

EVALUATION REPORT

WEAKNESSES IDENTIFIED DURING THE FY 2017 FEDERAL INFORMATION SECURITY MODERNIZATION ACT REVIEW





EXECUTIVE SUMMARY

WEAKNESSES IDENTIFIED DURING THE FY 2017 FEDERAL INFORMATION SECURITY MODERNIZATION ACT REVIEW

Report No.
18-14

March 20,
2018

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 seven CyberScope domains: risk management, configuration management, identity and access management, 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 2017 Inspector General FISMA Reporting Metrics*. 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 risk management and configuration management and at the defined level for the other domains. The overall program was evaluated as not effective. These results are summarized in the following tables.

Legend SBA CyberScope Maturity Level*

| | |
|---------------------------------|--|
| Defined | Policies, procedures, and strategy are formalized and documented but not consistently implemented. |
| Consistently Implemented | Policies, procedures, and strategy are consistently implemented, but effectiveness measures are lacking. |

| CyberScope Domain | Maturity Level |
|---|--------------------------|
| Risk Management | Consistently Implemented |
| Configuration Management | Consistently Implemented |
| Identity and Access Management | Defined |
| Security Training | Defined |
| Information Security Continuous Monitoring | Defined |
| Incident Response | Defined |
| Contingency Planning | Defined |

*SBA's CyberScope domains were not rated at the ad hoc, 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 14, 2018, in addition to the 17 open FISMA recommendations (Appendix II), OIG made 11 additional recommendations in the following CyberScope domains: risk management (3), identity and access management (2), security training (3), and contingency planning (3). SBA management concurred with all 11 recommendations.




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

Final Report Transmittal
Report Number 18-14

DATE: March 20, 2018

TO: Linda E. McMahon
Administrator

FROM: Hannibal "Mike" Ware 
Acting Inspector General

SUBJECT: *Weaknesses Identified During the FY 2017 Federal Information Security
Modernization Act Review*

This report presents the results of our evaluation on weaknesses identified during the FY 2017 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 at (202) 205-6586 or Andrea Deadwyler, Assistant Inspector General for Audits, at (202) 205-6616.

cc: Allie Leslie, Deputy Administrator
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 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..... | 1 |
| Objectives..... | 1 |
| Results..... | 2 |
| Risk Management..... | 2 |
| Implementation of Information Security Guidance Needs Improvement..... | 2 |
| Plan of Action and Milestone Remediation Dates Are Not Monitored..... | 3 |
| Oversight of Systems Security Risk and Control Needs Improvement..... | 3 |
| Independent Assessment and Analysis of Contractor Systems' Security Posture Not Conducted..... | 3 |
| Recommendations..... | 3 |
| Configuration Management..... | 4 |
| Identity and Access Management..... | 4 |
| Verification Systems for Physical Access at All SBA Offices and Field Sites Not in Place..... | 4 |
| Systems Account Recertification Controls Need Improvement..... | 4 |
| Recommendations..... | 5 |
| Security Training..... | 5 |
| Security Awareness and Training Was Not Consistently Implemented and Completed..... | 5 |
| Principal and Specialized IT Personnel Did Not Take Specialized Training..... | 5 |
| IT Workforce Training Needs Assessment Not Performed..... | 6 |
| Recommendations..... | 6 |
| Information Security Continuous Monitoring..... | 6 |
| Incident Response..... | 6 |
| Aggregation and Analysis Tools and File Integrity Checking Software Is Not Used..... | 6 |
| Contingency Planning..... | 7 |
| Contingency Plans and Alternate Processing and Storage Site Not Established..... | 7 |
| Backups for Four Major Systems Were Not Performed..... | 7 |
| Recommendations..... | 7 |
| Analysis of Agency Response..... | 8 |
| Summary of Actions Necessary to Close the Report..... | 8 |
| Appendix I: Objective, Scope, and Methodology..... | 11 |
| Maturity Levels..... | 11 |
| Prior Work..... | 12 |
| Appendix II: Open IT Security Recommendations Related to FISMA..... | 13 |
| Risk Management..... | 13 |
| Configuration Management..... | 13 |
| Identity and Access Management..... | 14 |

| | |
|--|----|
| Continuous Monitoring Management | 15 |
| Incident Response | 15 |
| Contingency Planning | 16 |
| Appendix III: Assessment Maturity Level Definitions..... | 17 |
| Appendix IV: Agency Comments | 18 |

Introduction

This report summarizes the results of our fiscal year (FY) 2017 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.

