EVALUATION REPORT

WEAKNESSES IDENTIFIED DURING THE FY 2015 FEDERAL INFORMATION SECURITY MANAGEMENT ACT REVIEW

March 10, 2016

Report Number 16-10

EXECUTIVE SUMMARY

Evaluation Report No. 16-10

WEAKNESSES IDENTIFIED DURING THE FY 2015 FEDERAL INFORMATION SECURITY MANAGEMENT

What OIG Reviewed

The Federal Information Security Management Act (FISMA) requires that the Office of Inspector General (OIG) review the Small Business Administration's (SBA) Information Technology (IT) Security Program. Our objective was to assess SBA's compliance with FISMA and progress in Cyberscope areas for fiscal year (FY) 2015. We tested SBA's controls and reviewed open recommendations from past reviews to evaluate SBA's progress in 10 areas: (1) continuous monitoring management, (2) configuration management, (3) identity and access management, (4) incident response and reporting, (5) risk management, (6) security training, (7) plan of action and milestones, (8) remote access management, (9) contingency planning, and (10) contractor systems.

We contracted with an independent public accountant to perform review procedures relating to FISMA, monitored its work, and reported SBA's compliance with FISMA in the Agency FISMA filings in November 2015.

What OIG Found

In FY 2015, SBA made progress in some FISMA evaluation categories. SBA met the established guidelines in evaluation areas of configuration management and security training. While SBA continued to make progress in two categories, the remaining eight areas made limited or no progress due to a lack of management oversight and resources and the absence of formalized processes. As a result, information security weaknesses continue to occur in these eight areas.

Continuous Monitoring Management	Limited or No Progress
Configuration Management	Substantial Progress
Identity and Access Management	Limited or No Progress
Incident Response and Reporting	Limited or No Progress
Risk Management	Limited or No Progress
Security Training	Substantial Progress[1]
Plan of Action and Milestones	Limited or No Progress
Remote Access Management	Limited or No Progress
Contingency Planning	Limited or No Progress
Contractor Systems	Limited or No Progress

OIG Recommendations

In addition to the 31 open FISMA recommendations in Appendix II, OIG made 5 new recommendations to address FISMA-related vulnerabilities.

Agency Response

SBA management agreed with the findings and recommendations of this report. For the five new recommendations, SBA management provided documentation to support that two have been implemented. Therefore, these recommendations are considered closed. The Office of the Chief Information Officer reports that they remain committed to providing quality information technology services and has made it a priority to significantly improve its cybersecurity program.

[1] SBA satisfied all FY 2014 and FY 2015 Cyberscope questions in this area.

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

Final Report Transmittal
Report Number: 16-10

DATE: March 10, 2016

TO: Maria Contreras-Sweet
Administrator

Douglas Kramer
Deputy Administrator

Keith Bluestein
Deputy Chief Information Officer

FROM: Troy M. Meyer /s/
Assistant Inspector General for Audit

SUBJECT: *Weaknesses Identified During the FY 2015 Federal Information Security Management Act Review*

This report presents the results of our evaluation report on the weaknesses identified during the FY 2015 Federal Information Security Management Act review. The overall report is resolved. 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 cooperation that we received from your staff during our audit. Please contact me if you would like to discuss this report or any related issues.

cc: Nick Maduros, Chief of Staff
Melvin F. Williams, Jr., General Counsel
Martin Conrey, Attorney Advisor, Legislation and Appropriations
Tami Perriello, Chief Financial Officer
LaNae Twite, Director, Office of Internal Controls

Table of Contents

Introduction

The Federal Information Security Management Act (FISMA) requires Federal agencies to develop, implement, and report on the effectiveness of each agency's information security program. For fiscal year (FY) 2015, the Office of Inspector General (OIG) was required to report on the following 10 areas: (1) continuous monitoring, (2) configuration management, (3) identify and access management, (4) incident response and reporting, (5) risk management, (6) security training, (7) plan of action and milestones, (8) remote access management, (9) contingency planning, and (10) contractor systems.[2]

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 13, 2015.

Objectives

This report summarizes the results of our FY 2015 FISMA evaluation and assesses progress in each of the Cyberscope areas. We assessed progress by testing controls and reviewing resolved and open recommendations. We initiated new recommendations where we identified additional vulnerabilities that SBA needs to remediate. We did not initiate duplicate recommendations in instances where SBA still needs to implement outstanding recommendations to remediate existing vulnerabilities.

