EVALUATION REPORT

WEAKNESSES IDENTIFIED DURING THE FY 2018 FEDERAL INFORMATION SECURITY MODERNIZATION ACT REVIEW

APRIL 9, 2019 REPORT NUMBER 19-09

EXECUTIVE SUMMARY

WEAKNESSES IDENTIFIED DURING THE FY 2018 FEDERAL INFORMATION SECURITY MODERNIZATION ACT REVIEW

Report No. 19-09

April 9, 2019

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 (1) to determine whether the Small Business Administration (SBA) complied with FISMA and (2) to 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 2018 Inspector General FISMA Reporting Metrics as issued by the Office of Management and Budget. We tested against these metrics by selecting a subset of 11 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 consistently implemented level for data protection and privacy, at a defined level for the six other domains, and at the ad hoc level for contingency planning. The results of control tests showed SBA had not completed contingency plan tests for two major systems. The overall program was evaluated as not effective due to SBA not achieving managed and measurable in any of the eight domains. These results are summarized in the following table.

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

*SBA's CyberScope domains were not rated at the managed and measurable, 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

As of February 28, 2019, in addition to the 5 open FISMA recommendations (appendix II), the Office of Inspector General made 18 additional recommendations in the following CyberScope domains: risk management (3), configuration management (3), identity and access management (5), data protection and privacy (3), information security and continuous monitoring (1), incident response (1), and contingency planning (2).

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 19-09

DATE: April 9, 2019

TO: Linda E. McMahon
Administrator

FROM: Hannibal "Mike" Ware
Inspector General

SUBJECT: Weaknesses Identified During the FY 2018 Federal Information Security Modernization Act Review

This report presents the results of our evaluation on weaknesses identified during the FY 2018 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 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 at (202) 205-6586 or Andrea Deadwyler, Assistant Inspector General for Audits, at (202) 205-6616.

cc: Pradeep Belur, Chief of Staff
Maria A. Roat, Chief Information Officer
Guy V. Cavallo, Deputy Chief Information Officer
Beau M. Houser, Chief Information Security Officer
Chris M. Pilkerton, General Counsel
Martin Conrey, Attorney Advisor, Legislation and Appropriation
Timothy E. Gribben, Chief Financial Officer and Associate Administrator for Performance Management
LaNae Twite, Director, Office of Internal Controls
Michael A. Simmons, Attorney Advisor

Table of Contents

Introduction

This report summarizes the results of our fiscal year (FY) 2018 Federal Information Security Modernization Act (FISMA) evaluation and assesses the maturity of controls used to address risks in each of the CyberScope domains. We initiated new recommendations where we identified new vulnerabilities. We did not initiate 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 and in the outstanding recommendations summarized in appendix II, Open IT Security Recommendations Related to FISMA.

FISMA requires federal agencies to develop, implement, and report on the effectiveness of each agency's information security program. For FY 2018, 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 2018 FISMA evaluation, KPMG, an independent public accounting firm, tested a representative subset of 11 SBA systems and security controls. OIG monitored KPMG's work and used test results to report SBA's compliance with the FY 2018 Inspector General FISMA Reporting Metrics as issued by the Office of Management and Budget (OMB), and in the CyberScope submission to the Department of Homeland Security (DHS) in October 2018.[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 (1) to determine whether SBA complied with FISMA and (2) to 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 18-02, Fiscal Year 2017–2018 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 2018 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 consistently implemented level for data protection and privacy, at a defined level for the six other domains, and at the ad hoc level for contingency planning. The results of control tests showed SBA had not completed contingency plan tests for two major systems. The overall program was evaluated as not effective due to SBA not achieving managed and measurable in any of the eight domains.