FISMA requires Federal agencies to develop, implement, and report on the effectiveness of each agency's information security program. For FY 2017, the Office of Inspector General (OIG) was required to report on the following domains: risk management, configuration management, identity and access management, security training, information security continuous monitoring, incident response, and contingency planning.

Federal agencies are required to annually submit a FISMA CyberScope report, an online collection tool, to the Department of Homeland Security (DHS) on October 31. As part of the FY 2017 FISMA evaluation, OIG tested a representative subset of 11 SBA systems and their security controls. We 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. In addition, we tested against SBA's standard operating procedure (SOP) 90 47 3, *Information System Security Program*.

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, security training, information security continuous monitoring, incident response, and contingency planning.

Results

To determine whether SBA complied with FISMA, we assessed the maturity of SBA's information security program as outlined in the *FY 2017 Inspector General FISMA Reporting Metrics*.

Inspectors General are required to assess the effectiveness of information security programs on a maturity model spectrum. Tests using the FISMA metrics indicated that SBA made progress in the risk management and configuration management domains. However, within the context of the maturity model, performance below managed and measurable (i.e., ad hoc, defined, or consistently implemented) represents an ineffective level of security. Using the maturity model, we assessed SBA at the defined level and evaluated the program as not effective.¹

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.

Risk Management

Risk management, as outlined in National Institute of Standards and Technology (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. Without an effective security and risk management program, including oversight of contractor systems, SBA management may not be aware of the actual security posture of the Agency and may not identify and sufficiently mitigate risks.

We determined that the Agency's maturity level was consistently implemented. This domain can be improved through resolution of two outstanding recommendations (Appendix II) and the resolution of the three improvement areas identified below.

Implementation of Information Security Guidance Needs Improvement

SBA does not have an effective process to ensure that Federal guidance is implemented within 1 year from the date of final publication, as required by Office of Management and Budget (OMB) Memorandum 14-04. Our testing identified that SBA did not issue entity-level guidance on NIST SP 800-53 within the required time frame. NIST SP 800-53, Revision 4, was issued in April 2013 and required authorizing officials to ensure that comprehensive continuous monitoring processes for information systems are in place prior to commencing operations. At the time of our review, the Agency was using *Information System Security Program* (SOP 90 47 3), which was based on outdated guidance. On September 8, 2017, SBA issued *Information Technology Security Policy* (SOP 90 47 4), which incorporated the NIST SP 800-53, Revision 4, requirement, more than 4 years after NIST issued the new guideline.

¹ 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.

Plan of Action and Milestone Remediation Dates Are Not Monitored

Our review found that SBA does not adhere to its established remediation dates and program offices are not amending the scheduled plan of action and milestones (POA&M) completion dates to accurately reflect the remediation status. Additionally, the Office of the Chief Information Officer (OCIO) does not ensure that the program offices provide justification for missed milestones, and milestone amendments were not documented for the past due POA&M. Our testing identified 66 open POA&M due on, or before, June 13, 2017, that were not remediated by the scheduled completion date. Forty-four of the 66 were open and not remediated, 11 were identified as finished but were denied closure, and 11 were identified as finished and pending assessment for closure.

Oversight of Systems Security Risk and Control Needs Improvement

SOP 90 47 3 established guidelines for a system security authorization and risk profile. Our testing identified that 5 SBA systems did not receive security risk assessments, and 10 SBA systems did not receive security control assessments, as required by this policy. According to SBA management, the OCIO IT security group lacked the resources required to complete security control, and security risk assessments for all SBA systems in FY 2017. Without an effective security and risk management program, including oversight of contractor systems, SBA management may not be aware of the actual security posture of the Agency, and risks may not be identified and sufficiently mitigated. This finding was previously identified in OIG Report 14-12.² See Appendix II, Risk Management, Recommendation 1.

Independent Assessment and Analysis of Contractor Systems' Security Posture Not Conducted

Our testing identified that SBA has no assurance that security controls were implemented by three third-party service providers. SBA management did not enforce contractual requirements for contractor information security reporting. Furthermore, SBA did not perform an internal assessment to determine that the contractors' security controls were designed, implemented, and operating effectively in accordance with SBA security requirements.

