EVALUATION REPORT

Weaknesses Identified During the FY 2014 Federal Information Security Management Act Review

March 13, 2015 REPORT NUMBER 15-07

EXECUTIVE SUMMARY

Weaknesses Identified During the FY 2014 Federal Information Security Management Act Review

Report 15-07
March 13, 2015

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. To determine SBA's compliance with FISMA, OIG contracted with an independent public accountant, KPMG, to perform review procedures relating to FISMA. OIG monitored KPMG's work and reported SBA's compliance with FISMA in the Agency FISMA filings in November 2014. We also assessed the Agency's progress in implementing open recommendations and compared our current year assessment with our fiscal year (FY) 2013 FISMA evaluation.

What OIG Found

SBA continues to progress in certain FISMA evaluation categories. For example, OIG found that SBA met the majority of established guidelines in continuous monitoring, incident response, security training, its plan of actions and milestones, remote access management, contractor systems, and security capital planning.

However, SBA still needs to implement 32 long-standing open recommendations and related, unresolved vulnerabilities in SBA's FISMA areas. The FISMA areas of highest priority include configuration management, identity and access management, and contingency planning.

First, SBA has not met configuration management criteria, even though past audits have recommended implementing effective software patch management and establishing baseline configurations.

Second, prior recommendations addressing identity and access management controls—including oversight of authorized personnel's access to SBA systems, and proper separation controls—also remain open. SBA also needs to implement personal identification verification for accessing SBA information resources.

Finally, in the area of contingency planning, open recommendations identified that SBA needs to have adequate disaster recovery capabilities for systems and data processed at SBA's headquarters (HQ) data center.

Until SBA takes steps to address these long-standing weaknesses in its IT systems and control structures, the Agency will be at risk of data loss or system penetration.

Summary of FISMA Progress by Category for FY 2014

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

OIG Recommendations

In addition to the 32 open FISMA recommendations in Appendix II, OIG made 6 new recommendations to address FISMA-related vulnerabilities.

Agency Comments

SBA reviewed the report, but did not provide a written response to the draft report.

Actions Taken

SBA fully agreed with all six recommendations, and projected they would be implemented by February 2017.

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

Final Report Transmittal
Report Number: 15-07

DATE: March 13, 2015

TO: Renee Macklin,
Chief Information Officer

SUBJECT: *Weaknesses Identified During the FY 2014 Federal Information Security Management Act Review*

This report presents the results of our evaluation of the FY 2014 Federal Information System Management Act (FISMA) review. FISMA requires Federal agencies to develop, implement, and report on the effectiveness of the agency's information security program.

We made 6 new recommendations to address FISMA-related vulnerabilities, in addition to the 32 open FISMA recommendations presented in Appendix II. Please provide us within 90 days your progress in implementing the recommendations.

We appreciate the courtesies and cooperation SBA extended to the staff during this review.

/S/
Troy M. Meyer
Assistant Inspector General for Auditing

Table of Contents

Introduction

The Federal Information Security Management Act (FISMA) requires Federal agencies to develop, implement, and report on the effectiveness of the agency's information security program. For fiscal year (FY) 2014, the Office of Inspector General (OIG) was required to report on the following 11 areas: (1) continuous monitoring; (2) configuration management; (3) identity and access management; (4) incident response and reporting; (5) risk management; (6) security training; (7) plan of actions and milestones; (8) remote access management; (9) contingency planning; (10) contractor systems; and (11) security capital planning.

On November 17, 2014, SBA submitted its FISMA Cyberscope report to the Department of Homeland Security (DHS). Cyberscope is an online data collection tool administered by DHS to collect FISMA cybersecurity performance data.

Results

In FY 2014, SBA made progress in meeting certain FISMA requirements. This included establishing an entity-wide incident management and response program, as well as implementing port security access controls across SBA's network. However, SBA still 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 32 prior-year open recommendations relating to FISMA reporting areas identified in Appendix II of this report.

1) Continuous Monitoring Management

According to the Cyberscope evaluation, SBA established its continuous monitoring management program consistently with FISMA reporting criteria. However, we identified one new issue in this area.