[2] In FY 2014, FISMA required we evaluate security capital planning. However, this was not an area that was required for review in FY 2015.

Results

SBA made progress in two FISMA evaluation categories in FY 2015. This included configuration management, in which the Agency defined standard baseline configurations, and security training, in which SBA personnel with specialized security positions undergo enhanced security training. However, SBA needs to address long-standing vulnerabilities identified in its configuration management, identity and access management, and contingency planning. To demonstrate measurable progress, SBA needs to remediate the 31 prior-year open recommendations relating to FISMA reporting areas identified in Appendix II of this report. Our Cyberscope results and open recommendations indicate limited or no progress in the following areas:

- continuous monitoring management,
- identity and access management,
- incident response and reporting,
- risk management,
- plan of action and milestones,
- remote access management,
- contingency planning, and
- contractor systems.

The results of each Cyberscope evaluation category are summarized below.

1. Continuous Monitoring Management

In FY 2015, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) introduced a five-level maturity model for evaluating the continuous monitoring management section of the Cyberscope questionnaire. The maturity model provides a framework rating for people, process, and technology and classifies the overall process in five levels: Level 1- ad hoc, Level 2- defined, Level 3- consistently implemented, Level 4 -managed and measurable, and Level 5 - optimized (See Table 1 for complete maturity level definitions).

Table 1. IG ISCM Maturity Model Definitions

Level	ISCM Program Maturity Level	Definition
Level 1	ad hoc	ISCM program is not formalized, and ISCM activities are performed in a reactive manner.
Level 2	defined	The organization has formalized its ISCM program through developing comprehensive ISCM policies, procedures, and strategies.
Level 3	consistently implemented	In addition to formalizing and defining its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM 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), ISCM activities are repeatable, and metrics are used to measure and manage the implementation of the ISCM 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 ISCM 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.

Our evaluation showed SBA's information security continuous monitoring (ISCM) strategy has not been finalized. The Office of Management and Budget (OMB) Memorandum 14-03, *Enhancing the Security of Federal Information and Information Systems*, requires agencies to have an approved ISCM strategy by February 28, 2014. Based on the absence of a formalized ISCM strategy, we evaluated the overall maturity level for this area as Level 1-ad hoc. SBA needs to approve the ISCM strategy as a key step in establishing a robust ISCM program. Without an approved ISCM strategy, there is an increased risk that SBA is not aware of or will not be able to identify security threats. Moreover, an outstanding recommendation in this area remains open regarding finalizing, implementing, and communicating the ISCM strategy. As of the date of this report, SBA does not anticipate implementing this recommendation until February 2017.[3]

2. Configuration Management

Configuration management guidance requires that agencies document policies and ensure information system software is patched and configured securely. In FY 2015, SBA made substantial progress in its configuration management. Cyberscope results reflected that tested systems had established configuration baselines, and SBA implemented a process for handling identified weaknesses. However, our tests also indicated that vulnerabilities were not timely remediated.

Vulnerabilities Were Not Timely Remediated

Limited vulnerability and configuration scans of SBA's system found that configuration management weaknesses continued to exist in FY 2015. OIG's independent public accountant found that multiple configuration management vulnerabilities were carried over from FY 2014 in both existing and new systems. SBA policy requires these vulnerabilities to

[3] See Appendix II for the outstanding recommendation pertaining to Continuous Monitoring Management.

be patched within 90 days at the very latest.[4] These default configurations and configuration weaknesses increase the risk that SBA systems could be compromised.

SBA Needs to Enhance Controls over Baselines

While SBA had established baselines for systems sampled, continued improvement is needed. Three of seven systems reviewed did not have mechanisms in place to track baseline changes. Without an auditable trail of configuration changes, there is an increased risk that SBA will not be able to maintain compliance with the prescribed baseline or detect unauthorized changes.

SBA has improved in this area, but progress is still needed to maintain configuration baselines and remediate vulnerabilities timely. SBA should establish and approve a process to ensure settings are tracked, reviewed, and any issues are addressed timely.

SBA has five open OIG audit recommendations in this area (See Appendix II – Configuration Management). These recommendations call for SBA to:

- enhance vulnerability management processes,
- implement approved configuration baselines, and
- follow procedures for change control of SBA software.

The current year Cyberscope results indicate that these conditions still exist.