Recommendations

1. We recommend that the Office of the Chief Information Officer, in coordination with SBA program offices, develop internal processes to implement Federal information security guidance within established deadlines.
2. We recommend that the Office of the Chief Information Officer 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.
3. We recommend that the Office of the Chief Information Officer perform independent assessment and analysis of contractor systems' security posture to ascertain compliance with SBA's security policies and Federal requirements.

² OIG Report 14-12, *Weaknesses Identified During the FY 2013 Federal Information Security Management Act Review*, Recommendation 2.

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 consistently implemented. This domain can be improved through resolution of three outstanding recommendations (Appendix II). The results of this year's FISMA test work indicate that SBA continues to lack a comprehensive hardware and software inventory system. A comprehensive hardware and software inventory application mitigates the risks that the confidentiality and integrity of the systems and data therein are compromised. This finding was previously identified in OIG Report 17-14.³ See Appendix II, Configuration Management, Recommendation 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 nine outstanding recommendations (Appendix II) and the remediation of the two improvement areas identified below.

Verification Systems for Physical Access at All SBA Offices and Field Sites Not in Place

Personal identity verification (PIV) is a common means of authentication for access to an agency's facilities, networks, and information systems. Our testing identified that SBA had not implemented PIV for physical access across the Agency's field sites, in accordance with DHS Memorandum for the Heads of All Departments and Agencies, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 Policy*, and SOP 90 43 0, *Procedure for Personal Identity Verification (PIV) Credential (Cards) to Access SBA's Facilities, Network, and Information System*. SBA did not possess a current listing of PIV-enforced physical access offices and could not provide a documented plan to implement PIV for physical access across the Agency's various locations, as required. Without a plan to implement PIV for physical access, the Agency does not have a clear direction or established timeline with milestones to complete the effort.

Systems Account Recertification Controls Need Improvement

SOP 90 47 3 requires biannual account recertification. Our testing identified that three systems could not provide documentation that a review of external users was conducted on a biannual basis in FY 2017. In addition, two of the three systems could not provide evidence that a review of internal users was conducted on a biannual basis in FY 2017. Due to a lack of training and guidance, the program offices were unaware of how to properly conduct the biannual access recertifications for the systems. This finding was previously identified in OIG Report 12-15.⁴ See Appendix II, Identity and Access Management, Recommendation 6.

Independent Reviews Not Performed

SOP 90 47 3 and NIST SP 800-53 require that individuals performing audit log reviews must be objective and impartial. Only authorized security personnel should have access to modify or delete audit records. In the event that audit log compilation or consolidation occurs, appropriate

³ OIG Report 17-14, *Weaknesses Identified During the FY 2016 Federal Information Security Modernization Act Review*, Recommendation 4.

⁴ OIG Report 12-15, *Improvement Is Needed in SBA's Separation Controls and Procedures*, Recommendation 3.

precautions against unauthorized deletion or modification of audit trails must be implemented on any consolidated servers used for reporting or analysis. The lack of independent reviews can impact the integrity of the data processed by and stored within the system.

Due to a lack of resources and managerial awareness of appropriate audit logging procedures, there was no independent review performed for one of the selected system's audit logs for administrative actions. The system's administrators performing the audit log reviews also had root access on the production application and database servers. By not enforcing independent audit log reviews, there is an increased risk that unauthorized activity and other relevant security events may go undetected.

Recommendations

4. We recommend that the Office of the Chief Information Officer, in conjunction with the Office of Management and Administration, develop and implement a plan for SBA personal identity verification for physical access for SBA field sites as required by Homeland Security Presidential Directive 12 and SOP 90 43 0.
5. We recommend that the Office of the Chief Information Officer enforce segregation of duties or implement mitigating controls to help ensure that personnel performing security functions, such as database and system administrators, are restricted from modifying audit records and reporting audit log reviews to management.

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. The effectiveness of security training can be improved through resolution of the three improvement areas identified below.

Security Awareness and Training Was Not Consistently Implemented and Completed

SBA's security awareness and training strategy is not consistently implemented in accordance with SOP 90 47 3 and NIST SP 800-53. This SOP requires that Cyber Security Awareness Training (CSAT) be made available and completed within specific time frames. This training was neither available nor completed within these time frames. All authorized users are required to take CSAT prior to accessing the network, as well as annually. Our testing noted that 227 out of 1,430 network users with access to SBA network as of May 15, 2017, were not registered to take CSAT as of August 4, 2017.