An Information Security Continuous Monitoring Strategy Had Not Been Finalized

Office of Management and Budget (OMB) guidance requires SBA to implement continuous monitoring of security controls as part of a phased approach through FY 2017.[1] SBA must also ensure adequate staff and training are in place to meet the objectives of the information security continuous monitoring (ISCM) program.[2] However, we found that SBA had not finalized an ISCM strategy, which OMB required to be implemented by February 28, 2014. According to SBA management, an ISCM strategy was in draft but had not been finalized. Additionally, SBA management had not identified resources and skill gaps nor identified individuals to manage the ISCM program as required, by April 30, 2014.

Recommendation 1

We recommend that the Chief Information Officer implement the ISCM program requirement which includes: (1) finalizing and implementing the ISCM strategy, (2) identifying resource and skill requirements and gaps (if any), and (3) identifying individuals to manage SBA's ISCM program.

2) Configuration Management

According to the Cyberscope evaluation, SBA's configuration management program does not meet key criteria specified in FISMA guidance. Current year vulnerability scan results and open recommendations from prior years indicate that SBA continues to have configuration management vulnerabilities that risk the secure operation of SBA's general support systems and major applications.

SBA has 12 open OIG audit recommendations from the previous years in this area. Of the 12 open recommendations, 5 recommended enforcing and enhancing SBA's vulnerability management processes, 3 recommended implementing approved security configuration baselines, 3 recommended maintaining documentation to support the change control of SBA software, and 1

[1] OMB Memorandum 14-03, "*Enhancing the Security of Federal Information and Information Systems.*"
[2] According to the attachment to Memorandum 14-03.

recommended establishing an inventory of all Agency hardware and software. The complete recommendations are listed in Appendix II.

3) Identity and Access Management

According to the Cyberscope evaluation, SBA does not have an identity and access management program that is consistent with FISMA reporting areas. SBA has nine prior-year OIG audit recommendations remaining open in this area. Of the nine open recommendations, two recommended establishing an effective off-boarding or separation process, two recommended ensuring that highly privileged users duties were segregated and reviewed, one recommended timely recertification of end-users, one recommended using personal ID verification cards for logical access to SBA's network and systems, one recommended ensuring that new users are assigned random passwords and are subsequently required to change their initial password on first login, one recommended that access is appropriately granted consistent with the conditions on access forms, and one recommended that access to the headquarters data center is more closely reviewed. These nine recommendations are listed in Appendix II. In addition to these recommendations, we identified one new weakness in this area. These weaknesses could potentially affect the security and authenticity of connections to SBA's general support systems and major applications.

Multifactor Authentication for Public Facing Internet Applications Had Not Been Implemented

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.[3] 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 such as the Office of Capital Access and Office of Investment and Innovation. As a result, SBA is at a higher risk that inappropriate access to one of these major applications could occur and go undetected.

Recommendation 2

We recommend that SBA's Chief Information Officer—in conjunction with appropriate program offices—implement two-factor authentication for public-facing internet applications.

4) Incident Response and Reporting

According to the Cyberscope evaluation, SBA has established an incident response and reporting program that is consistent with FISMA reporting areas. However, we found one area whereby SBA could improve its incident response and reporting program.

[3] OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, Attachment 1, Section C, "Control Remote Access" (May 22, 2007).

Security Incidents Were Not Timely Reported to the United States Computer Emergency Readiness Team (US-CERT)

Both SBA and OMB guidance require that SBA report all incidents involving personally identifiable information (PII) to the United States Computer Emergency Readiness Team (US-CERT) within one hour.[4] However, we found SBA did not timely report three of five sampled security incidents to US-CERT. At least one of these incidents involved the suspected disclosure of PII to the public. As a result, a security breach could occur and not be reported within established time-fames.

OCIO IT-Security identified that the three security incidents that were late being reported to US-CERT had been initially investigated by SBA program offices. These program offices had not followed SBA guidance in timely reporting security incidents to OCIO IT-Security for subsequent reporting to US-CERT.

Recommendation 3

We recommend that the Chief Information Officer reinforce to SBA program offices the need to timely report security incidents to OCIO IT-Security in accordance with established SBA procedures.

5) Risk Management Program

This fiscal year, SBA made progress in categorizing information systems and communicating security risks to senior agency officials. Specifically, the senior officials are briefed on IT security incidents, threats, and vulnerabilities identified through SBA's continuous monitoring efforts.

