

EVALUATION REPORT

WEAKNESSES IDENTIFIED DURING THE FY 2016 FEDERAL INFORMATION SECURITY MODERNIZATION ACT REVIEW





EXECUTIVE SUMMARY

WEAKNESSES IDENTIFIED DURING THE FY 2016 FEDERAL INFORMATION SECURITY MODERNIZATION ACT REVIEW

Report
No. 17-14

June 15, 2017

What OIG Reviewed

This report summarizes the results of our reviews of the Cybersecurity Information Sharing Act of 2015 (Section 406) and the Federal Information Security Modernization Act (FISMA).

Our objective under the Section 406 review was to report on the design and implementation of the SBA's cybersecurity logical access controls and information security management controls. The results of our Section 406 review are included in the FISMA controls areas noted below.

Our objective under FISMA was to assess SBA's compliance and progress in CyberScope areas for fiscal year (FY) 2016. We tested SBA's controls and reviewed open recommendations from past reviews to evaluate SBA's progress in eight areas: risk management, contractor systems, configuration management, identity and access management, security and privacy training, continuous monitoring, incident response, and contingency planning.

We contracted with an independent public accountant to perform review procedures relating to Section 406 and FISMA, and we monitored their work in both areas. We reported SBA's compliance with Section 406 in August 2016.¹ Related recommendations from this Section 406 review are being included in this report.

What OIG Found

In FY 2016, SBA met the established guidelines in the contingency planning area. However, controls testing identified limited or no progress in four areas—risk management, contractor systems, configuration management, and identity and access management—due to a lack of management oversight, resources, and the absence of formalized processes. The following table summarizes progress over the prior reporting period by Cyberscope area.

CyberScope Area	Status
Risk Management	Limited Progress
Contractor Systems	Limited Progress
Configuration Management	Limited Progress
Identity and Access Management	Limited Progress
Security and Privacy Training	Substantial Progress
Continuous Monitoring	Progress
Incident Response	Progress
Contingency Planning	Substantial Progress

OIG Recommendations

In addition to the 28 open FISMA recommendations in Appendix II, OIG made 9 new recommendations to address Section 406 and FISMA-related vulnerabilities.

Agency Response

SBA management agreed with the findings and all nine new recommendations of this report. The Office of the Chief Information Officer further stated that they remain committed to providing quality information technology services and have made it a priority to significantly improve their cybersecurity program.

¹ Report 16-17, *Fiscal Year 2016 Report of the U.S. Small Business Administration Pursuant to the Cybersecurity Act of 2015, Section 406, Federal Computer Security*.




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

Final Report Transmittal
Report Number: 17-14

DATE: June 15, 2017

TO: Linda E. McMahon
Administrator



FROM: Hannibal "Mike" Ware
Acting Inspector General

SUBJECT: *Weaknesses Identified During the FY 2016 Federal Information Security
Modernization Act Review*

This report represents the results of our evaluation on weaknesses identified during the FY 2016 Federal Information Security Modernization Act (FISMA). Our objectives were to (1) determine whether the Small Business Administration complied with FISMA, (2) assess progress in each of the CyberScope areas, and (3) report results of the Cybersecurity Information Sharing Act of 2015 (Section 406) review.

We considered management comments on a draft of this report when preparing the final report. SBA management agreed with the findings and all nine new recommendations of this 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 Jeffrey R. Brindle, Director, IT and Financial Management Group, at (202) 205-7490.

cc: Joseph P. Loddo, Chief Operating Officer
Maria A. Roat, Chief Information Officer
Mary Anne Bradfield, Chief of Staff
Eric Benderson, Acting 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