3. 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.[5] However, SBA has a number of public-facing internet applications that do not require multifactor authentication to gain access to those applications. These applications are owned by the various offices within SBA. As a result, SBA is at a higher risk that inappropriate access to one of these major applications could occur and go undetected. In FY 2015, SBA continued to need improvement in this area. This review identified weaknesses in authentication requirements, separation of duties, and separation controls. The weaknesses identified below could potentially affect the security and authenticity of connections to SBA's general support systems and major applications. We believe SBA needs to implement a two-factor authentication for public-facing internet applications weaknesses in authentication requirements, separation of duties, and separation controls.

SBA currently has 13 prior-year OIG audit recommendations remaining open (See Appendix II - Identity and Access Management). These recommendations address:

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

[4] SBA Vulnerability Assessment Team, Version 1.0 (May 2014).
[5] OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).

Logical Access Using PIV Credentials

SBA has not implemented personal identity verification (PIV) authentication requirements for network access, as required by OMB.[6] Agency officials reported that as of October 15, 2015, 86 percent of unprivileged users and 100 percent of privileged users authenticated to the network using their PIV credentials. OMB required agencies to implement physical and logical access control to authenticate using PIV credentials by FY 2012; however, due to management oversight and a lack of resources, SBA has not completed its implementation.[7] As a result, SBA faces an increased risk that the confidentiality, integrity, and availability of data in its systems may be compromised.

Least Privilege

SBA's policy states SBA computer systems end-user access is based on a need-to-know or need-to-use basis.[8] This policy further requires accounts only be given access to systems that allow users to perform their day-to-day duties. Our review identified accounts with permissions exceeding those required and, as a result, exposes SBA's network to increased risks. Adhering to existing SBA policy would ensure that accounts have necessary permissions.

Separation Controls

SBA continued to experience weaknesses over its separation process in FY 2015. In a prior report, OIG identified eight employee accounts that were not always disabled within 24 hours after employee separation. SBA Standard Operating Procedure (SOP) 90-47.3, *Information System Security Program*, requires that system access be deactivated when personnel separate from the Agency.[9] SBA supervisors are responsible for ensuring that employee separation checklists are completed, including steps for deactivating the employee system accounts. However, supervisors are not ensuring checklists are completed. As a result, SBA systems are at an increased risk of unauthorized access.

4. Incident Response and Reporting

FISMA requires Federal agencies to establish incident response, handling, and reporting capabilities.[10] As part of our annual FISMA review, we reviewed SBA's incident response program for policies, procedures, analysis capabilities, documentation, and reporting. While we concluded that SBA has established an incident response and reporting program that is consistent with FISMA requirements, we identified weaknesses in the tracking incidents and reporting to the United States Computer Emergency Readiness Team (US-CERT).

[6] OMB Memorandum 11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors* (February 3, 2011).
[7] OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).
[8] SBA SOP 90.47.3, *Information System Security Program,* Chapter 1, "Access Control" (August 28, 2012).
[9] SBA SOP 90.47.3, *Information System Security Program*, Chapter 13, "Personnel Security" (August 28, 2012).
[10] 44 U.S.C. 3553 (b) (2), *Authority and functions of the Director and the Secretary* (December 18, 2014).

Incident Documentation and Reporting

In FY 2015, we found that SBA's current process did not track time of incidents and did not ensure incidents were reported to US-CERT within allotted timeframes. One incident involving personally identifiable information (PII) was not reported to US-CERT until 69 hours after it was detected. Additionally, incidents were not centrally tracked between October 1, 2014, and April 22, 2015, due to personnel turnover and transitioning from the previous tracking system. US-CERT requires incidents involving PII to be reported within 1 hour of detection; however, due to management oversight, at least one incident was not reported timely to US-CERT. Consequently, SBA's incident response was delayed, which could, in turn, delay notification to the affected parties. We made a new recommendation in this area to ensure that SBA properly tracks and reports incidents.

Recommendation

We recommend the Office of Chief Information Officer:

1. Enhance the current process for tracking incidents to ensure that SBA comprehensively validates incidents and implements controls so that incidents are reported compliant with US-CERT requirements.