However, according to the Cyberscope, SBA still had not established a risk management program that is consistent with FISMA reporting criteria. Three of the seven systems in our FISMA sample did not have a current risk assessment. We identified this issue in our FY 2013 FISMA report and recommended SBA update risk assessments annually for general support systems and major applications. However, this recommendation remains open. (See the Risk Management recommendation listed in Appendix II.)

SBA's Major Systems Were in Production without a Valid Authority to Operate

SBA guidance requires that SBA authorize an information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.[5] However, according to the Cyberscope evaluation, SBA did not have valid authorizations to operate (ATO) for two of seven sampled systems in FY 2014: the Customer Relationship Management System and the Local Area Network/Wide Area Network (LAN/WAN). The ATO for SBA's customer relationship management system was originally authorized on December 17, 2010 and was valid for 3

[4] According to SBA SOP 90-50, *Breach Notification Response Plan,* Section 8.2, SBA must comply with OMB M-06-19, *Reporting Incident Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* and OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.*

[5] SBA SOP 90-47.3*, Information System Security Program,* Appendix K, "Security Assessment and Authorization Process (Risk Management Process)" (August 28, 2012).

years. The ATO for SBA's LAN/WAN was only valid starting on September 30, 2013 but only for a 7-month period due to concerns of senior SBA officials. Without a valid authority to operate, SBA systems could potentially be put into production with known vulnerabilities which if exploited could affect SBA data and resources.

Recommendation 4

We recommend that the Chief Information Officer ensure that SBA general support systems and major applications have valid and up-to-date ATO's while those systems are in production.

6) Security Training

According to the Cyberscope evaluation, SBA established a security training program that is consistent with FISMA reporting criteria. However, one OIG audit recommendation from last year remains open in this area (See Appendix II). That recommendation requires that personnel with specialized security positions take enhanced security training.

7) Plan of Actions and Milestones

According to the Cyberscope evaluation, SBA established a plan of actions and milestones (POA&M) program that is consistent with FISMA reporting criteria. However, we noted two areas of improvement that need to be implemented to be consistent with FISMA reporting areas in the Cyberscope evaluation. Additionally, SBA has one audit recommendation open from last year in this area (See Appendix II).

Plan of Actions and Milestones Were Not Entered Into SBA's Cyber Security Assessment Management Tool

Two of seven systems in our FISMA sample had POA&Ms that were not developed and entered into SBA's Cyber Security Assessment and Management (CSAM) tool. SBA uses CSAM to track and manage IT weaknesses. This issue was also reported in our prior-year FISMA report and the recommendation to require that POA&Ms are included for general support systems and major applications remains open (See Appendix II—Risk Management).

Weaknesses Identified in POA&Ms Were Not Timely Mitigated

SBA guidance requires that the estimated date of completion for each weakness must be based on realistic timelines that allow for resources to be obtained and associated steps to be completed.[6] However, SBA had 987 security weaknesses with established POA&M dates due to be completed by August 10, 2014. Of these 987 security weaknesses, 343 weaknesses (34.8 percent) had not been mitigated by their POA&M due dates. As a result, over 34 percent of SBA's security weaknesses were not being timely remediated. Given the prior-year FISMA finding that POA&M remediation costs were not adequately estimated for vulnerabilities in last year's FISMA report (OIG Report 14-12), SBA had 180 of 236 weaknesses with either $0 or $1 as the remediation cost to correct the weakness. We

[6] SBA SOP 90-47.3, *Information System Security Program*, Appendix J, "SBA's POA&M Process" (August 28, 2012).

conclude that SBA is not realistically estimating either the timeline or the cost to remediate the security weaknesses in the POA&M process.

Recommendation 5

We recommend that the Chief Information Officer, in conjunction with other SBA program offices, accurately update system and program POA&Ms to reflect the current status for each weakness, including scheduled completion dates of corrective actions.

8) Remote Access Management

According to the Cyberscope evaluation, SBA established a remote access management program that is consistent with FISMA reporting criteria. However, SBA has four open prior-year recommendations, which are listed in Appendix II. Of the four open recommendations, one recommendation was to implement a remote access audit log review process, one recommendation to fully incorporate required encryption standards, one recommendation was to upgrade SBA's remote access solution to time-out after 30 minutes, and one recommendation was to enhance the telework process.