Table of Contents

Introduction.....	1
Objectives.....	1
Results.....	2
Risk Management.....	2
Integrating Risk Management and Internal Controls.....	2
Central Repository for System Interconnections Not Updated.....	2
Current NIST Security Controls Have Not Been Implemented.....	3
Recommendations.....	3
Contractor Systems.....	3
Recommendation.....	3
Configuration Management.....	4
Vulnerabilities Were Not Timely Remediated.....	4
Hardware, Software Inventory and Licenses Not Updated.....	4
Recommendation.....	4
Identity and Access Management.....	4
Data Exfiltration Policies and Data Rights Management Capabilities Need Improvement.....	5
Recommendations.....	5
Continuous Monitoring.....	5
Incident Response.....	5
No Automated Tool for Log Data.....	5
Incident Response Processes Not Consistent.....	5
Trusted Internet Connection Not Established.....	6
Baseline of Network Operations Not Established.....	6
Recommendations.....	6
Contingency Planning.....	6
Analysis of Agency Response.....	7
Summary of Actions Necessary to Close the Report.....	7
Appendix I: Scope and Methodology.....	9
Progress Ratings.....	9
Prior Work.....	10
Appendix II: Open IT Security Recommendations Related to FISMA.....	11
Risk Management.....	11
Contractor Systems.....	11
Configuration Management.....	11
Identity and Access Management.....	12

Security and Privacy Training	14
Continuous Monitoring Management	14
Incident Response	15
Contingency Planning	15
Appendix III: ISCM Maturity Level Definitions.....	16
Appendix IV: Agency Comments	17

Introduction

This report summarizes the results of our fiscal year (FY) 2016 Federal Information Security Modernization Act (FISMA) evaluation and assesses progress in each of the CyberScope areas, as well as the results of the Cybersecurity Information Sharing Act of 2015 (Section 406) review. We assessed progress by testing controls and reviewing resolved and open recommendations. We initiated new recommendations where we identified additional vulnerabilities that the Small Business Administration (SBA) needs to remediate. We did not initiate duplicate recommendations in instances where SBA still needs to implement outstanding recommendations to remediate existing vulnerabilities.

FISMA requires Federal agencies to develop, implement, and report on the effectiveness of each agency's information security program. For FY 2016, the Office of Inspector General (OIG) was required to report on the following eight areas: risk management, contractor systems, configuration management, identity and access management, security and privacy training, continuous monitoring, incident response, and contingency planning.

Federal agencies are required to annually submit a FISMA CyberScope report on the above areas to the Department of Homeland Security (DHS). CyberScope is an online data collection tool administered by DHS to collect FISMA cybersecurity performance data. SBA submitted its FISMA CyberScope report to DHS on November 17, 2016.

As part of the FY 2016 FISMA evaluation, OIG tested a representative subset of SBA systems and security controls. We performed testing to assess the SBA's adherence to or progress in implementing minimum security standards and requirements commensurate with each system's security categorization and risk.

On August 11, 2016, we issued a report outlining SBA's compliance with selected security controls identified in Section 406 for systems that access personally identifiable information (PII). The results of our Section 406 review are included in the FISMA controls areas.

Objectives

Our objective under the Section 406 review was to report on the design and implementation of SBA's cybersecurity logical access controls and information security management controls. The results of our Section 406 review are included in the FISMA controls areas noted below.

Our objective under FISMA was to assess SBA's compliance and progress in CyberScope areas for FY 2016. We tested SBA's controls and reviewed open recommendations from past reviews to evaluate SBA's progress in eight areas: risk management, contractor systems, configuration management, identity and access management, security and privacy training, continuous monitoring, incident response, and contingency planning.

Results

SBA made substantial progress in the contingency planning FISMA area. Current year test results indicated improvement, including ensuring backups of enterprise servers were completed, backups are retained according to SBA policies, supply chain threats are considered, an alternate processing site is established, and after-action reports are generated. In addition, for the FISMA area of security and privacy training, no exceptions have been found.

However, SBA needs to address long-standing vulnerabilities identified in its configuration management and identity and access management areas. To demonstrate measurable progress, SBA needs to remediate the 28 open recommendations relating to FISMA reporting areas identified in Appendix II of this report. Our CyberScope results and open recommendations indicate limited progress in the following areas:

- risk management
- contractor systems
- configuration management
- identity and access management

In addition, Section 406 focuses on controls for current cybersecurity logical access and information security management monitoring. Section 406 also requires a report on selected security controls for systems that access PII.

