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

Final Report Transmittal
Report No. 16-17

DATE: August 11, 2016

TO: Matthew Varilek
Chief Operating Officer
Office of the Chief Operating Officer

Keith A. Bluestein
Acting Chief Information Officer
Office of the Chief Information Officer

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

SUBJECT: *Fiscal Year 2016 Report of the U.S. Small Business Administration (SBA) Pursuant to the Cybersecurity Act of 2015, Section 406, Federal Computer Security*

The Cybersecurity Information Sharing Act of 2015 (the Cybersecurity Act) requires Offices of Inspectors General (OIG) to submit a report on select security controls identified in Section 406, Federal Computer Security, for systems that provide access to personally identifiable information (PII). Per the Cybersecurity Act requirements, this assessment includes the following areas:

- logical access policies and procedures,
- logical access and multi-factor authentication for privileged users,
- information security management practices, and
- information security management practices over contractors.

We contracted with the independent certified public accounting firm, KPMG, to evaluate whether the Small Business Administration (SBA) designed and implemented its cybersecurity logical access controls and information security management controls in accordance with the Cybersecurity Act. We selected a subset of PII development and production systems for KPMG's review and evaluation. KPMG's review found that the Agency did not meet Federal standards relating to Section 406 of the Cybersecurity Act. Specific areas for improvement are outlined in KPMG's attached report. We provided a draft of this report to the acting Chief Information Officer, (CIO) who concurred with its findings and conclusions. The acting CIO also concurred with related recommendations, which will be issued in conjunction with our annual Federal Information Security Management Act (FISMA) assessment.

This evaluation was performed in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) quality standards for inspection and evaluations. We monitored KPMG's work to ensure conformance with CIGIE quality standards, including identifying PII systems, validating auditor independence and qualifications, attending key meetings, and reviewing related documentation and completed work products. Our review did not note any instances where KPMG did not comply, in all material respects, with the CIGIE quality standards for inspection and evaluations.

Please contact us if you would like to discuss this report or any related issues.

cc: Maria Contreras-Sweet, Administrator
Nicolas Maduros, Chief of Staff
Melvin F. Williams, Jr., General Counsel
Martin Conrey, Attorney Advisor, Legislation and Appropriations
Tami Perriello, Associate Administrator for Performance Management
and Chief Financial Officer
LaNae Twite, Director, Office of Internal Controls

Attachment

Fiscal Year 2016 Report of the U.S. Small Business Administration (SBA) Pursuant to The Cybersecurity Act of 2015, Section 406, Federal Computer Security, Pub. L. 114-113, 129 Stat. 694

Prepared for: SBA Office of Inspector General (OIG)

As of August 10, 2016

KPMG LLP
1676 International Drive
Mclean, VA 22102

TABLE OF CONTENTS

KPMG LLP
1676 International Drive
McLean, VA 22102

Office of Inspector General (OIG)
U.S. Small Business Administration (SBA)

This report presents the results of our work conducted to address The Cybersecurity Act of 2015, Section 406, Federal Computer Security, Pub. L. 114-113, 129 Stat. 694 (SEC406) objectives. This report and the work therein was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation. Our work was performed during the period of April 11, 2016 to July 29, 2016 and was scoped for the Fiscal Year (FY) 2016 systems development environment that provide access to Personally Identifiable Information (PII). The SBA Office of Inspector General (OIG) selected the systems to be in-scope for the evaluation. The scope included a subset of ten systems within SBA's systems environment: nine production systems (including development environment for five of the production systems), and one development system. Of the ten systems, three were contractor systems.

On December 18, 2015, the President signed SEC406, which focuses on the current cybersecurity logical access controls and information security management monitoring controls. Congress is requiring Offices of the Inspectors General (OIGs) to submit a report on select security controls identified in SEC406 for national security systems and systems that provide access to PII.