9) Contingency Planning

According to the Cyberscope evaluation, SBA did not establish a contingency planning program that is consistent with FISMA reporting criteria. Contingency planning ensures that general support systems—which host major applications that are critical to the continued successful operation of SBA loan programs—will still operate, even in the event of a disaster. However, we noted that SBA does not have an alternate recovery site for three general support systems and three applications in our sample. Two prior-year recommendations to procure and implement an alternate recovery site, with due dates of September 30, 2013 and March 31, 2016, still remain open.[7]

Full Back-up Files Were Not Retained for Appropriate Timeframes for SBA Major Applications

SBA guidance requires that all data stored on enterprise servers will be backed up monthly and retained for one year.[8] However, we found that SBA did not retain full back-up files as required for three major applications in our FISMA sample. As a result, full restoration of major applications may be unavailable if the production systems become unavailable due to a disaster at SBA's data center.

Recommendation 6

We recommend that the Chief Information Officer ensure that data stored on enterprise servers are backed up monthly and retained for 1 year for disaster recovery and restoration purposes.

---

[7] See OIG Report 13-04, *Independent Auditors' Report on SBA's FY 2012 Financial* Statements (November 14, 2012), recommendation 18 and OIG Report 14-04, *Independent Auditors' FY 2013 Financial Statements* (December 16, 2013), recommendation 21.

[8] SBA SOP 90-47.3, *Information System Security Program,* Chapter 6, Section 8, *Contingency Planning* (August 28, 2012).

10) Contractor Systems

According to the Cyberscope evaluation, SBA established a contractor systems program that is consistent with FISMA reporting criteria. However, one major contractor-operated system in our FISMA sample did not have interfaces and interconnections with SBA's internal systems specified in its system security plan. Two prior-year recommendations to update system interfaces, with a corrective action due date of September 30, 2011, still remain open.[9]

11) Security Capital Planning

According to the Cyberscope evaluation, SBA established a security capital planning program that is consistent with FISMA reporting criteria.

Analysis of Agency Response

While SBA did not provide formal comments to this report, Agency management agreed with all six recommendations, and projected they would be implemented by February 2017.

Summary of Actions Necessary to Close the Report

1. **Implement the ISCM program requirement which includes: (1) finalizing and implementing the ISCM strategy, (2) identifying resource and skill requirements and gaps (if any), and (3) identifying individuals to manage SBA's ISCM program.**

   This recommendation can be closed when OCIO IT Security develops and implements an ISCM strategy for information systems within SBA. SBA projected that the full ISCM would be implemented by February 28, 2017.

2. **Implement two-factor authentication for public-facing internet applications.**

   This recommendation can be closed when OCIO completes an e-Authentication risk assessment to determine if public-facing internet applications requires two-factor authentication, and recommend that funding be allocated to ensure implementation. SBA projected that the initial e-Authentication risk assessments would be complete by June 30, 2015.

3. **Reinforce to SBA program offices the need to timely report security incidents to OCIO IT-Security in accordance with established SBA procedures.**

   This recommendation can be closed when OCIO develops and delivers an incident training program for SBA program offices on incident response procedures and requirements. Periodic review and testing will need to occur to reinforce to SBA program offices the need to timely report security incidents to OCIO IT Security. SBA projected that the incident training program would be completed by September 30, 2015.

[9] See Report 11-06, *Weaknesses Identified during the FY 2010 Federal Information Security Management Act Review*, issued January 11, 2011.

4. **Ensure that SBA general support systems and major applications have valid and up-to-date ATO's while those systems are in production.**

   This recommendation can be closed when OCIO reinforces with authorizing officials and system owners that all SBA systems are evaluated, tested, approved, and authorized to operate in accordance with authorization timelines and requirements. OCIO projected that their efforts to ensure that all systems have valid and up-to-date ATO's would be complete by December 30, 2015.

5. **Accurately update system and program POA&Ms to reflect the current status for each weakness, including scheduled completion dates of corrective actions.**

   This recommendation can be closed when OCIO reinforces with authorizing officials and system owners the importance of accurately updating and maintaining system and program POA&M's to reflect the current status for each weakness, including scheduled completion dates of corrective actions. OCIO projected that their efforts to accurately update and maintain system POA&Ms would be complete by May 30, 2015.