Using FISMA and Section 406 results, we assessed the overall capability of the information technology (IT) security environment. The results of the assessment are summarized below.

Risk Management

Risk management, as outlined in National Institute of Standards and Technology (NIST) SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, is vital to an organization in developing, implementing, and maintaining safeguards against vulnerabilities. In FY 2016, CyberScope metrics assessed SBA as “defined,” or having developed comprehensive policies and procedures (as outlined in Appendix III ISCM Maturity Level Definitions). SBA has two outstanding recommendations open in risk management.

Integrating Risk Management and Internal Controls

Our review found that although SBA has a risk management structure in place, key components as defined in NIST SP 800-37 have not been implemented. At the time of the review, the agency was evaluating and defining significant risks, mitigation measures, risk tolerances, and processes to oversee risk management decisions.

Central Repository for System Interconnections Not Updated

Our review found that the central repository for system interconnections in the Cyber Security Asset Management (CSAM) tool were not up-to-date as of April 28, 2016. Specifically, we found three interconnections that were in the CSAM tool but were not updated in the systems security plan, and three interconnections that were in the plan but were not identified in the CSAM tool. In addition, 3 out of 10 systems were not able to provide evidence that there was an Interconnection Security Agreement (ISA)/Memorandum of Understanding between the in-scope system and their

interfacing system. SBA standard operating procedure (SOP) 90 47 3 requires an ISA for all system interconnections between SBA and external systems.

Current NIST Security Controls Have Not Been Implemented

Our review for Section 406 found that SBA had not updated the current controls listed in NIST SP 800-53, which were required to be incorporated by April 2014. SBA has issued SOP 90 47 4, which incorporates NIST SP 800-53 Rev 4; however, as of July 6, 2016, this policy was still in draft. This issue was previously identified.

Recommendations

1. We recommend that the Office of the Chief Information Officer (OCIO) document policies and procedures regarding the organizational risk management strategy, and define the organization's significant risks, mitigation measures, risk tolerances, and processes as defined in NIST SP 800-37.
2. To ensure that SBA properly identifies all system interconnections between SBA and external systems, we recommend that the OCIO enforce SOP 90 47 3 requirements for establishing ISAs that define the types of permissible, and impermissible flow of information between SBA and external information systems.

Contractor Systems

We reviewed SBA's oversight of a selection of information systems operated by SBA contractors. We determined that SBA established and implemented a process to ensure that contracts/statements of work/solicitations for systems and services, as appropriate, included appropriate information security and privacy requirements and material disclosures, Federal Acquisition Regulation clauses, and clauses on protection, detection, and reporting of information. However, we identified weakness in security controls over PII, which includes an expired Memorandum of Agreement for a payroll system operated by an outside party for enforcement of security controls over PII.

Our review for Section 406 compliance found that SBA did not enforce two of the in-scope systems security controls between system providers. SBA did not enforce contractual obligations for system providers to provide documentation that security controls were designed, implemented, and operating according to SBA security requirements.² Due to the lack of contractor oversight, SBA may not be aware of security risks or the security posture.

Recommendation

3. To ensure that SBA enforces contract requirements over security controls, we recommend that the OCIO ensure SBA program offices have security controls implemented for contractor systems that comply with SBA policies and Federal requirements.

² SBA SOP 90.47.3, *Information System Security Program*, Appendix J - "SBA's POA&M Process" (August 28, 2012).

Configuration Management

Configuration management guidance requires that agencies document policies and ensure information system software is patched and configured securely. SBA had weaknesses in the areas of patch management, as well as hardware and software inventory.

Vulnerabilities Were Not Timely Remediated

Our review found that SBA did not consistently remediate weaknesses within stipulated guidelines for IT systems. Vulnerabilities identified in the FY 2015 FISMA review that had not been remediated remained open in the FY 2016 FISMA review. If vulnerabilities are not mitigated, there is increased risk that the SBA IT environment could be compromised. SBA has one open recommendation in this area.