Our approach to accomplishing the SEC406 reporting was to collect information regarding the design and implementation of the SBA IT cybersecurity practices. The design of SBA's security controls refers to the cybersecurity-related policies and guidelines established by SBA. KPMG inquired with management, inspected SBA's IT policies and practices, and observed the implementation of the security controls.

KPMG LLP

EXECUTIVE SUMMARY

KPMG LLP (KPMG) was contracted by the SBA OIG to collect information regarding the SBA cybersecurity program. The objectives were to report on the design and implementation of SBA's cybersecurity logical access controls and information security management controls in accordance with SEC406. The work was performed at SBA facilities located in Herndon, VA and Washington, DC during the period of April 11, 2016 to July 29, 2016. The design of SBA's security controls refers to the cybersecurity-related policies and guidelines established by SBA. KPMG's approach to accomplishing SEC406 reporting was to inquire with and collect information from SBA management regarding the design and implementation of the SBA IT cybersecurity practices. Exceptions to criteria or standards were discussed with SBA officials and recommendations for improvement are being issued through the OIG. The results of our review are summarized below:

SEC406 Requirement	Did the agency meet federal standards[1]?	Areas for Improvement
Logical Access Policies and Procedures (SEC406-b-2.A and SEC406-b-2.C)	No	• Update existing security policies and security plans for all SBA systems to meet the latest revision of NIST SP 800-53.
Logical Access and Multi-Factor Authentication for Privileged Users (SEC406-b-2.B and SEC406-b-2.C)	No	• Enhance PIV-deployment strategies for logical access to enforce mandatory multi-factor authentication for all privileged users. Implement mitigating controls for web-based applications where SBA is unable to enforce multi-factor authentication for external users.
Information Security Management Practices (SEC406-b.2.D.i-iv)	No	• Improve protocols to allow for a periodic and complete inventory of software, hardware, and licenses. • Improve controls over monitoring and detection of exfiltration and other threats. • Improve data loss prevention and digital rights management capabilities.
Information Security Management Practices over Contractors (SEC406-b-2.E)	No	• Enhance the agency's oversight of contractor systems by periodically performing assessments (or receiving assurance from the contractor) to ensure that security controls implemented for contractor systems comply with agency security policies and federal requirements.

[1] Federal standards include FISMA, OMB, and NIST requirements.

BACKGROUND

On December 18, 2015, the President signed into law SEC406, which focuses on the current cyber security logical access controls and information security management monitoring controls. Congress is requiring all departments to submit a report on selected security controls identified in SEC406 for national security systems and systems that access personally identifiable information.

OBJECTIVES, SCOPE AND METHODOLOGY

The objectives were to report on the design and implementation of SBA's cybersecurity logical access controls and information security management controls in accordance with SEC406 for a subset of ten systems within SBA's systems environment: nine production systems (including development environment for five of the production systems), and one development system. Of the ten systems, three were contractor systems. This report and the work therein was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation. The work was performed at SBA facilities located in Herndon, VA and Washington, DC during the period of April 11, 2016 to July 29, 2016.

As part of the Fiscal Year 2016 Federal Information Security Modernization Act (FISMA) evaluation, KPMG, with agreement from the OIG, tested a representative subset of SBA systems and security controls. KPMG performed testing to assess SBA's adherence to or progress in implementing minimum security standards and requirements commensurate with each system's security categorization and risk. KPMG used the results of these system reviews to focus the SEC406 report and provide an understanding of SBA's cybersecurity practices.

RESULTS

KPMG performed inquiry of SBA management, reviewed select policies and procedures, and observed the implementation of security controls regarding the following cybersecurity areas:

- Logical Access Policies and Procedures (SEC406-b-2.A and SEC406-b-2.C)
- Logical Access and Multi-Factor Authentication for Privileged Users (SEC406-b-2.B and SEC406-b-2.C)
- Information Security Management Practices (SEC406-b.2.D.i-iv)
- Information Security Management Practices over Contractors (SEC406-b-2.E)

SBA is required by FISMA to implement security controls over logical access and information security management practices. FISMA implementation guidance is issued by the Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST).