Principal and Specialized IT Personnel Did Not Take Specialized Training

NIST SP 800-53 requires that IT personnel with significant information security and privacy responsibilities complete adequate security related training relevant to their roles. Furthermore, SBA policies require specialized training for personnel with specialized IT roles and responsibilities. Our testing identified that 53 out of 61 users identified by OCIO as IT personnel with significant information security and privacy responsibilities had not completed the specialized training. Furthermore, our test identified 32 users with IT security responsibilities who were not included on OCIO's list. Additional tests showed that personnel with specialized IT roles and responsibilities were only required to take generic privacy and information security training that does not adequately prepare the personnel for their specific roles and responsibilities.

IT Workforce Training Needs Assessment Not Performed

SBA has not conducted an assessment of the knowledge, skills, and abilities of its workforce to tailor its specialized training as required by NIST SP 800-50, *Computer Security*. By not conducting periodic reviews or an appropriate skills assessment, SBA cannot update their security awareness training needs based on the skills of their personnel and workforce. Having outdated or irrelevant training materials could lead to having a workforce not prepared for potential security threats.

Recommendations

6. We recommend that the Office of the Chief Information Officer, in coordination with other SBA program offices, design and implement controls to ensure that all SBA network and privileged users complete Cyber Security Awareness Training within timelines required by SBA's policy.
7. We recommend that the Office of the Chief Information Officer, in coordination with other SBA program offices, design and implement controls to ensure that all principle and specialized users complete role-based training.
8. We recommend that the Office of the Chief Information Officer, in coordination with OHRS and other SBA program offices, design and implement a skills assessment that will be used to evaluate and train SBA's workforce.

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 in the CyberScope domains of risk management and incident response.

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 two outstanding recommendations (Appendix II) and full implementation of the SOP identified below.

Aggregation and Analysis Tools and File Integrity Checking Software Is Not Used

Our test identified that SBA did not use an aggregation and analysis tool and file integrity checking software to detect changes made to important files during incidents. SOP 90 47 3 and NIST SP 800-53 require the Chief Information Security Officer to develop an Agency-wide incident response plan that covers reportable incidents. The plan requires the Chief Information Security Officer to list resources and management support needed to effectively maintain an incident response maturity level. SBA does not have adequate technology resources necessary to effectively implement the incident response program. Without the implementation of an aggregation and analysis tool, SBA cannot effectively identify unusual or inappropriate activity trends. Without file integrity checking

software, SBA cannot detect alterations to important files during incidents, thus, leading to loss of integrity to SBA data and information. This finding was previously identified in OIG Report 17-14.⁵ See Appendix II, Incident Response, Recommendation 15.

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 defined. The effectiveness of contingency planning oversight can be improved through resolution of one outstanding recommendation (Appendix II) and the resolution of the improvement areas identified below.

Contingency Plans and Alternate Processing and Storage Site Not Established

OCIO was unable to complete the system's Information System Contingency Plan (ISCP) test in FY 2017, as required by NIST SP 800-53. OCIO could not provide test results and lessons learned for a major system because their resources were allocated to support disaster tasks during August and September 2017. Without a contingency plan test, OCIO is unable to address weaknesses in the system and its operating components. This finding was previously identified in OIG Report 16-10.⁶ See Appendix II, Contingency Planning, Recommendation 17.

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. Without an alternate processing site, OCIO is unable to determine whether it is able to resume critical operations should the primary processing capabilities become unavailable.

Backups for Four Major Systems Were Not Performed

SOP 90 47 3 and NIST SP 800-53 require that major systems perform daily incremental backups and monthly full backups. OCIO could not provide sufficient evidence that required backups were performed for four major systems tested. We further noted that SBA could not provide evidence that daily incremental and weekly full backups were performed throughout the period of October 1, 2016, to August 15, 2017, for 9 out of 15 selected servers. Weaknesses in the backup process and procedures can lead to loss of SBA data and an incomplete record of data for disaster recovery procedures.

Recommendations

9. We recommend that the Office of the Chief Information Officer complete their Information System Contingency Plan tests in accordance with SOP 90 47 4 requirements.
10. We recommend that the Office of the Chief Information Officer, in coordination with SBA program offices, establish alternate processing sites for all major general support systems and applications to help ensure that data is recoverable in the event that the primary site becomes unavailable, as required by NIST SP 800-53.

⁵ OIG Report 17-14, *Weaknesses Identified During the FY 2016 Federal Information Security Modernization Act Review*, Recommendation 7.