6. **Ensure that data stored on enterprise servers are backed up monthly and retained for one year for disaster recovery and restoration purposes.**

   This recommendation can be closed when OCIO contacts its off-site storage vendor to revise retention requirements in SBA's service level agreements. OCIO will also coordinate with other SBA program offices to determine the most efficient back-up solutions and recovery methods to meet or exceed NIST 800-34, Revision 1 *Contingency Planning Guide for Federal Information System* requirements. SBA projected that updating service level agreements will be completed by September 30, 2016.

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 the National Institute of Standards and Technology (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 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 2014.

Prior Coverage

Small Business Administration—Office of Inspector General Reports

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

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

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

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

Report 14-01, *Report on the Most Serious Management and Performance Challenges Facing the Small Business Administration in Fiscal Year 2014* (October 31, 2013).

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

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

Appendix II: Open Current and Prior Year IT Security Recommendations Relating to FISMA

There are 32 open prior-year audit recommendations which directly affect SBA's Cyberscope evaluation as it relates to FISMA compliance as of September 11, 2014. The 6 recommendations given in this report, along with the 32 prior-year open audit recommendations, represent SBA's current FISMA condition.

OMB Circular A-50 states that agencies' audit follow-up system must require prompt resolution and corrective actions on audit recommendations. Further, resolutions shall be made within 6 months, and corrective actions should be implemented as soon as possible.

Configuration Management – The organization develops minimally-acceptable system configuration requirements to ensure a baseline level of security for its IT operations and assets.

- Develop and maintain a centralized inventory of all agency hardware and software. OIG Report 11-06, Recommendation 4, Closure was due 9/30/2011.

- 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.

- CFO and the AA, Office of Disaster Assistance, implement scans of financial systems in its production environment using privileged access authorization. OIG Report 14-04, Recommendation 19, Closure was due 05/30/2014.

- Enhance security vulnerability management processes. Specifically, the 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.

- 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.

- Enhance security vulnerability management process. Specifically, (a) ensure that servers, operating systems, and databases are properly configured and updated on a routine basis; (b) monitor SBA vulnerability reports for required patches; (c) update systems based upon risk determination and threats. OIG Report 13-04, Recommendation 1, Closure was due 3/31/2014.

- The CIO enforces an organization-wide configuration management process, to include policies and procedures for maintaining documentation that supports testing and approvals of software changes. OIG Report 13-04, Recommendation 15, Closure was due 9/30/2014.

- The CIO coordinates with the Chief Financial Officer (CFO) to implement configuration management policies and procedures for document retention to include supporting evidence to validate the authorization of operating system changes. OIG Report 13-04, Recommendation 16, Closure was due 3/01/2014.

- Enforce a network access security baseline(s) across the network consistent with SBA security policy, OMB directives, and United States Government Configuration Baseline requirements. OIG Report 14-04, Recommendation 7, Closure was due 9/30/2014.

- Address the vulnerabilities noted during the FY 2013 audit consistent with SBA policy and SBA Vulnerability Assessment Team, Internal Operating Procedures, Version 1.4 and implement procedures to ensure the consistent identification, tracking, and resolution of security vulnerabilities across the SBA's workstations, servers, databases, network devices, and other security relevant appliances. OIG Report 14-04, Recommendation 12, Closure was due 06/30/2014.

- The Associate Administrator for Capital Access in coordination with the CIO, design and implement preventive and detective controls to ensure an auditable trail of software changes is maintained to prevent and detect unauthorized changes to production programs. OIG Report 14-04, Recommendation 15, Closure was due 06/30/2014.

- The CIO coordinates with SBA program offices to address the existing configuration management vulnerabilities noted during our assessment to be in compliance with SBA policy and SBA Vulnerability Assessment Team Internal Operating Procedures, Version 1.4. In addition, implement procedures to ensure the consistent implementation and monitoring of SBA approved security configuration baselines across SBA workstations, servers, databases, network devices, and other security relevant appliances. OIG Report 14-04, Recommendation 18, Closure is due 12/31/2014.

Identity and Access Management – The organization identifies and authenticates system users and limits system users to the information, functions, and information systems those users are authorized to operate.