SBA has developed policies and procedures supporting SEC406. However, the agency described the following gaps and created corrective action plans within the information security program:

Logical Access Policies and Procedures (SEC406-b-2.A and SEC406-b-2.C)

A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.

SBA has implemented entity-wide logical access policies and procedures (SBA Standard Operating Procedure (SOP) 90 47 3, *Information System Security Program*). The SBA SOP 90 47 3 provides the baseline for System Owners to use when implementing system-specific access controls. However, the SOP 90 47 3 is documented in accordance with NIST Special Publication 800-53 Revision 3, and has not been updated to meet Revision 4 standards. In addition, although the SOP applies to all SBA systems, the agency places an emphasis on implementing access controls for the production environment as opposed to the development environment or new systems in development.

Logical Access and Multi-Factor Authentication for Privileged Users (SEC406-b-2.B and SEC406-b-2.C)

A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.

SBA has implemented SBA SOP 90 47 3, which provides a baseline for System Owners to use when implementing system-specific access controls. Below is the list of NIST SP 800-53 Access Controls (AC) covered in SOP 90 47 3:

- Access Control Policy and Procedures (AC-1)
- Account Management (AC-2)
- Access Enforcement (AC-3)
- Information Flow Enforcement (AC-4)
- Separation of Duties (AC-5)
- Least Privilege (AC-6)
- Unsuccessful Logon Attempts (AC-7)
- System Use Notification (AC-8)
- Session Lock (AC-11)
- Session Termination (AC-12)

- Permitted Actions without Identification or Authentication (AC-14)
- Remote Access (AC-17)
- Wireless Access (AC-18)
- Access Control for Mobile Devices (AC-19)
- Use of External Information Systems (AC-20)
- Publicly Accessible Content (AC-22)

The SBA network is the first level of access to the covered systems (production and development systems) for privileged users, and SOP 90 47 3 requires multi-factor authentication for network access to privileged accounts. SBA has begun rolling out machine-based Personal Identity Verification (PIV) credential enforcement, starting with workstations, and then moving on to servers.

Because SBA's PIV-enforcement strategy is machine-based as opposed to user-based, the agency would need to enforce PIV on 100% of their workstations in order to ensure that PIV for logical access is mandatory for 100% of privileged users. SBA has enforced PIV for 73% of their workstations, and none of their servers. Thus, SBA is not compliant with the SOP 90 47 3 requirements to mandate multi-factor authentication for privileged users and has not met OMB's requirement to enforce PIV for logical access for 100% of privileged users.

SOP 90 47 3 also requires SBA-configured equipment to be utilized for remote connections to the network. SBA uses two multi-factor authentication platforms for remote access (one is a virtual desktop infrastructure (VDI) and the other is a virtual private network (VPN) platform), which both require multi-factor authentication when authenticating remotely to the SBA network. However, the VPN remote connections do not require PIV authentication, and non-SBA-configured equipment can be utilized for remote connections using the VPN platform, which is not compliant with SBA's policies and procedures. Due to the limited number of licenses for the VDI platform, SBA still utilizes the VPN platform for remote access authentication.

According to SBA officials, end users only have access to the production application login platforms to process and input actual data. Five in-scope development systems use dummy data in the application layer development environment for testing and development purposes only. Thus, logical access controls would not be applicable.

Information Security Management Practices (SEC406-b-2.D.i-iv)

The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

SBA follows the agency-wide policies and procedures (SOP 90 47 3) to conduct inventories of the software present on SBA covered systems and the licenses associated with such software. SOP 90 47 3 requires information systems in use to maintain a component inventory of all hardware required to operate the information system. According to the SOP, the inventory must consist of hardware and software licenses, including: system/component owner, manufacturer, model or version number, serial number, software license information, and internal inventory labels (if internal labels are used on the hardware). The system component inventory must be reviewed at least annually.