⁶ OIG Report 16-10, *Weaknesses Identified During the FY 2015 Federal Information Security Management Act Review*, Recommendation 4.

11. We recommend that the Office of the Chief Information Officer, in coordination with SBA program offices, perform information system backups and maintain evidence of retention in a manner consistent with program needs and SOP 90 47 4.

Analysis of Agency Response

SBA management concurred with all 11 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 recommendations. These responses are summarized below.

Summary of Actions Necessary to Close the Report

The following provides the status of each recommendation and the necessary action to either resolve or close the recommendation.

- 1. Develop internal processes to implement Federal information security guidance within established deadlines.**

Closed. OCIO has developed and implemented an Agency-wide IT security policy and an implementation guide for the NIST Risk Management Framework. Both of these policies are aligned with NIST 800-53, Revision 4. Therefore, OIG considers the final action complete.

- 2. 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.**

Resolved. OCIO has stated that it will work with the program offices to update identified past due POA&M, to include milestone changes, revised anticipated completion dates, and mitigating strategies where applicable. This recommendation can be closed when SBA provides evidence that past due POA&Ms have been updated accordingly. Final action is scheduled to occur by February 1, 2019.

- 3. Perform independent assessment and analysis of contractor systems' security posture to ascertain compliance with SBA's security policies and Federal requirements.**

Resolved. OCIO stated that they will undertake security and risk assessments for the identified contractor IT systems in accordance with SBA's *Information Technology Security Policy* and NIST 800-37, Revision 1. This recommendation can be closed when SBA provides evidence that security and risk assessments have been updated. Final action is scheduled to occur by January 1, 2019.

- 4. Develop and implement a plan for SBA personal identity verification for physical access for SBA field sites as required by Homeland Security Presidential Directive 12 and SBA SOP 90 43 0.**

Resolved. OCIO stated that they will work with the Office of Management and Administration to produce a plan for the overall implementation of PIV-based physical access to SBA field sites. This recommendation can be closed when SBA provides evidence that a plan has been implemented for PIV access. Final action is scheduled to occur by February 28, 2019.

- 5. Enforce segregation of duties or implement mitigating controls to help ensure that personnel performing security functions, such as database and system administrators, are restricted from modifying audit records and reporting audit log reviews to management.**

Resolved. OCIO stated that they will improve the audit log review process to ensure independence and separation of duties. This recommendation can be closed when SBA provides evidence that an audit log review process is in place. Final action is scheduled to occur by September 30, 2018.

- 6. Design and implement controls to ensure that all SBA network and privileged users complete Cyber Security Awareness Training within timelines required by SBA's policy.**

Resolved. OCIO stated that they will update SBA CSAT content, communicate the training requirement to all users, and track program office completion. This recommendation can be closed when SBA provides evidence that CSAT training has been updated. Final action is scheduled to occur by September 30, 2018.

- 7. Design and implement controls to ensure that all principle and specialized users complete role-based training.**

Resolved. OCIO stated that they will design role-based SBA CSAT training content, communicate the training requirement to all users with significant IT security responsibilities, and track program office completion. This recommendation can be closed when SBA provides evidence that CSAT training is updated for specialized users. Final action is scheduled to occur by September 30, 2018.

- 8. Design and implement a skills assessment that will be used to evaluate and train SBA's workforce.**

Resolved. OCIO, in partnership with the Office of the Chief Human Capital Officer, initiated a strategic IT workforce planning effort in October 2017 to collect the IT capability requirements, develop a holistic approach to determine IT personnel requirements, and develop an IT competency and workforce plan. In addition, OCIO stated that the as-is analysis is completed, and the to-be and gap analysis phases are underway. OCIO expects the SBA IT workforce plan to be completed in April 2018, with execution beginning in 2018 Q4. This recommendation can be closed when SBA provides evidence that a workforce skills assessment has been implemented. Final action is scheduled to occur by September 30, 2018.

- 9. Complete the Information System Contingency Plan tests in accordance with SOP 90 47 4.**

Resolved. OCIO will conduct a FY 2018 contingency plan test for the LAN/WAN environment to include support subsystems. This recommendation can be closed when SBA provides evidence that the contingency plan has been tested. Final action is scheduled to occur by September 30, 2018.

- 10. Establish alternate processing sites for all major general support systems and applications to help ensure that data is recoverable in the event that the primary site becomes unavailable, as required by NIST SP 800-53.**

Resolved. OCIO stated that it will research options and develop a plan for establishing an alternate processing site for the Headquarters Data Services System (HQDSS) and supported applications. This recommendation can be closed when SBA provides evidence that an alternate processing site is established. Final action is scheduled to occur by February 28, 2019.