SBA's overall assessment was at the defined level and evaluated as not effective.[2] Within the context of the maturity model domains, performance below managed and measurable (i.e., ad hoc, defined, or consistently implemented) represents an ineffective level of security. To improve its FISMA effectiveness, SBA needs to proactively update and implement security operating procedures, remediate outstanding recommendations, 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, is 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 defined. This domain can be improved through resolution of three outstanding recommendations (appendix II, Risk Management, recommendations 1, 2, and 3) and the resolution of the improvement areas identified below.

System Hardware and Software Inventories Need to Be Consistently Maintained

SBA needs to consistently maintain its hardware and software asset inventories to ensure only authorized hardware and software are on its systems. SBA's implementation procedure for the NIST Risk Management Framework states that there must be a complete listing of hardware and software assets for each system. Our testing identified that inventories for hardware and software are not consistently maintained for all systems. Due to scanning software limitations, the Office of the Chief Information Officer (OCIO) could not identify all program offices' hardware and software inventories.

Enterprise Risk Management Strategy Needs to Be Formalized and Implemented

To ensure that SBA can identify and respond to risks, SBA needs to formalize and implement its enterprise risk management strategy. NIST SP 800-53 requires development and implementation of a comprehensive risk management strategy. At the time of our review, SBA's enterprise risk

[2] NIST SP 800-53, Revision 4, defines security control effectiveness as the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies.

management strategy was in draft and had not been implemented. A formalized risk management strategy is necessary to ensure that SBA can safeguard federal assets and provide efficient service delivery to the public.

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 22 open POA&Ms due on or before September 11, 2018, that were not remediated by the scheduled completion date. Our review found that SBA does not adhere to its established remediation dates and program offices are not amending the scheduled POA&M completion dates to accurately reflect the remediation status. Additionally, the OCIO does not ensure that the program offices provide justification for missed milestones, and milestone amendments were not documented for the past due POA&Ms.

Oversight of Systems Security Risk and Control Needs Improvement

To be aware of its actual security posture and to identify and mitigate risks, SBA needs to improve its oversight of its system security risk and control. SBA IT Security Policy, SOP 90 47 4, mandates that system owners design an authorization and risk profile. Our testing identified that two SBA systems did not receive security risk assessments, and six SBA systems did not receive security control assessments, as required by this policy. The recommendation for this finding was previously identified in OIG Report 14-12.[3] See appendix II, Risk Management, recommendation 1.

Independent Assessment and Analysis of Contractor Systems' Security Posture Need to Be Conducted

SBA needs to conduct independent assessment and analysis of contractor systems' security posture to determine that the contractors' security controls were designed, implemented, and operating effectively in accordance with SBA security requirements. SBA IT Security Policy, SOP 90 47 4, states that OCIO has overall responsibility for the SBA IT Security Program, including conducting independent assessment and compliance reviews. Our testing identified that SBA has no assurance that security controls were implemented by two third-party service providers. SBA management did not enforce contractual requirements for contractor information security reporting. Furthermore, SBA did not perform an internal assessment for one of the contractors. The recommendation for this finding was previously identified in OIG Report 18-14.[4] See appendix II, Risk Management, recommendation 3.

Recommendations

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

1. Enforce the risk management framework implementation procedures in establishing a process to maintain an accurate software and hardware inventory.

[3] OIG Report 14-12, Weaknesses Identified During the FY 2013 Federal Information Security Management Act Review, recommendation 2.
[4] OIG Report 18-14, Weaknesses Identified During the FY 2017 Federal Information Security Modernization Act Review, recommendation 3.

2. Formally implement and communicate the enterprise risk management strategy across the organization.

3. Update the plan of action and milestones to reflect progress against milestone completion dates, justification for revised milestones, status of all related remediation efforts, and amendments to plan of 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.

Configuration Management Controls Need to Be Defined or Implemented

To reduce the risk of outside threats and outdated configuration baselines, SBA needs to implement configuration management plans. SBA IT Security Policy, SOP 90 47 4, states that a configuration plan must be developed, implemented, and maintained for every system. Our testing indicated that SBA could not provide a configuration management plan or Service Organization Control (SOC) 1 report for one of its systems.

