act Review (April 9, 2019).

Appendix II: Assessment Maturity Level Definitions

	Maturity Level	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 strategy 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 strategy are collected across the organization and used to assess them and make necessary changes.
Level 5	optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

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 will serve as the domain rating.

Appendix III: Agency Comments

SBA U.S. Small Business Administration

Office of the Chief Information Officer

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

From: Maria Roat
Chief Information Officer
U.S. Small Business Administration

Subject: Management Response:
Draft FY 2019 Federal Information Security
Modernization Act Review, Project 19013

Dates: March 12, 2020

We appreciate the opportunity to review the draft report entitled "Weaknesses Identified during the FY 2019 Federal Information Security Modernization Act Review." We are encouraged that the Inspector General "observed improvement in cybersecurity oversight" in our continued delivery of resilient and cost-effective Enterprise Cybersecurity Services throughout the organization. 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 //

Maria Roat

Chief Information Officer