11. Perform information system backups and maintain evidence of retention in a manner consistent with program needs and SOP 90 47 4.

Resolved. OCIO stated that they will ensure that system backups are performed for all identified systems in accordance with SBA SOP 90 47 4, *Information Technology Security Policy*. This recommendation can be closed when SBA provides evidence showing that backups are being performed. Final action is scheduled to occur by June 1, 2018.

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 seven CyberScope domains: risk management, configuration management, identity and access management, 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 17, 2017, the *FY 2017 Inspector General FISMA Reporting Metrics* were issued to provide instructions for agencies to meet their FY 2017 reporting requirements. The metrics required an independent assessment of agencies' information security programs. The reporting metrics were developed as a collaborative effort among OMB, the Department of Homeland Security (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) 2017 FISMA evaluation, KPMG, an independent public accounting firm, with agreement from the Office of Inspector General (OIG), tested a representative subset of Small Business Administration (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 2017.

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

Report 17-03, *Independent Auditors' Report on SBA's FY 2016 Financial Statements* (November 14, 2016).

Report 16-17, *Fiscal Year 2016 Report of the U.S. Small Business Administration (SBA) Pursuant to The Cybersecurity Act of 2015, Section 406, Federal Computer Security* (August 10, 2016).

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

Report 15-12, *Improvement Is Needed in SBA's Separation Controls and Procedures* (May 26, 2015).

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

Report 15-02, *Independent Auditors' Report on SBA's FY 2014 Financial Statements* (November 17, 2014).

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

Report 14-04, *Independent Auditors' Report on SBA's FY 2013 Financial Statements* (December 16, 2013).

Appendix II: Open IT Security Recommendations Related to FISMA

As of February 14, 2018, there are 17 open audit recommendations that 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 follow-up systems must require prompt resolution and corrective actions on audit recommendations.

Risk Management

Identifying information system risk ensures that SBA minimizes vulnerabilities. Risk management includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system.⁷ 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 is due 09/30/2018.⁸
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 is due 09/30/2018.

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.⁹ Our past audits and reviews identified weaknesses in the development of baseline configurations and other configuration-related controls. To address these weaknesses, we made the following recommendations to SBA:

3. Enforce a network access security baseline(s) across the network, consistent with SBA security policy, Office of Management and Budget directives, and United States Government Configuration Baseline requirements. OIG Report 14-04, Recommendation 7, Closure is due 03/31/2018.

⁷ SBA SOP 90 47 3, *Information System Security Program*, Appendix C (August 28, 2012).

⁸ In FY 2016, this condition was repeated. We did not initiate a duplicate recommendation.

⁹ 44 U.S.C. 3554 (b) (2) (D) (iii), Federal agency responsibilities (December 18, 2014).

4. To ensure that hardware, and software licenses are updated to maintain accurate inventories, we recommend that OCIO implement an automated tool to ensure these inventories are updated annually. IG Report 17-14, Recommendation 4, Closure is due 03/16/2018.
5. We recommend the CIO coordinate with SBA program offices to address existing configuration and patch management vulnerabilities. In addition, implement procedures to ensure consistent implementation/monitoring of approved security configuration baselines. IG Report 17-03, Recommendation 9, Closure is due 09/30/2018.

Identity and Access Management

SBA policies state 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.¹⁰ Our past audits found weaknesses in SBA's account management and meeting authentication strength requirements. To address these weaknesses, we made the following recommendations to SBA:

6. Perform periodic recertification reviews of end users in Agency general support systems to ensure that users are authorized and have current access privileges. Alternatively, design compensating controls for recertification for end users of general support systems. IG Report 12-15, Recommendation 3, Closure is due 03/31/2018.
7. Implement procedures to ensure that user access, including user accounts and associated roles, is reviewed on a periodic basis consistent with the nature and risk of the system, and any necessary account modifications be performed when identified. IG Report 16-02, Recommendation 2, Closure is due 03/31/2018.
8. Improve SBA's administration of logical system access by taking the following actions:
 - a. Implement an effective off-boarding process, and periodically verify that controls to remove logical access for separated employees are implemented and operating as designed;
 - b. Establish a process for the identification and removal of separated contractors to help ensure that access is timely removed upon contractor separation; and
 - c. Timely remove access to general support systems and major applications (including development and test environments) when employees and contractors are terminated. IG Report 16-02, Recommendation 4, Closure is due 03/31/2018.
9. Continuously monitor remote access audit logs for potential unauthorized activity. IG Report 12-15, Recommendation 4, Closure is due 03/31/2018.
10. Implement procedures to ensure that user access, including user accounts and associated roles, is reviewed periodically consistent with the nature and risk of the system. IG Report 14-04, Recommendation 5, Closure is due 03/31/2018.
11. To ensure that digital rights management is used to prevent unauthorized distribution, we recommend that OCIO establish detailed policies and procedures regarding data