5. Risk Management

Risk management is vital to an organization in developing, implementing, and maintaining safeguards against vulnerabilities. The National Institute of Standards and Technology (NIST) SP 800-53*, Security and Privacy Controls for Federal Information Systems and Organization*, states that effective risk management ensures information systems have the necessary mechanisms to strengthen organizational information system.[11] In FY 2015, SBA made little to no progress in this area. Cyberscope results indicated SBA did not approve or perform security impact analysis, implement the current NIST controls, or maintain a complete inventory of systems. Additionally, SBA has three outstanding recommendations open in risk management (See Appendix II - Risk Management).

SBA Needs to Ensure Systems Have Been Authorized to Operate

Regulations require authorizing officials to approve the information system and perform a security impact analysis prior to the system's initial operation, as well as continuously monitor critical information contained in the authorization packages on an ongoing basis. SBA is also required to document any changes to the system or its environment and update the system security plan.[12] We determined that SBA did not maintain security assessment package documentation and did not properly re-approve the system prior to its migration to a third-party service provider, as required by SBA regulations. These risks occurred because the system owner and program office did not update mandatory security authorization requirements. System risk may increase because the Agency is unable to

[11]National Institute of Standards and Technology (NIST) SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organization*, Chapter 2.1, "Multitiered Risk Management" (April 2013).

[12] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organization,* Control CA-6, "Security Authorization" (April 2013).

identify potential threats or problems. SBA must update its security authorization packages to ensure the Agency is following current security policies and Federal guidance.

Current NIST Security Controls Have Not Been Implemented

Our review found that SBA has not adopted the current controls listed in NIST 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, issued in April 2013. Federal guidance requires agencies implement controls within 1 year of issuance.

SBA Needs to Maintain an Accurate Inventory of Systems

SBA is required to maintain an inventory and descriptions of the Agency's major information systems.[13] We found that SBA did not maintain a complete and accurate record of their cloud system. Without an accurate Agency-wide system inventory, there is an increased risk that systems are not subject to the proper oversight and that the necessary security controls are not implemented. SBA should update their inventory of cloud supported systems to remain in compliance with policies and procedures.

6. Security Training

FISMA requires agencies to establish both general security awareness training and specialized, role-based training.[14] We found that SBA had an established security training program consistent with FISMA reporting requirements. Therefore, we have no exceptions in this area.

7. Plan of Action and Milestones

A plan of action and milestones (POA&M) is a management process that plans, tracks, and prioritizes the information system weaknesses to ensure they are resolved.[15] Weaknesses are identified from multiple sources such as OIG audits, security control assessments, vulnerability scans, and risk assessments.[16] Our review found that SBA's POA&M process was overall consistent with the FISMA reporting requirements, but weakness previously identified continue to occur and a prior year recommendation remains open (See Appendix II – Plan of Action and Milestones). SBA continues to miss and not update POA&M remediation dates. Additionally, SBA did not always include weaknesses identified during security control assessments, or complete remediation cost information.

POA&M Remediation Dates are Missed and Not Updated

Our review found that while OCIO tracks open POA&Ms, as of June 13, 2015, 223 open POA&M milestones had not been remediated by their planned completion date. According to SBA policy, remediation dates are based on the outcome of prioritization decisions and available resources and should be updated separately, if needed.[17] Timely POA&Ms

[13] OMB Circular A-130, *Management of Federal Information Resources* (November 28, 2000).

[14] 44 U.SC. 3554. (b) (2) (4), *Federal agency responsibilities* (December 18, 2014) .

[15] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organization,* Control CA-5, "Plan of Action and Milestones" (April 2013).

[16] SBA SOP 90.47.3, *Information System Security Program*, Chapter 4, "Assessment and Authorization" (August 28, 2012).

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

remediation will eliminate vulnerabilities and correct deficiencies in the system while ensuring SBA acts in accordance with requirements.

Weaknesses Identified During Security Control Assessments Are Not Always Included

Six out of eight systems sampled had weaknesses identified in their security control assessment that were not documented in SBA's POA&M process. SBA policy and OMB guidance states that all information system weaknesses identified be documented and tracked as a POA&M.[18] The POA&M process is SBA's process for tracking and ensuring weaknesses are remediated. Weaknesses not captured by the POA&M process have an increased risk of not being timely and effectively remediated.

Remediation Costs

We also found that SBA did not consistently identify the cost of remediating each of the weaknesses. Out of a sample of 15 POA&Ms, 3 did not list a remediation cost. SBA must ensure that capital planning identifies resources needed to implement the cost of remediating information security program weaknesses.[19] Cost information should be captured to ensure the cost of security can be planned and linked to the Agency budget.