Hardware, Software Inventory and Licenses Not Updated

Our review for Section 406 found that SBA did not update its network scanning tool to include all subnets within 1 of the 10 systems sampled. This was due to SBA having added subnets to the system while it was still in the process of updating its scanning tool to detect those additional subnets. By not scanning all subnets, there are increased risks to the confidentiality and integrity of the system. NIST SP 800-53 requires that all systems be accurately documented. Our review for Section 406 also found that SBA does not have an automated tool to account for software inventories and software licenses for 3 of the 10 systems sampled. Missing information includes the system owner, serial number, and license information. SBA policy requires all system inventories to have this information.³

Recommendation

4. To ensure that hardware, and software licenses are updated to maintain accurate inventories, we recommend that the OCIO implement an automated tool to ensure these inventories are updated annually.

Identity and Access Management

The identity and access management area defines policies and procedures for identifying users and ensures only authorized users can access SBA resources. According to OMB guidance, remote access is only allowed with two-factor authentication, where one of the factors is provided by a device separate from the computer gaining access.⁴ SBA continues to experience major challenges in implementing effective identify and access management controls as reflected by the Agency having 17 open OIG audit recommendations in these areas. These recommendations address the following:

- user accounts
- separation of duties
- timely end user recertification
- personal identification verification and two-factor authentication

³ SBA SOP 90.47.3, *Information System Security Program*, Chapter 5 Configuration Management.

⁴ OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).

- password complexity
- document retention
- logical system access
- system logging

Data Exfiltration Policies and Data Rights Management Capabilities Need Improvement⁵

Our review for Section 406 found that SBA does not have digital rights management procedures and capabilities to prevent unauthorized redistribution of digital media and restrict the usage of proprietary software, hardware, or content. In addition, although SBA does protect data being transmitted across the network, it does not have capabilities to protect data residing on a server or data in use by a user. As a result, SBA could be unaware of their security posture, which could expose the agency to risks of unauthorized access.

Recommendations

5. To ensure that digital rights management is used to prevent unauthorized distribution, we recommend that the OCIO establish detailed policies and procedures regarding data exfiltration and implement a robust data exfiltration program across the agency.
6. To ensure sensitive data residing on a server or in use is protected, the OCIO should implement data rights management capabilities.

Continuous Monitoring

Continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Our review found that SBA's continues to lack an Information System Continuous Monitoring policy.⁶

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.

No Automated Tool for Log Data

Our review of SBA found that no automated tool is used at the entity level for the aggregation and analysis of log data, and no file integrity checking software is used to detect changes made to important files during incidents. SBA continues to rely on manual/procedural methods in instances where automation would be more effective. Currently, SBA does not have the technological resources to implement this into the incident response program.

Incident Response Processes Not Consistent

Our review found that SBA does not consistently apply incident response processes as required by the United States Computer Emergency Response Team (US-CERT). Specifically, we found 3 out of

⁵ Data exfiltration is the unauthorized copying, transfer, or distribution of data from a computer or server.

⁶ In FY 2015 and FY 2016, this condition was previously identified and resolution was scheduled for 2/28/2017. We did not initiate a duplicate recommendation.

15 incidents were not reported to US-CERT within the 1-hour time frame. SBA's incident response plan requires all incidents that affect confidentiality, integrity, and or availability to be reported within 1 hour of detection. By not reporting within the required time frame, SBA risks having incidents not being contained or eradicated without compromise to the agency's data.

Trusted Internet Connection Not Established

Although SBA's local-area and wide-area network outbound traffic passes through DHS' EINSTEIN system, SBA has not set up a trusted internet connection (TIC) for its mobile and cloud traffic.⁷ OMB memorandum 16-04 requires all possible traffic, including mobile and cloud, go through a TIC. Not routing through a TIC increases the risk of data being compromised, due to the high number of external connections.