Baseline Configuration Deviations Require Approval

SBA should require approvals for baseline configuration deviations to reduce the risk that deviations in baseline configurations may not be remediated. NIST SP 800 53 states that an organization should identify, document, and approve exceptions from established configuration settings. Due to management oversight, SBA could not provide a rationale or approval for baseline configuration deviations for one system.

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 2017 review. Due to inconsistent application of the SBA IT Security Policy, SOP 90 47 4, identified systems may not be securely configured and/or updated.

Recommendations

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

4. Ensure all systems have a configuration management plan that is implemented and maintained as required by SBA IT Security Policy, SOP 90 47 4.

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

6. 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, SOP 90 47 4.

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 resolution of one outstanding recommendation (appendix II, Identity and Access Management, recommendation 4) and the remediation of the five vulnerabilities identified below.

Continuous Diagnostics Mitigation Program Should Be Formalized and Implemented

OMB memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems, requires SBA to implement the DHS Continuous Diagnostics Mitigation (CDM) program.[5] This guidance requires the Agency to identify and mitigate security risks in four phases. During the review, SBA could not provide evidence of an Identity, Credential, and Access Management strategy as required by phase 2 of CDM. Phase 2 monitors and validates that users' privileges are properly aligned with their work responsibility and need to know. Full implementation of CDM is needed for agencies to prioritize and mitigate cybersecurity vulnerabilities.

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 a listing for new users added during FY 2018, nor could it provide evidence that access granted to new users added in FY 2018 was appropriate for two systems.

Personal Identification Verification Enforcement Exemptions Require Approvals

SBA needs to improve its processes for personal identification verification (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 an employee is temporary, they have forgotten their PIV for the day, or they are being issued a new one. Our testing identified that SBA could not provide approvals for these exemptions for 4 out of 15 selected workstations.

Audit Logging Controls Need to Be Implemented

To reduce the risk that vulnerabilities could go undetected, SBA needs to define and implement its audit logging procedure. SBA IT Security Policy, SOP 90 47 4, states that audit logging procedures include sufficient information to determine when events have occurred, as well as the source and outcome of the event. In addition, audit log data must be archived for at least 180 days. Our testing identified that three systems tested could not provide evidence that they have audit logging controls that are appropriately defined and implemented.

[5] Consistent with the federal government's deployment of information security continuous monitoring (ISCM), the CDM program is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides agencies with tools and capabilities to prioritize and mitigate cybersecurity vulnerabilities.

Session Timeouts Settings Need to Be Implemented

SBA needs to implement its session timeout 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 lockout for 30 minutes, unless the account is unlocked by an administrator. Our testing identified that one system inherited the lockout settings from the vendor, and that users were able to set their own lockout times.

Recommendations

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

7. Develop a plan to continue implementation of the Department of Homeland Security Continuous Diagnostics Mitigation program's requirements as outlined by the federal identity and access management strategy, as required by OMB memorandum M-14-03.

8. Develop a process that ensures timely retrieval of access authorizations of new users as required by SBA IT Security Policy, SOP 90 47 4.

9. Maintain approvals for removing personal identification verification enforcement on SBA workstations as required by SBA IT Security Policy, SOP 90 47 4.

10. Develop a process to ensure that evidence of audit logging of privileged users is maintained as required by SBA IT Security Policy, SOP 90 47 4.

11. Work with the vendor to ensure lockout settings meet SBA policy as required by SBA IT Security Policy, SOP 90 47 4.

Data Protection and Privacy

The data protection and privacy domain requires implementation of policies and procedures to protect personal identifiable information (PII), as well as the response required if such information is disclosed without authorization. We determined that the Agency's maturity level was consistently implemented. This domain can be improved through the resolution of the one outstanding recommendation (appendix II, Identity and Access Management, recommendation 4) and the remediation of the four vulnerabilities identified below.