8. Remote Access Management

Federal agencies are required by FISMA to ensure that remote access programs are consistent with standards set by NIST.[20] Our FY 2015 FISMA review found that SBA's remote access program was generally consistent with FISMA requirements, but we identified weaknesses in the configuration of SBA's remote access software and policies and procedures. This evaluation area has six open recommendations addressing audit logs, encryption, and access timeouts (See Appendix II-Remote Access Management).

SBA's Remote Access Software Does Not Meet Requirements

During the FY 2015 FISMA review, we found that SBA's remote access software continued to have weaknesses. Specifically, SBA has not enforced its policy requiring the use of SBA configured machines and timing out remote access sessions after 30 minutes of inactivity. Additionally, SBA did not use cryptographic modules for all software, as specified in the Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*. SBA policy requires that these controls be in place; however, weaknesses persist from year to year.[21] These conditions were previously identified and have outstanding recommendations (See Appendix II – Remote Access Management). Requiring the Agency to strengthen and enforce controls will resolve the issue.

[18] SBA SOP 90.47.3, Information System Security Program, Appendix J-"SBA's POA&M Process;*"* OMB Memorandum 02 01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones* (October 17, 2001).

[19] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organization,* Control PM-3, "Information Systems Resources" (April 2013).

[20] 44 U.SC. 3553. (a) (2) (4), *Authority and functions of the Director and the Secretary* (December 18, 2014); NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organization*, Control AC-17, "Remote Access" (April 2013).

[21] SBA SOP 90.47.3, *Information System Security Program*, Chapter 1, "Access Control" (AC-17)-Common (August 28, 2012).

Remote Access Rules of Behavior

Our review also identified that users were not required to sign rules of behavior indicating the users' responsibilities with respect to managing and safeguarding tokens used for remotely logging into SBA systems. SBA's information system security program policy requires that users sign a rules of behavior when they receive their token.[22] Due to management oversight, there is an increased risk that personnel are not aware of their responsibilities. We made two new recommendations, which will ensure users have read, understand, and agree to manage and safeguard tokens.

Recommendations

We recommend the Office of Chief Information Officer:

2. Enforce procedures and controls designed to ensure that non-SBA equipment used for remote access is properly approved.

3. Require users to sign the remote access rules of behavior document.

9. Contingency Planning

Contingency planning involves the organization's efforts for achieving continuity of operations.[23] Contingency planning ensures that general support systems, which host major applications critical to SBA's continued, successful operation, will still operate even in the event of a disaster. As part of a complete strategy, organizations should plan, test, and train personnel on a system's contingency plan. During our FY 2015 FISMA review, we found weaknesses in several areas that could hinder SBA's ability to re-establish services in the event of a disruption. Some systems did not have alternate processing sites, test their contingency plan annually, or retain system backups according to SBA guidance.[24] Two prior recommendations addressing backup retention remain open (See Appendix II – Contingency Planning).

Systems Do Not Have Alternate Processing Sites

Two out of seven sampled systems did not have alternate processing sites. SBA policy requires that an alternate processing site be identified for critical functions of SBA information systems.[25] OCIO officials were aware of the issue and explained that they had been unable to secure funding for an alternate processing site for the system. Alternate processing sites allow organizations to maintain essential functions in case of a service disruption at the primary site. By not maintaining alternate processing sites for the two systems, SBA would be unable to maintain operations should a failure occur.

[22] SBA SOOP 90.47.3, *Information System Security Program*, Chapter 12, "Planning" (August 28, 2012).

[23] NIST SP 800-53*, Security and Privacy Controls for Federal Information Systems and Organization*, Control CP-2 "Contingency Plan" (April 2013).

[24] SOP 90.47.3, *Information System Security Program,* Chapter 6, No. 1 "Contingency Planning Policies and Procedures" (August 28, 2012).

[25] SBA SOP 90.47.3, *Information System Security Program*, Chapter 6, "Contingency Planning" (August 28, 2012).

Contingency Plan Testing

One out of seven systems sampled did not test its contingency plan or conduct contingency plan training in the past 12 months. NIST guidance and SBA policy require that contingency and continuity of support plans are developed and tested annually.[26] Due to management oversight, one sampled system was not tested annually and, as a result, increased the risk that in the event of an emergency, SBA may not properly operate and provide critical functions.