Baseline of Network Operations Not Established

Our review determined that SBA has not defined how it plans to use technology to develop and maintain a baseline of network operations and expected data flows for users and systems. NIST SP 800-83 recommends establishing baselines for network performance so that deviations from that baseline can be investigated. The lack of baselines could cause the agency to not detect suspicious network activity, which could compromise agency data. SBA does not have a program in place to monitor network operations and data flows for users and systems. This finding was previously reported in OIG Audit Report 14-04.⁸

Recommendations

7. To ensure automated collection of log data, we recommend that the OCIO, where feasible, implement an automated mechanisms tool and file integrity checking that are configured 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.
8. To ensure consistent incident responses, we recommend that the OCIO enhance the existing process through improved validation as well as reporting any incidents in accordance with US-CERT requirements.
9. To conform to OMB memorandum 16-04, we recommend that the OCIO establish a TIC security control to ensure that all agency traffic, including mobile and cloud, are routed through defined and secure access points.

Contingency Planning

We reviewed SBA's implementation of an enterprise-wide continuity/disaster recovery program. We identified one weakness in SBA's implementation of a continuity plan ensuring that backups of data were successful. This finding was previously reported in OIG Audit Report 17-03.⁹

⁷ EINSTEIN is an intrusion detection system used by DHS which consolidates and monitors an agency access points against unauthorized intrusions.

⁸ Report 14-04, *Independent Auditors' Report on SBA's FY 2013 Financial Statements*, Recommendation 7.

⁹ Report 17-03, *Independent Auditors' Report on SBA's FY 2016 Financial Statements*, Recommendation 10.

Analysis of Agency Response

SBA management provided formal comments that are included in their entirety in Appendix IV. SBA agreed with our nine recommendations.

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. Document policies and procedures regarding the organizational risk management strategy, and define the organization's significant risks, mitigation measures, risk tolerances, and processes as defined in NIST SP 800-37.**

Resolved. The OCIO stated it will produce an agency-wide implementation guide for the NIST Risk Management Framework, based on NIST SP 800-37 Revision 1. This recommendation can be closed when an implementation guide based on NIST SP 800-37 Revision 1 has been completed.

- 2. The OCIO enforce SOP 90 47 3 requirements for establishing ISAs that define the types of permissible, and impermissible flow of information between SBA and external information systems.**

Resolved. The OCIO stated it will clarify its IT security policy with regards to situations where an ISA is required, and produce a signed ISA, for the systems identified that were missing ISAs. This recommendation can be closed when SBA submits signed ISAs for the systems missing ISAs.

- 3. Ensure SBA program offices have security controls implemented for contractor systems that comply with SBA policies and Federal requirements.**

Resolved. The OCIO stated it will generate updated IT security language for IT acquisition efforts in accordance with agency policy and Federal requirements. The OCIO will vet such language through the Office of General Counsel, and provide to the Denver Finance Center. This recommendation can be closed when SBA submits evidence that security controls have been implemented.

- 4. Ensure that the OCIO implements an automated tool to ensure hardware and software inventories are updated annually.**

Resolved. The OCIO stated it will enhance its automated inventory capabilities to include all LAN/WAN subnets and ranges. This recommendation can be closed when SBA provides documentation evidencing that hardware and software inventories being updated on an annual basis.

- 5. Ensure that the OCIO establish detailed policies and procedures regarding data exfiltration and implement a robust data exfiltration program across the agency.**

Resolved. The OCIO stated it will implement a strategy supporting the prevention of data exfiltration by insiders. This recommendation can be closed when SBA submits evidence that a data exfiltration program has been implemented.

6. Ensure the OCIO implements data rights management capabilities.

Resolved. The OCIO stated it will provide a digital rights management solution. Delivery of a solution will include end-user training and associated documentation. This recommendation can be closed when evidence is submitted that data rights management has been implemented.

7. Ensure the OCIO, where feasible, implement an automated mechanisms tool and file integrity checking that are configured 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.

Resolved. The OCIO stated it will research the feasibility of implementing file integrity checking software, considering the appropriate scope of such a solution. This recommendation can be closed when file integrity software has been implemented and the incident response plan has been updated accordingly.

8. Ensure the OCIO enhance the existing process through improved validation as well as reporting any incidents in accordance with US-CERT requirements.

Resolved. The OCIO stated it has updated its cybersecurity incident response procedures as of April 30, 2017. This recommendation can be closed when the OCIO provides our office with the updated procedures that are compliant with US-CERT requirements.