The SBA OCIO recently implemented an enterprise architecture tool to manually inventory the hardware and deployed software version for the systems used throughout the agency. The SBA OCIO has begun collecting server names, deployed applications, hardware product information, server location, server type, and the deployed software product version (this inventory is incomplete and still in progress). Additionally, the SBA OCIO uses the automated IT asset management software tool to conduct inventories of the software present (including software license information) on the local area and wide area network; however, this does not encompass all SBA systems.

Program Offices outside of the SBA OCIO are manually maintaining their software inventories and tracking software licenses via Microsoft Excel.

What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including: data loss prevention capabilities; forensics and visibility capabilities; or digital rights management capabilities.

According to SBA officials, SBA has implemented automated capabilities to monitor and detect exfiltration and other threats. Several Data Loss Prevention (DLP) capabilities are utilized to safeguard data in motion (network traffic). However, SBA currently does not have DLP capabilities for data stored physically in digital form, such as databases, spreadsheets, archives, tapes, and mobile devices.

SBA also utilizes automated forensics and visibility capabilities such as intrusion detection systems.

According to SBA officials, SBA currently does not have capabilities for data rights management.

A description of how the covered agency is using the data loss prevention capabilities; forensics and visibility capabilities; or digital rights management capabilities.

The SBA OCIO uses DLP capabilities to:

a. Prevent users from sending sensitive data to external networks (e.g., quarantine outgoing emails that contain potential PII)
b. Scan incoming and outgoing traffic to detect malware and block malicious domains
c. Perform weekly scans of the SBA network to identify vulnerabilities

The SBA OCIO uses forensics and visibility capabilities to:

d. Analyze network traffic and research incidents
e. Sniff network traffic for specific malicious signatures
f. Detect data exfiltration via intrusion detection
g. Allow or block devices from connecting to the SBA network

If the covered agency is not utilizing data loss prevention capabilities; forensics and visibility capabilities; or digital rights management capabilities, a description of the reasons for not utilizing such capabilities.

According to SBA officials, due to the lack of funding and continuity in senior leadership, SBA has not implemented a robust information security program to include DLP capabilities for data in-use and at rest, or data rights management capabilities.

Information Security Management Practices over Contractors (SEC406-b-2.E)

A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph (D).

SOP 90 47 3 establishes the security requirements for entities, including contractors, that provide services to SBA. It requires SBA to include security clauses within the executed contracts to help ensure that the entities, including contractors, adhere to the information security management practices described in subparagraph (D). Although the security clause exists within their contracts, SBA does not review the entities', including contractors, implementation of SBA's information management practices.

Additionally, SBA performs annual security control assessments for each SBA system (including contractor systems) in order to determine that security controls are designed, implemented and operating effective in accordance with SBA and federal security requirements.

According to SBA officials, due to a lack of resources, SBA does not have sufficient personnel to complete internal assessments over all contractor systems in FY 2016 in order to determine that the entities, including contractors, are enforcing contractual requirements to conduct inventories of the software present and licenses associated with such software; implement capabilities to monitor and detect exfiltration, including: data loss prevention, forensics and visibility, and digital rights management capabilities.

APPENDIX I: LIST OF ACRONYMS

Acronym	Definition
A&A	Authorization and Accreditation
AC	Access Controls
CIGIE	Council of Inspectors General on Integrity and Efficiency
DLP	Data Loss Prevention
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GPO	Group Policy Object
IDS	Intrusion Detection System
ISE	Identity Services Engine
KPMG	KPMG LLP
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personally Identity Verification
SBA	Small Business Administration
SEC406	The Cybersecurity Act of 2015, Section 406, Federal Computer Security, Pub. L. 114-113, 129 Stat. 694
SOC	Security Operations Center
SOP	Standard Operating Procedure