System Backup Retention

Six out of seven systems sampled did not perform or appropriately store system backups. Specifically, four of seven systems did not retain systems backups for the duration required by SBA policy and evidence of backups for two of seven systems could not be provided for days in a selected sample. Potential SBA data could be lost in the event of disaster recovery. We have issued two new recommendations to address agency contingency planning.

Recommendations

We recommend the Office of Chief Information Officer ensure that:

4. Information system contingency plans are tested and consistent with the NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organization* requirements for the FIPS 199 categorization of each major general support system and application.

5. An alternate processing site is established for all major general support systems and applications.

10. Contractor Systems

We reviewed SBA's oversight of a selection of information systems operated by SBA contractors. We identified a couple of weaknesses in SBA's oversight of contractor systems, but overall it was consistent with FISMA reporting criteria. As identified in prior sections risk management and plan of action and milestones, during our FY 2015 review, we found that POA&Ms were not created for weaknesses identified for one contractor system and SBA did not include a cloud systems operated by one of its contractors in its inventory.

[26] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organization*, Control CP-4 "Contingency Plan Testing" (April 2013); SBA SOP 90.47.3, *Information System Security Program*, Chapter 6, "Contingency Planning" (August 28, 2012).

Analysis of Agency Response

SBA management provided formal comments that are included in their entirety in Appendix III. SBA agreed with our five recommendations, and its planned actions resolve two 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. **Enhance the current process for tracking incidents to ensure that SBA comprehensively validates incidents and implements controls so that incidents are reported compliant with US-CERT requirements.**

   Resolved. The Office of Chief Information Officer (OCIO) stated that the SBA Security Operations Center implemented a process to track and validate incidents and report incidents to US-CERT when applicable. This recommendation can be closed when OCIO provides our office with the implemented incident reporting process that is compliant with US-CERT requirements.

2. **Enforce procedures and controls designed to ensure that non-SBA equipment used for remote access is properly approved.**

   Closed. SBA management agreed with this recommendation and provided a risk acceptance form that was signed by the system owner and authorizing official. This recommendation is considered closed.

3. **Require users to sign the remote access rules of behavior document.**

   Resolved. OCIO proposed implementation of this recommendation by March 31, 2017. This recommendation can be closed upon OCIO providing evidence that its office has incorporated the remote access rules of behavior into the standard user rules of behavior.

4. **Information system contingency plans are tested and consistent with the NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organization requirements for the FIPS 199 categorization of each major general support system and application**.

   Resolved. OCIO proposed implementation of this recommendation by September 30, 2016. This recommendation can be closed upon OCIO providing evidence of its information system contingency plan testing and that its testing was consistent with NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organization*, requirements for the FIPS 199 categorization of each major general support system and application.

5. **An alternate processing site is established for all major general support systems and applications.**

   Closed. SBA management agreed with this recommendation and provided a risk acceptance form that was signed by the system owner and authorizing official. This recommendation is considered closed.

Appendix I: Scope and Methodology

The Federal Information Security Management Act (FISMA) of 2002 provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. The Act requires (1) agencies to implement a set of minimum controls to protect Federal information and information systems and (2) the agencies' OIG to perform annual, independent evaluations of the information security program and practices of that agency to determine its effectiveness. Finally, the Act directs NIST to develop standards and guidelines for implementing its requirements in coordination with OMB.

On October 3, 2014, OMB issued Memorandum 15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*, providing instructions for agencies to meet their FY 2014-2015 reporting requirements under FISMA. This memorandum requires IGs to answer a set of information security questions in Cyberscope that evaluates agency implementation of security capabilities and measures their effectiveness.

To determine SBA's compliance in these areas, OIG contracted with an independent public accountant, KPMG, to perform review procedures relating to FISMA. KPMG interviewed SBA personnel, inspected documentation, and tested the effectiveness of SBA's IT security controls. OIG monitored KPMG's work and reported SBA's compliance with FISMA with the Agency FISMA Cyberscope submission in November 2015.

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 that we 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 2014 Cyberscope results to FY 2015 Cyberscope results. We determined if SBA either 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 or no progress as less than 5 percent improvement. Areas in which no exceptions were made to the Cyberscope questions for multiple years were viewed as substantial progress.

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 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).

Report 13-15, *Briefing Report for the FY 2012 Federal Information Security Management Act Review* (March 29, 2013).

Report 13-04, *Independent Auditors' Report on SBA's FY 2012 Financial Statements* (November 14, 2012).