Controls for Desktop Hardware and Legacy Assets Need to Be Implemented

To reduce the risk that information could be stolen or corrupted through unauthorized access of desktop hardware and legacy assets, SBA needs to implement controls to protect PII. SBA IT Security Policy, SOP 90 47 4, requires that PII stored on SBA IT resources be encrypted using an approved Federal Information Processing Standard 140-2 encryption method. Our testing identified that SBA has not implemented encryption over desktop hardware or legacy assets. SBA management determined that there are compensating physical controls in place to prevent removal of hardware that may contain PII and therefore decided not to implement encryption.

Universal Serial Bus Controls Need to Be Implemented

SBA needs to ensure its Universal Serial Bus (USB) drives are encrypted to ensure, that in the event they are lost or stolen, PII cannot be accessed. SBA IT Security Policy, SOP 90 47 4, states that any

PII stored on USB drives must be encrypted using a Federal Information Processing Standard 140-2 encryption method. Our testing identified that SBA has not implemented encryption for USB drives that may contain PII.

Sanitation/Reuse and Disposal of Hardware Assets Need to Be Monitored

To ensure that PII or sensitive information is not accessed by unauthorized individuals, SBA needs to ensure that its hardware has been properly sanitized. SBA IT Security Policy, SOP 90 47 4, states that hardware assets are to be sanitized in accordance with NIST 800-88 Guidelines for Media Sanitization, before disposal or transfer outside of SBA.

NIST 800-88 states that documentation should be maintained as to what was sanitized, the process, the date, and a final disposition. Our testing identified that SBA does not have a centralized process in place concerning monitoring and tracking of hardware that has been sanitized or disposed of. Due to the decentralized nature of SBA's program offices, SBA was unable to provide evidence that all hardware was sanitized before reuse or disposal.

Privacy Impact Assessments Need to Be Conducted

SBA needs to ensure privacy impact assessments (PIAs) are conducted for required systems to ensure risks are identified and a process is established to respond to privacy risks. SBA IT Security Policy, SOP 90 47 4, states that conducting a PIA is one the primary responsibilities of system owners. In addition, a PIA must be completed as part of the assessment and authorization process. Our testing identified that one of the systems tested had not conducted or maintained a PIA.

Recommendations

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

12. Implement encryption on desktops, legacy hardware assets, and universal serial bus drives as required by SBA IT Security Policy, SOP 90 47 4.

13. Develop a centralized process to monitor and track hardware that has been sanitized before reuse or disposal as required by SBA IT Security Policy, SOP 90 47 4.

14. Ensure privacy impact assessments are completed 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. Users also should be properly designated, monitored, and trained. We determined that the Agency's maturity level was defined. This area was identified as defined because role-based training was not implemented. The Agency has subsequently included role-based training.

Information Security Continuous Monitoring

Information security continuous monitoring (ISCM) 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. The effectiveness of ISCM oversight can be improved through resolution of recommendations identified below.

Security Control Assessments Need to Be Performed

To ensure security controls are implemented correctly, SBA needs to perform full security assessments. SBA's Information System Continuous Monitoring Policy details minimum frequency levels of review depending on the control risk associated with the application. These reviews may occur as frequently as daily but no more than annually. Our testing identified that for one system, the controls were not being assessed within these frequencies, unless the system was undergoing a reauthorization to operate.

Authorizations to Operate Need to Be Updated and Maintained

SBA needs to improve its process to update a system's authorization to operate (ATO) to identify and mitigate risks resulting from the continued operation and to update critical information contained in authorization packages. SBA IT Security Policy, SOP 90 47 4, states that all systems that have undergone a full security risk assessment of NIST SP 800-53 controls have a current ATO. Our testing identified that one system could not provide evidence that an ATO was within the 3-year requirement. Due to management oversight, the ATO was not completed, and therefore could not be provided. The recommendation for this finding was previously identified in OIG Report 15-07.[6] See appendix II, Risk Management, recommendation 2.