- 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.

- The CIO coordinates with SBA program offices to ensure that all new system users are assigned random passwords and are subsequently required to change their password upon first log-in. Report 13-04, Recommendation 6, Closure was due 05/31/2013.

- 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 09/30/2013.

- Ensure that database administrators and system administrator access is restricted through role-based segregation of duties and managed through an effective audit log review process. OIG Report 13-04, Recommendation 12, Closure was due 3/01/2014.

- Improve the SBA's administration of logical system access by taking the following actions: (1) Implement an effective off-boarding process and verify periodically that controls to remove logical access for separated employees from SBA systems are implemented and operating as designed; (2) establish a process for the identification and removal of separated contractors in order to help ensure that access is timely removed upon contractor separation; (3) remove access to the general support systems and major applications (including development and test environments) timely when terminated employees and contractors are identified. OIG Report 14-04, Recommendation 4, Closure was due 09/30/2014.

- The CIO coordinates with SBA program offices to 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 14-04, Recommendation 6, Closure is due 12/31/2014.

- The CIO coordinates with the SBA program offices to review the list of individuals with headquarters data center access permissions periodically, to ensure that only authorized personnel retain access to the HQ data center. OIG Report 14-04, Recommendation 10, Closure is due 12/31/2014.

- 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 is due 12/31/2014.

- The CIO implements personal identification verification for logical access to all SBA systems. OIG Report 14-12, Recommendation 1, Closure is due 12/31/2014.

Risk Management – The organization establishes a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

- We recommend that the CIO in conjunction with other program offices 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.) Require 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 is due 12/31/2014.

Security Training – The organization has established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

- The CIO require that personnel with specialized security positions within the Agency take the enhanced security training to ensure that those personnel are adequately trained to perform their duties. OIG Report 14-12, Recommendation 6, Closure is due 12/31/2014.

Plan of Actions and Milestones (POA&M) – The organization has established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, and tracks and monitors known information security weaknesses.

- The CIO in conjunction with other program offices identifies estimated costs to correct each POA&M vulnerability entered into CSAM so that the SBA has an understanding of the price of mediation of its security vulnerabilities. OIG Report 14-12, Recommendation 3, Closure is due 12/31/2014.

Remote Access Management – The organization documents allowed methods of remote access, establishes usage restrictions, and monitors for unauthorized remote access.

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

- Improve the SBA's remote access program by taking the following actions: (1) Incorporate security requirements into the Teleworking Standard Operating Procedures (SOP) consistent with NIST 800-46 Rev. 1; (2) ensure employees acknowledge compliance with security requirements prior to establishing a remote connection to the SBA network when teleworking or otherwise connecting remotely to a SBA system; and (3) monitor compliance with the revised SOP 90.47.3 and the updated teleworking SOP. OIG Report 14-04, Recommendation 14, Closure was due 07/01/2014.

- The CIO upgrades the SBA's remote access solution to fully incorporate required encryption standards. OIG Report 14-12, Recommendation 4, Closure is due 05/30/15.

- The CIO upgrades the SBA's remote access solution to time out after 30 minutes of inactivity. OIG Report 14-12, Recommendation 5, Closure is due 12/31/14.

Contingency Planning – The organization implements plans for emergency response, backup operations, and post-disaster recovery for organizational information systems.

- The CIO conducts a business impact analysis, develops and implements the contingency plans, and establishes an alternate processing site. OIG Report 13-04, Recommendation 18, Closure was due 9/30/2013.

- The CIO designs and implements procedures, resources, and controls to ensure the timely recovery of resources and systems hosted by SBA headquarters. OIG Report 14-04, Recommendation 21, Closure is due 03/31/2016.

Contractor Systems – The organization ensures that its contractors abide by FISMA requirements.

- Update the list of major systems to include all the interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency, and obtain written interconnection security agreements for every SBA system that has an interconnection to another system. OIG Report 11-06, Recommendation 1, Closure was due 9/30/2011.

Establish a program at the SBA to manage, control, and monitor system interconnections throughout their lifecycle. The program should encompass planning, establishing, maintaining and terminating system interconnections, including enforcement of security requirements. OIG Report 11-06, Recommendation 2, Closure was due 9/30/2011.