Report 12-15, *Weaknesses Identified during the FY 2011 Federal Information Security Management Act Review (*July 16, 2012).

Report 12-02, *Independent Auditors' Report on SBA's FY 2011 Financial Statements* (November 14, 2011).

Report 11-06, *Weaknesses Identified During the FY 2010 Federal Information Security Management Act Review* (January 28, 2011).

Appendix II: Open IT Security Recommendations Related to FISMA

There are 31 open audit recommendations that directly affect SBA's Cyberscope evaluation as it relates to FISMA compliance as of September 30, 2015. OMB Circular A-50 states that agencies' audit follow-up system must require prompt resolution and corrective actions on audit recommendations.

Continuous Monitoring Management

Continuous monitoring is essential to an organization to determine ongoing effectiveness of information systems.[27] Our past audits identified weaknesses in this area. To address these weaknesses, we recommended SBA:

1. Implement the ISCM program requirement which includes: 1.Finalizing and implementing the ISCM strategy; 2. Identifying resource and skill requirements/gaps; 3. Identifying individuals to manage SBA ISCM program. OIG Report 15-07 Recommendation 1, Closure is due 2/28/2017.[28]

Configuration Management

FISMA requires organizations develop minimally-acceptable system configuration requirements to ensure a baseline level of security for its IT operations and assets.[29] Our past audits and reviews identified weaknesses in how the development of baseline configurations along with other configuration-related controls. We recommended SBA:

2. Develop and document baseline configurations for each information system and maintain the baseline under configuration control. OIG Report 11-06, Recommendation 5, Closure was due 9/30/2011.[30]

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 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.

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

[28] In FY 2015 this condition was repeated. We did not initiate a duplicate recommendation.

[29] 44 U.SC. 3554. (b) (2) (D) (iii), *Federal agency responsibilities* (December 18, 2014).

[30] In FY 2015 this condition was repeated. We did not initiate a duplicate recommendation.

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.[31]

6. Implement controls and processes to ensure that system changes are adequately tested, testing documentation is maintained, and system Security Authorization Packages are updated to reflect major system changes.[32] OIG Report 16-02, Recommendation 8.[33]

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.[34] Our past audits found weaknesses in SBA's account management and meeting authentication strength requirements. To address these weaknesses, we recommended SBA:

7. 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.

8. 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.[35]

9. 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.

10. Implement personal identification verification (PIV) for logical access to all SBA systems. OIG Report 14-12, Recommendation 1, Closure was due 12/31/2014.

11. Ensure that sensitive passwords meet SBA standards for password strength and complexity. OIG Report 15-02, Recommendation 9, Closure was due 12/31/2015.

12. 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.

[31] In FY 2015, this condition was repeated. We did not initiate a duplicate recommendation.
[32] SBA has not established a closure date.
[33] SBA has not established a closure date.
[34] SBA SOP 90.47.3, *Information System Security Program*, Chapter 7(August 28, 2012).
[35] In FY 2015 this condition was repeated. We did not initiate a duplicate recommendation.

13. 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.[36]

14. 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.[37]

15. 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.[38]

16. 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.[39]

17. 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 us in g 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 9/30/2014.

18. Clarify email access policies as defined in SOP 90 49.1. OIG Report 15-12, Recommendation 4, Closure was due 10/1/2015.

19. Implement two-factor authentication for public-facing internet applications. OIG Report 15-07, Recommendation 2, Closure was due 6/30/2015.[40]

[36] SBA has not established a closure date.
[37] SBA has not established a closure date.
[38] SBA has not established a closure date.
[39] SBA has not established a closure date.
[40] In FY 2015 this condition was repeated. We did not initiate a duplicate recommendation.

Incident Response and Reporting

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.[41] Our past audits found weaknesses in SBA's incident response and reporting. However, all outstanding recommendations in this area are considered closed.