¹⁰ SBA SOP 90 47 3, *Information System Security Program*, Chapter 7 (August 28, 2012).

exfiltration and implement a robust data exfiltration program across the Agency. OIG Report 17-14, Recommendation 5, Closure is due 06/01/2018.

12. To ensure sensitive data residing on a server or in use is protected, OCIO should implement data rights management capabilities. OIG Report 17-14, Recommendation 6, Closure is due 12/31/2018.
13. We recommend the CIO implement procedures to ensure that user access is reviewed periodically consistent with the nature/risk of the system and account modifications are performed when identified and accounts are independently reviewed for appropriateness. OIG Report 17-03, Recommendation 4, Closure is due 03/31/2018.
14. Improve SBA's administration of logical system access by taking the following actions:
 - a. Implement an effective off-boarding process, and periodically verify that controls to remove logical access for separated employees are implemented and operating as designed;
 - b. Establish a process for the identification and removal of separated contractors to help ensure that access is timely removed upon contractor separation; and
 - c. Timely remove access to general support systems and major applications (including development and test environments) when employees and contractors are terminated. OIG Report 17-03, Recommendation 6, Closure is due 03/31/2018.

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.¹¹ Our past audits identified weaknesses in this domain. However, all outstanding recommendations in this domain are considered closed.

Continuous Monitoring Management

Continuous monitoring is essential to an organization to determine ongoing effectiveness of information systems.¹² Our past audits identified weaknesses in this domain. However, all outstanding 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.¹³ Our past audits found weaknesses in SBA's incident response and reporting. To address these weaknesses, we made the following recommendations to SBA:

15. To ensure automated collection of log data, we recommend that OCIO, where feasible, implement an automated mechanisms tool and file integrity checking that are configured

¹¹ SBA SOP 90 47 3, *Information System Security Program, "Roles and Responsibilities"* (August 28, 2012).

¹² NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organization*, Chapter 1 (April 2013).

¹³ NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Control IR-1 (April 2013).

for aggregation/analysis of log data and to detect changes to significant files, respectively. Additionally, update the incident response plan to include procedures for using such automated capabilities. OIG Report 17-14, Recommendation 7, Closure is due 6/30/2018.

16. We recommend that OCIO 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 is due 06/30/2018.

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.¹⁴ A past audit identified weaknesses. To address this weakness, we made the following recommendation to SBA:

17. Information system contingency plans are tested and consistent with the NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requirements for the Federal Information Processing Standards 199 categorization of each major general support system and application. OIG Report 16-10, Recommendation 4, closure is due 12/01/2018.

¹⁴ 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. |

Appendix IV: Agency Comments



MEMORANDUM FOR: HANNIBAL M. WARE
INSPECTOR GENERAL (ACTING)
U.S. SMALL BUSINESS ADMINISTRATION

THRU: MARIA A. ROAT
CHIEF INFORMATION OFFICER
U.S. SMALL BUSINESS ADMINISTRATION

Subject: Management Response:
Draft FY 2017 Federal Information Security Modernization Act
Review, Project 17010

Dates: February 21, 2018

We appreciate the opportunity to provide comments on the draft report entitled, “Weaknesses Identified during the FY 2017 Federal Information Security Modernization Act Review”, and thank the Inspector General’s staff for their consideration of our response. We concur with all eleven recommendations.

The Office of the Chief Information Officer remains committed to providing quality Information Technology (IT) services and has made it a priority to continue to improve its enterprise cybersecurity program. We appreciate your audit recommendations, as they will help improve our overall security posture.

APPROVED:

MARIA ROAT

Digitally signed by MARIA
ROAT
Date: 2018.02.21 15:12:28
-05'00'

Maria A. Roat
Chief Information Officer
U.S. Small Business Administration