Recommendation

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

15. Ensure that all systems have current up-to-date security control assessments as required by SBA IT Security Policy, SOP 90 47 4.

Incident Response

The incident response domain relates to protecting information systems. Incident response relates to establishing and implementing policies and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. We determined that the Agency's maturity level was defined. The effectiveness of incident response oversight can be improved through resolution of the one outstanding recommendation (appendix II, Incident Response, recommendation 5) and the remediation of the vulnerability identified below.

Incident Response Procedures Need to Be Consistently Implemented

SBA needs to consistently implement incident response procedures to reduce the risk of unauthorized access or unidentified security incidents, both of which can lead to greater risk of data loss. NIST SP 800-53 requires that organizations retain audit records to provide support for after-the-fact investigations of security incidents. Our testing identified that SBA was unable to provide evidence of tickets between October 2017 and March 2018, because archived tickets were irretrievable due to data loss and limitations of the system used to archive tickets.

IT incidents need to be reported within the established timeframes to reduce the risk that security events may not be properly reported, documented, or contained. SBA cybersecurity incident response procedures state that all confirmed incidents must be reported to the U.S. Computer

[6] OIG Report 15-07, Weaknesses Identified During the FY 2015 Federal Information Security Management Act Review, recommendation 5.

Emergency Readiness Team (US-CERT) within 1 hour of detection. Our testing indicated that out of 25 tickets selected, 9 were not reported to US-CERT within the 1-hour requirement. If incidents are not reported within the established timeframe, there is a greater risk that security events may not be properly documented or contained, and that notifications to affected parties will be delayed.

Recommendation

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

16. Strengthen the audit logging process of incident tickets to limit lost tickets and ensure that the current process for tracking incidents that are reported are compliant with US-CERT requirements.

Contingency Planning

NIST SP 800-53 requires that organizations must develop contingency plans. These plans must address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. We reviewed SBA's Continuity of Operations Plan and determined that the Agency's maturity level was ad hoc. The effectiveness of contingency planning oversight can be improved through the resolution of the issues identified below.

Alternate Processing and Storage Site Needs to Be Established

SBA needs to establish alternative processing and storage sites to ensure they can resume critical operations should the primary processing capabilities become unavailable. NIST SP 800-53 requires that major systems have an alternate processing and storage site. Our testing identified that SBA lacked an alternate processing location for one of its general support systems. The recommendation for this finding was previously identified in OIG Report 18-14.[7] Following completion of fieldwork, this issue was remediated.

Contingency Planning Strategies Require Lessons Learned

To increase the effectiveness of contingency plan strategies and to ensure plan operability, SBA needs to require tests and lessons learned be conducted annually. SBA IT Security Policy, SOP 90 47 4, states that contingency plans must be developed and tested annually. Our testing identified that two systems did not complete a test of the contingency plan within the required annual timeframe. Due to lack of resources, and management oversight, contingency tests were not conducted as required. The recommendation for this finding was previously identified in OIG Report 18-14.[8] Following completion of fieldwork, this issue was remediated.

Business Impact Analysis Are Required for Contingency Planning Activities

To prioritize the restoration of critical functions that will allow the system to continue to support the agency mission, SBA needs to ensure that a business impact analysis (BIA) is included in contingency planning activities, as required by SBA IT Security Policy, SOP 90 47 4. Our testing identified that SBA could not provide a BIA for one of its systems. Due to management oversight, SBA was not able to provide a BIA that was integrated in a contingency test plan.

[7] OIG Report 18-14, Weaknesses Identified During the FY 2017 Federal Information Security Modernization Act Review, recommendation 9.
[8] OIG Report 18-14, Weaknesses Identified During the FY 2017 Federal Information Security Modernization Act Review, recommendation 9.

