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

Final Report Transmittal
Report Number: 18-08

DATE: December 18, 2017

TO: Linda E. McMahon
Administrator

FROM: Hannibal "Mike" Ware
Acting Inspector General

SUBJECT: KPMG Management Letters Communicating Matters Relative to SBA's FY 2017 Financial Statement Audit and DATA Act Attestation Engagement

We contracted with the independent certified public accounting firm KPMG LLP (KPMG) to audit the U.S. Small Business Administration's (SBA's) consolidated financial statements for fiscal year (FY) 2017, ending September 30, 2017, and to perform an attestation engagement regarding SBA's FY 2017 second quarter submission, in accordance with the Digital Accountability and Transparency Act of 2014 (DATA Act).

The engagements were conducted in accordance with applicable standards contained in the U.S. Government Accountability Office's (GAO's) *Government Auditing Standards.* The financial statement audit was also performed in accordance with the Office of Management and Budget's Bulletin No. 17-03, *Audit Requirements for Federal Financial Statements*; GAO/President's Council on Integrity and Efficiency *Financial Audit Manual;* and GAO's *Federal Information System Controls Audit Manual.* Additionally, the DATA Act examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and guidance issued in the U.S. Department of the Treasury Office of Inspector General's publication, *Inspectors General Guide to Compliance Under the DATA Act*.

The management letters represent matters that were identified during the respective engagements. Specifically, KPMG reported that

- there were inadequate reviews of time and attendance reports for the financial statement audit (see Exhibit I), and
- improvement was needed in information technology general and application controls related to the DATA Act (see Exhibit II).

In the management letters, KPMG addressed recommendations to the Chief Human Capital Officer, and the Chief Information Officer in coordination with SBA program offices. We provided a draft of KPMG's findings to each of these officials or their designees, who fully or substantially concurred with the findings relative to their respective areas. The officials or designees agreed to implement the recommendations or have already taken action to address the underlying conditions. Should you have any questions, please contact me at (202) 205-6586 or Andrea Deadwyler, Assistant Inspector General for Audits, at (202) 205-6616.

***

cc: Allie Coetzee, Deputy Administrator
Pradeep Belur, Chief of Staff
Tim Gribben, Chief Financial Officer and Associate Administrator for Performance Management
Maria Roat, Chief Information Officer
Dorrice Roth, Deputy Chief Financial Officer
Nate Reboja, Director of Financial Systems
Christopher Pilkerton, General Counsel
Martin Conrey, Attorney Advisor, Legislation and Appropriations
LaNae Twite, Director, Office of Internal Controls
Michael Simmons, Attorney Advisor

Attachments

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

December 14, 2017

Hannibal “Mike” Ware
Acting Inspector General
U.S. Small Business Administration
Washington, DC 20416

Tim Gribben
Chief Financial Officer
U.S. Small Business Administration
Washington, DC 20416

In planning and performing our audit of the consolidated financial statements of the U.S. Small Business Administration (SBA), as of and for the year ended September 30, 2017 and 2016, in accordance with auditing standards generally accepted in the United States of America, the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and the Office of Management and Budget Bulletin No. 17-03, *Audit Requirements for Federal Financial Statements*, we considered SBA’s internal control over financial reporting (internal control) as a basis for designing auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of SBA’s internal control. Accordingly, we do not express an opinion on the effectiveness of SBA’s internal control.

During our audit, we noted certain matters related to internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized in Exhibit I. We would be pleased to discuss these comments and recommendations with you at any time.

In addition, we identified a combination of certain deficiencies in internal control that we considered to be significant deficiencies, and communicated them in writing to management and those charged with governance on November 14, 2017.

Our audit procedures were designed primarily to enable us to form an opinion on the financial statements, and therefore may not have brought to light all weaknesses in policies or procedures that may have existed. We aim, however, to use our knowledge of the SBA that we gained during our work to make comments and suggestions that we hope will be useful to you.