9. To conform to OMB memorandum 16-04, ensure that the OCIO establish a TIC security control to ensure that all agency traffic, including mobile and cloud, are routed through defined and secure access points.

Resolved. The OCIO stated it will develop a strategy placing all systems behind TIC access points. This recommendation can be closed when the OCIO provides documentation evidencing this TIC access strategy.

Appendix I: Scope and Methodology

The Federal Information Security Modernization Act (FISMA) of 2014 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 reduce inefficient or wasteful reporting, change reporting guidelines for threats, and ensure that all agency personnel are responsible for complying with agency security programs.

As part of the fiscal year (FY) 2016 FISMA evaluation, KPMG, an independent public accountant, 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. KPMG used the results of these system reviews to focus the Section 406 report and provide an understanding of SBA's cybersecurity practices.

On October 30, 2015, OMB issued Memorandum 16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, providing instructions for agencies to meet their FY 2015-2016 reporting requirements under FISMA. This memorandum requires Inspectors General to answer a set of information security questions in CyberScope that evaluates agency implementation of security capabilities and measures their effectiveness.

On December 18, 2015, the Cybersecurity Information Sharing Act of 2015 (Section 406) was signed into law, which focuses on the current cybersecurity logical access controls and information security management monitoring controls. We subsequently submitted a report on August 11, 2016, outlining SBA compliance. We included identified vulnerabilities and related recommendations within the body of this report.

To determine SBA's compliance in both FISMA and the related Section 406 areas, OIG contracted with KPMG to perform review procedures relating to FISMA. KPMG interviewed SBA personnel, inspected documentation, and tested the effectiveness of SBA's information technology (IT) security controls. OIG monitored KPMG's work and reported SBA's compliance with FISMA with the agency FISMA CyberScope submission in November 2016.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency'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.

Progress Ratings

We measured progress in each CyberScope area by comparing FY 2016 CyberScope results to FY 2015 CyberScope results. We determined whether SBA made substantial progress, progress, or limited or no progress. Categories that have a 15 percent or more improvement were determined to make substantial progress. We considered an evaluation area where there was 5 to 15 percent improvement as progress. We judged limited as less than 5 percent improvement.

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 17-03, *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 Pursuant to the Cybersecurity Act of 2015, Section 406, Federal Computer Security* (August 11, 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

There are 28 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 as of March 9, 2017. The Office of Management and Budget 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.¹⁰ Past audits found weaknesses in the agency's risk management. To address these weaknesses, we recommended that 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 (POA&M) 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 (CSAM) tool. OIG Report 14-12, Recommendation 2, Closure was due 12/31/2014.¹¹
2. Ensuring that SBA general support systems and major applications have valid and up-to-date ATOs while those systems are in production. OIG Report 15-07, Recommendation 4, Closure was due 12/31/2015.

Contractor Systems

SBA program areas supported by a contractor-hosted system must have written agreements for the necessary support to effectively monitor, respond, report, and prevent incidents within the operating office.¹² Our past audits found weaknesses in this area. However, SBA does not have any outstanding recommendations in this area.

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

¹⁰ SBA SOP 90.47.3, *Information System Security Program*, Appendix C (August 28, 2012).

¹¹ In FY 2016 this condition was repeated. We did not initiate a duplicate recommendation.

¹² SBA SOP 90.47.3, *Information System Security Program*, Chapter 8 (August 28, 2012).

assets.¹³ Our past audits and reviews identified weaknesses in the development of baseline configurations and other configuration-related controls. We recommended that SBA:

3. Enhance security vulnerability management processes. Specifically, SBA should:
 - a. Redistribute procedures and train employees on the process for reviewing and mitigating security vulnerabilities;
 - b. Periodically monitor the existence of unnecessary services and protocols running on their servers and network devices;
 - c. Perform vulnerability assessments with administrative credentials and penetration tests on all SBA offices from a centrally managed location with a standardized reporting mechanism that allows for trending, on a regularly scheduled basis in accordance with National Institute of Standards and Technology (NIST) guidance;
 - d. Develop a more thorough approach to track and mitigate configuration management vulnerabilities identified during monthly scans; and
 - e. Monitor security vulnerability reports for necessary or required configuration changes to their environment. OIG Report 12-02, Recommendation 1, Closure was due 3/31/2012.
4. Implement configuration management policies and procedures for document retention (to include supporting evidence) to validate the authorization of operating system changes. OIG Report 12-02, Recommendation 14, Closure was due 9/28/2012.
5. 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 was due 9/30/2014. (B.5.1, Appendix II)