Backups Contractor and Cloud Systems Need to Be Conducted and Reviewed

SBA needs to conduct and review backups of contractor and cloud systems. In the event of a disaster recovery event, loss of data could occur if backups are not being completed by the vendor. SBA IT Security Policy, SOP 90 47 4, states that system and data owners should ensure confidentiality, integrity, and availability of agency data through regular backups. Our testing identified that SBA could not provide evidence that they are ensuring that backups are being conducted for contractor and cloud-hosted systems. SBA did not request Service Organization Controls (SOC) 1 or SOC 2 reports that would evidence those backups of agency data are being conducted.

Recommendations

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

17. Coordinate with SBA program offices to complete a business impact analysis that is incorporated into the contingency plan of each system as required by SBA IT Security Policy, SOP 90 47 4.

18. Coordinate with SBA program offices to ensure that systems hosted by contractors and cloud vendors are backed up as required by SBA IT Security Policy, SOP 90 47 4.

Analysis of Agency Response

SBA management concurred with all 18 recommendations in their written response to the draft report and provided corrective action plans in separate documents. In all instances, we found that the planned corrective actions resolved or closed the recommendation. These responses are summarized below.

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 enforce risk management implementation procedures to maintain software and hardware inventories. This recommendation can be closed when management provides evidence that hardware and software inventories are consistently maintained. Final action is scheduled to occur by July 31, 2019.

2. **Resolved.** SBA agreed with our recommendation to formally implement and communicate the enterprise risk management strategy across the organization. This recommendation can be closed when management provides evidence that the enterprise risk management strategy is implemented. Final action is scheduled to occur by July 31, 2019.

3. **Resolved.** SBA agreed with our recommendation to work with program offices to update identified past due POA&Ms, to include progress on completion dates, justifications for revised milestones, status of remediated efforts, and amendments to past due POA&Ms. This recommendation can be closed when management provides evidence that POA&Ms are updated accordingly. Final action is scheduled to occur by June 30, 2019.

4. **Closed.** SBA agreed with our recommendation to ensure that all systems have an implemented and maintained configuration management plan. Therefore, OIG considers the final action complete.

5. **Resolved.** SBA agreed with our recommendation to establish a process for deviating from baseline configurations. This recommendation can be closed when management provides evidence that there is an approval and justification for deviations from baseline configurations. Final action is scheduled to occur by July 31, 2019.

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. Final action is scheduled to occur by June 30, 2019.

7. **Resolved.** SBA agreed with our recommendation to continue implementation of CDM. This recommendation can be closed when management provides evidence of continued implementation of CDM. Final action is scheduled to occur by June 30, 2019.

8. **Resolved.** SBA agreed with our recommendation to develop a process for timely retrieval of access authorizations for new users. This recommendation can be closed when management provides evidence that access authorizations are available in a timely manner. Final action is scheduled to occur by August 31, 2019.

9. **Resolved.** SBA agreed with our recommendation to maintain approvals for PIV removal on workstations. This recommendation can be closed when management provides evidence that approvals for PIV removal are available. Final action is scheduled to occur by June 30, 2019.

10. **Resolved.** SBA agreed with our recommendation to develop processes for audit logging of privileged users. This recommendation can be closed when management provides evidence that audit logging for privileged users has been established. Final action is scheduled to occur by July 31, 2019.

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. Final action is scheduled to occur by August 31, 2019.

12. **Resolved.** SBA agreed with our recommendation to implement encryption on desktops, hardware assets, and USBs. This recommendation can be closed when management provides evidence that encryption is implemented according to SBA IT Security Policy. Final action is scheduled to occur by August 31, 2019.

13. **Resolved.** SBA agreed with our recommendation to develop a process to monitor and track hardware that has been sanitized before reuse or disposal. This recommendation can be closed when management provides evidence that processes are in place to ensure hardware is sanitized before being reused or disposed of in accordance with SBA IT policy. Final action is scheduled to occur by August 31, 2019.