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.[42] Past audits found weaknesses in the agency's risk management. To address these weaknesses, we recommended SBA:

20. 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 Assessment and Management Tool (CSAM). OIG Report 14-12, Recommendation 2, Closure was due 12/31/2014.[43]

21. Ensuring that SBA general support systems and major applications have valid and up-to-date ATO's while those systems are in production. OIG Report 15-07, Recommendation 4, Closure was due 12/31/2015.[44]

22. Ensuring 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 is due 9/30/2016.

Security Training

System users should have proper IT security training relevant to their IT security role and to the system and are also required to be properly designated, monitored, and trained.[45] Our past audits

[41] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organization*, Control IR-1 (April 2013).
[42] SBA SOP 90.47.3, *Information System Security Program*, Appendix C (August 28, 2012).
[43] In FY 2015 this condition was repeated. We did not initiate a duplicate recommendation.
[44] In FY 2015 this condition was repeated. We did not initiate a duplicate recommendation.
[45] SBA SOP 90.47.3, *Information System Security Program*, "Roles and Responsibilities" (August 28, 2012).

found identified weaknesses in this area. However, all outstanding recommendations in this area are considered closed.

Plan of Action and Milestones (POA&M)

POA&Ms document the planned, implemented, and evaluated remedial actions that correct system deficiencies.[46] Past audits identified weaknesses in SBA's POA&M. To address these weaknesses, we recommended SBA:

23. 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) Ensure that systems security plans are timely and accurately completed for all relevant general support systems and major applications.
    (c) Ensure that security assessment reports are timely and accurately completed for all relevant general support systems and major applications.
    (d) Create 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 Assessment and Management Tool (CSAM). OIG Report 14-12, Recommendation 2, Closure was due 12/31/2014. This recommendation is also listed under the Risk Management section.[47]

Remote Access Management

SBA's network and information systems can be remotely accessed by a user communicating through an external network.[48] Our past audits have found weaknesses. To address these weaknesses, we recommended SBA:

24. Continuously monitor remote access audit logs for potential unauthorized activity. OIG Report 12-15, Recommendation 4, Closure was due 12/30/2012.

25. Upgrade SBA's remote access solution to fully incorporate required encryption standards. OIG Report 14-12, Recommendation 4, Closure was due 5/30/2015.

26. Upgrade SBA's remote access solution to time-out after 30 minutes of inactivity. OIG Report 14-12, Recommendation 5, Closure was due 12/31/2014.

27. 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.

[46] SBA SOP 90.47.3, *Information System Security Program*, Chapter 4 (August 28, 2012).
[47] In FY 2015 this condition was repeated. We did not initiate a duplicate recommendation.
[48] SBA SOP 90.47.3, *Information System Security Program*, Chapter 1 (August 28, 2012).

28. To 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.[49]

29. 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.

Contingency Planning

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organization*, states organizations should develop contingency plans. The plan must addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.[50] A past audit has identified weaknesses. To address this weakness, we recommended SBA:

30. 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.[51, 52]

31. Ensure that data stored on enterprise servers are backed up monthly and retained for one year for disaster recovery and restoration purposes. OIG Report 15-07, Recommendation 6, Closure is due at 9/30/16.

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. [53]Our past audits found weaknesses in this area. However, SBA does not have any outstanding recommendations in this area.

[49] SBA has not established a closure date.
[50] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organization*, Control CP-1 (April 2013).
[51] In FY 2015 this condition was repeated. We did not initiate a duplicate recommendation.
[52] SBA has not established a closure date.
[53] SBA SOP 90.47.3, *Information System Security Program*, Chapter 8 (August 28, 2012).

Appendix III: Agency Comments

SBA

SBA

OFFICE OF THE CHIEF INFORMATION OFFICER'S

RESPONSE TO EVALUATION REPORT

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, DC 20416

DATE: March 8, 2016

TO: Troy Meyer
Assistant Inspector General for Audit

FROM: Keith Bluestein /S/
Acting, Chief Information Officer
Office of the Chief Information Officer

VIA: Jerome Nash /S/
Chief, Risk Management and Continuous Monitoring
Office of the Chief Information Security Officer

SUBJECT: OCIO Response to OIG's Draft FY 2015 Federal Information Security Management Act Review, Project 15007

We appreciate the opportunity to provide comments on the draft report entitled, "Weaknesses Identified during the FY 2015 Federal Information Security Management Act Review", and wish to thank the Inspector General's staff for their consideration of our response. As a result of our review the OCIO concurs with all recommendations.

For further details on our planned corrective actions to all weaknesses please refer to the Appendix detailed in a separate attachment. There are two weaknesses pertaining to incident response in the report which were previously closed by the OIG. Also, a closure for documenting configuration baseline is currently under OIG review. Looking forward, the OCIO will complete final action section on any open recommendations where corrective action has been taken and timely return to the OIG for closure review.

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. We appreciate your audit recommendations because they will help improve our security posture.