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.¹⁴ Our past audits found weaknesses in SBA's account management and meeting authentication strength requirements. To address these weaknesses, we recommended that 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. OIG Report 12-15, Recommendation 3, Closure was due 12/30/2012.
7. Develop and implement procedures for user access termination to ensure access for terminated or transferred personnel is removed from systems in a timely manner. OIG Report 13-04, Recommendation 7, Closure was due 9/30/2013.¹⁵
8. Grant elevated network privileges per business needs only and enforce the concept of least privilege or implement mitigating controls to ensure that activities performed using privileged network accounts (including service accounts) are properly monitored. OIG Report 14-04, Recommendation 13, Closure was due 12/31/2014.

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

¹⁴ SBA SOP 90.47.3, *Information System Security Program*, Chapter 7 (August 28, 2012).

¹⁵ In FY 2016 this condition was repeated. We did not initiate a duplicate recommendation.

9. Implement personal identification verification for logical access to all SBA systems. OIG Report 14-12, Recommendation 1, Closure was due 12/31/2014.
10. Ensure its network oversight includes enabled network accounts which have never been accessed. OIG Report 15-12, Recommendation 3, Closure was due 11/30/2015.
11. Implement and monitor procedures to ensure that access is appropriately granted to employees and contractors, consistent with the conditions on their access forms after all approvals have been obtained. OIG Report 16-02, Recommendation 1, Closure is due 3/31/2017.
12. 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. OIG Report 16-02, Recommendation 2, Closure is due 12/31/2016.
13. Grant elevated privileges per business needs only, and enforce the concept of least privilege or implement mitigating controls to ensure that activities performed using privileged accounts (including service accounts) are properly monitored. OIG Report 16-02, Recommendation 3, Closure is due 12/31/2016.
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 16-02, Recommendation 4, Closure is due 3/31/2017.
15. Improve SBA's information system logging and auditing program by:
 - a. Reviewing and rationalizing current audit and logging activities and capabilities to determine their effectiveness in addressing risks to systems and data, and their ability to implement effective and sustainable continuous monitoring;
 - b. Implementing and enforcing consistent and effective creation of audit records, capturing of relevant auditable events, auditing (i.e., manual or automated review of audit records) for specified events, and automated alerting on specified events across SBA's infrastructure using a risk based approach; and
 - c. Developing an agency-wide plan and schedule for implementation of the above recommendations. OIG Report 14-04, Recommendation 8, Closure was due 11/4/2016.
16. Clarify email access policies as defined in SOP 90 49.1. OIG Report 15-12, Recommendation 4, Closure was due 10/1/2015.
17. Implement two-factor authentication for public-facing internet applications. OIG Report 15-07, Recommendation 2, Closure was due 6/30/2015.
18. Continuously monitor remote access audit logs for potential unauthorized activity. OIG Report 12-15, Recommendation 4, Closure was due 12/30/2012.

19. Improve SBA's remote access program by (1) ensuring employees acknowledge compliance with security requirements prior to establishing a remote connection and (2) monitoring compliance with SOP 90 47 3. OIG Report 15-02, Recommendation 8, Closure was due 12/31/2015.
20. Improve SBA's information system logging and auditing program by taking the following actions: review and rationalize current audit and logging activities and capabilities to determine their effectiveness in addressing risks to systems and data; implement and enforce consistent and effective creation of audit records, capturing relevant auditable events, auditing (i.e., manual or automated review of audit records) for specified events, and automated alerting on specified events across SBA's infrastructure using a risk-based approach; retain evidence of the audit log review; and develop an agency-wide plan and schedule for implementing the above recommendations. OIG Report 16-02, Recommendation 5, Closure is due 3/31/2017.
21. 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. OIG Report 14-04, Recommendation 5, Closure was due 9/30/2014.
22. Require users to sign the remote access rules of behavior document. OIG Report 16-10, Recommendation 2, Closure is due 3/31/2017.
23. Upgrade SBA's remote access solution to time out after 30 minutes of inactivity.