14. **Closed.** SBA agreed with our recommendation and subsequently has completed PIAs for the systems that require them. Therefore, OIG considers the final action complete.

15. **Closed.** SBA agreed with our recommendation and subsequently has completed security control assessments for all systems SBA agreed with our recommendation to ensure all systems have up-to-date security control assessments. Therefore, OIG considers the final action complete.

16. **Resolved.** SBA agreed with our recommendation to limit lost tickets by strengthening the audit process and ensuring that tracking incidents are compliant with US-CERT. This recommendation can be closed when management provides evidence that the audit logging process has been improved and incidents are tracked. Final action is scheduled to occur by June 30, 2019.

17. **Resolved.** SBA agreed with our recommendation to complete a business impact analysis that is incorporated into a system's contingency plan. This recommendation can be closed when management provides evidence of a business impact analysis that has been incorporated into the contingency plan. Final action is scheduled to occur by June 30, 2019.

18. **Resolved.** SBA agreed with our recommendation to ensure contractor and cloud systems are being backed up. This recommendation can be closed when management provides evidence that SBA is ensuring that cloud and contractor systems are being backed up according to SBA IT policy. Final action is scheduled to occur by May 31, 2019.

Appendix I: Objective, Scope, and Methodology

Our objectives were (1) to determine whether the Small Business Administration (SBA) complied with the Federal Information Security Modernization Act (FISMA) of 2014 and (2) to 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 policy, 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 Office of Management and Budget (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 11, 2018, the FY 2018 Inspector General FISMA Reporting Metrics were issued to provide instructions for agencies to meet their FY 2018 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 fiscal year (FY) 2018 FISMA evaluation, KPMG, an independent public accounting firm, with agreement from the Office of Inspector General (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 2018.

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 2018 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 2018 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 18-14, Weaknesses Identified During the FY 2017 Federal Information Security Management Act Review (March 20, 2018).

Report 17-14, Weaknesses Identified During the FY 2016 Federal Information Security Management Act Review (June 15, 2017).

Report 16-10, Weaknesses Identified During the FY 2015 Federal Information Security Management Act Review (March 10, 2016).

Report 15-07, Weaknesses Identified During the FY 2014 Federal Information Security Management Act Review (March 13, 2015).

Report 14-12, Weaknesses Identified During the FY 2013 Federal Information Security Management Act Review (April 30, 2014).

Appendix II: Open IT Security Recommendations Related to FISMA

As of February 28, 2019, there were five open audit recommendations to correct identified control weakness and vulnerabilities. We've indicated below which of the control areas were recurring in the FY 2018 review. All these unresolved recommendations directly affect the Small Business Administration's (SBA's) CyberScope evaluation as it relates to Federal Information Security Modernization Act (FISMA) compliance. The Office of Management and Budget (OMB) Circular A-50 states that agencies' audit followup systems must require prompt resolution and corrective actions on audit recommendations.

Risk Management[9]

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, is the program and supporting processes to manage information security risk to organizational operations, organizational assets, individuals, other organizations, and the nation. Past audits found weaknesses in the Agency's risk management. To address these weaknesses, we made the following recommendations to SBA:

1. Improve the quality of security authorization packages for SBA systems and ensure that all required documentation is included in all authorization packages. This includes:
    a. Requiring that risk assessments are updated yearly for all general support systems and major applications;
    b. Ensuring that systems security plans are timely and accurately completed for all relevant general support systems and major applications;
    c. Ensuring that security assessment reports are timely and accurately completed for all relevant general support systems and major applications;
    d. Creating plans of actions and milestones for all general support systems and major applications when vulnerabilities are identified during security control assessments or other evaluations. Additionally, enter the vulnerabilities identified during review into the Cyber Security Asset Management tool. OIG Report 14-12, recommendation 2, closure was due 09/30/2018.[10]

2. Ensure that SBA general support systems and major applications have valid and up-to-date authorizations to operate while those systems are in production. OIG Report 15-07, recommendation 4, closure was due 09/30/2018.