Security and Privacy Training

System users should have proper IT security training relevant to their IT security role and to the system. Users should also be properly designated, monitored, and trained.¹⁶ Our past audits found identified weaknesses in this area. However, all outstanding recommendations in this area are considered closed.

Continuous Monitoring Management

Continuous monitoring is essential to an organization to determine ongoing effectiveness of information systems.¹⁷ Our past audits identified weaknesses in this area. To address these weaknesses, we recommended that SBA:

24. Implement the Information System Continuous Monitoring (ISCM) program requirement, which includes (1) finalizing and implementing the ISCM strategy, (2) identifying resource and skill requirements/gaps, and (3) identifying individuals to manage SBA ISCM program. Office of Inspector General (OIG) Report 15-07, Recommendation 1, Closure is due 2/28/2017.¹⁸

¹⁶ SBA SOP 90.47.3, *Information System Security Program, "Roles and Responsibilities"* (August 28, 2012).

¹⁷ NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organization*, Chapter 1 (April 2013).

¹⁸ In FY 2016, this condition was repeated. We did not initiate a duplicate recommendation.

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.¹⁹ Our past audits found weaknesses in SBA's incident response and reporting. To address these weaknesses, we recommended that SBA:

25. Enhance the current process for tracking incidents to ensure that SBA comprehensively validates incidents and implements controls so that incidents are reported compliant with United States Computer Emergency Response Team requirements. OIG Report 16-10, Recommendation 1, Closure was due on 9/30/2016.

Contingency Planning

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, states that organizations should develop contingency plans. The plan must address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.²⁰ A past audit identified weaknesses. To address this weakness, we recommended that SBA:

26. Ensure that data stored on enterprise servers are backed up monthly and retained for 1 year for disaster recovery and restoration purposes. OIG Report 15-07, Recommendation 6, Closure was due 9/30/16.
27. Ensure that incremental and full backups for all systems, including related support infrastructure, are configured and retained in accordance with SBA policies. OIG Report 16-02, Recommendation 10, closure date is due 3/31/2017.
28. Information system contingency plans are tested and consistent with the NIST SP800-53, Security and Privacy Controls for Federal Information Systems and Organization requirements for the FIPS 199 categorization of each major general support system and application. OIG Report 16-10, Recommendation 4, closure due date was established for 9/30/2016.

¹⁹ NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Control IR-1 (April 2013).

²⁰ NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Control CP-1 (April 2013).

Appendix III: ISCM Maturity Level Definitions

Level	ISCM Program Maturity Level	Definition
Level 1	ad hoc	Agency program is not formalized, and activities are performed in a reactive manner.
Level 2	defined	The organization has formalized its program through developing comprehensive policies, procedures, and strategies.
Level 3	consistently implemented	In addition to formalizing and defining its program (Level 2), the organization consistently implements its program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the program across the organization are not captured or utilized to make risk-based decisions.
Level 4	managed and measurable	In addition to being consistently implemented (Level 3), activities are repeatable, and metrics are used to measure and manage the implementation of the program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.
Level 5	optimized	In addition to being managed and measurable (Level 4), the organization's program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis, based on changes in business/mission requirements and a changing threat and technology landscape.

SBA Response to Evaluation Report



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 2016 Federal Information Security Modernization Act
Review, Project 16007

Dates: May 16, 2017

We appreciate the opportunity to provide comments on the draft report entitled, "Weaknesses Identified during the FY 2016 Federal Information Security Modernization Act Review", and thank the Inspector General's staff for their consideration of our response. The Office of the Chief Information Officer concurs with all nine recommendations.

SBA and 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:

MARIA ROAT Digitally signed by MARIA ROAT
Date: 2017.05.16 09:21:33 -0400

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