3. Perform independent assessment and analysis of contractor systems' security posture to ascertain compliance with SBA's security policies and Federal requirements. OIG Report 18-14, recommendation 3, closure was due 01/01/2019.

Configuration Management

FISMA requires that organizations develop minimally acceptable system configuration requirements to ensure a baseline level of security for information technology (IT) operations and assets.[11] Our past audits identified weaknesses in this domain. However, all recommendations in this domain are considered closed.

[9] All three findings in this domain are duplicated in the FY 2018 report.
[10] In FY 2016, this condition was repeated. We did not initiate a duplicate recommendation.
[11] 44 U.S.C. 3554 (b) (2) (D) (iii), Federal Agency Responsibilities (December 18, 2014).

Identity and Access Management

SBA IT Security Policy, SOP 90 47 4, states the Agency is required to identify and authenticate system users and limit system users to the information, functions, and information systems those users are authorized to operate. Our past audits found weaknesses in SBA's account management and meeting authentication strength requirements. To address these weaknesses, we made the following recommendation to SBA:

4. To ensure that digital rights management is used to prevent unauthorized distribution, we recommend that OCIO establish detailed policies and procedures regarding data exfiltration and implement a robust data exfiltration program across the Agency. OIG Report 17-14, recommendation 5, closure was due 03/31/2019.

Security and Privacy Training

System users should have proper IT security training relevant to their IT security role and to the system. Users also should be properly designated, monitored, and trained.[12] Our past audits identified weaknesses in this domain. However, all recommendations in this domain are considered closed.

Information System Continuous Monitoring

Information system continuous monitoring is essential to an organization to determine ongoing effectiveness of information systems.[13] All recommendations in this area are considered closed.

Incident Response

Incident response and reporting is a control to protect information systems. Policies and procedures should be implemented that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.[14] Our past audits found weaknesses in SBA's incident response and reporting. To address these weaknesses, we made the following recommendation to SBA:

5. Establish a Trusted Internet Connection security control to ensure that all Agency traffic, including mobile and cloud, are routed through defined and secure access points. OIG Report 17-14, recommendation 9, closure was due 01/31/2019.

Contingency Planning

NIST SP 800-53 states that contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised.[15] Our past audits identified weaknesses in this domain. However, all recommendations in this domain are considered closed.

---

[12] SBA SOP 90 47 4, Information System Security Program, "Security and Privacy Awareness Training" (September 8, 2017).
[13] NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organization, Chapter 1 (April 2013).
[14] NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control IR-1 (April 2013).
[15] NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control CP-1 (April 2013).

Appendix III: 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 IV: Agency Comments

Office of the Chief Information Officer

MEMORANDUM FOR:	HANNIBAL M. WARE INSPECTOR GENERAL U.S. SMALL BUSINESS ADMINISTRATION
THRU:	BEAU M. HOUSER CHIEF INFORMATION SECURITY OFFICER U.S. SMALL BUSINESS ADMINISTRATION
Subject:	Management Response: Draft Fiscal Year 2018 Federal Information Security Modernization Act Review, Project 18011
Dates:	March 25, 2019

We appreciate the opportunity to provide comments on the draft report entitled, "Weaknesses Identified during the Fiscal Year (FY) 2018 Federal Information Security Modernization Act Review." The Office of the Chief Information Officer has no comments and concurs with all recommendations.

The Office of the Chief Information Officer remains committed to providing quality Information Technology (IT) services and has made it a priority to significantly improve its Cybersecurity program.

APPROVED:

BEAU HOUSER Digitally signed by BEAU HOUSER Date: 2019.03.25 13:58:43 -04'00'

Beau M. Houser
Chief Information Security Officer
U.S. Small Business Administration