This communication is intended solely for the information and use of SBA management, the Office of Inspector General, and others within the organization, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

Exhibit I

U.S. Small Business Administration

Management Letter Comments

Inadequate Review of STAR Time and Attendance Worksheets

The SBA has controls in place to ensure the timely review and approval of System for Time and Attendance Reporting (STAR) Time and Attendance (T&A) Worksheets as well as requests for leave or approved absence. During our fiscal year 2017 audit test work over the approval and certification STAR T&A Worksheets and related supporting documentation for amounts certified, in a sample of 40 payroll transactions, we noted the following eight control deficiencies:

- three STAR T&A Worksheets could not be provided timely for audit review;
- two STAR T&A Worksheets were not signed by the timekeeper (certifier) and supervisor (approver) until after the payroll disbursement;
- one other STAR T&A Worksheet was not signed by the supervisor (approver) until after the payroll disbursement occurred;
- one STAR T&A Worksheet was not dated by the employee's supervisor; and
- one instance where the STAR T&A Worksheet was not signed by the timekeeper or the employee's supervisor.

Criteria

SBA Manager's Toolkit, Time and Attendance

Question: How do I ensure timely processing of T&A for my office? Answer:

- Ensure all STAR T&A Worksheets are signed by timekeeper, employee, and supervisors.
- Ensure timekeepers do not transmit T&A before all the proper signatures are obtained.
- All T&A must be transmitted by COB on Friday following the end of the pay period.

These deficiencies were caused by the lack of adequate oversight and proper accountability for supervisors and timekeepers to perform timely, sufficient reviews and approvals of hours charged by employees.

When an employee's timekeeper and/or supervisor does not properly approve the STAR T&A Worksheet, there is no evidence that the employee's hours are accurate. This could result in a misstatement in the payroll expense reported in SBA's financial statements.

We recommend that the Chief Human Capital Officer

1. Continues to reinforce policies and procedures regarding the certification of STAR T&A Worksheets with supervisors and timekeepers (i.e., issuance of a memorandum, training).
2. Continues to perform periodic quality assurance reviews to ensure supervisors and timekeepers are properly certifying and dating all STAR T&A Worksheets.

3. Develops and implements appropriate enforcement actions against individuals and offices with multiple instances of noncompliance.

Management's Response

SBA management concurred with the findings and recommendations.

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

December 14, 2017

Hannibal “Mike” Ware
Acting Inspector General
U.S. Small Business Administration
Washington, DC 20416

Tim Gribben
Chief Financial Officer
U.S. Small Business Administration
Washington, DC 20416

Ladies and Gentlemen:

We have examined the U.S. Small Business Administration’s (SBA’s) fiscal year 2017, second quarter financial and award spending data presented in the Files A, B, C, D1, and D2 (the selected files) prepared for publication on Beta.USASpending.gov in accordance with the Digital Accountability and Transparency Act of 2014 (DATA Act) (hereinafter referred to as the submission), and have issued our report thereon dated November 8, 2017. In planning and performing our examination of the selected files of the SBA, we considered internal controls over the submission as a basis for designing our examination procedures for the purpose of expressing our opinion on the selected files. The objective of our audit was to express an opinion on whether the selected files were presented in accordance with the criteria described above and not for the purpose of expressing an opinion on the internal control over reporting of the selected files or on compliance and other matters. Accordingly, we do not express an opinion on the effectiveness of SBA’s internal control.

During our examination, we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized in Exhibit II. We would be pleased to discuss these comments and recommendations with you at any time.

Our examination procedures were designed primarily to enable us to form opinion on the submission and therefore may not have brought to light all weaknesses in policies or procedures that may have existed. We aim, however, to use our knowledge of the SBA that was gained during our work to make comments and suggestions that we hope will be useful to you.

This communication is intended solely for the information and use of SBA management, the Office of Inspector General, and others within the organization, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

Exhibit II

U.S. Small Business Administration

Management Letter Comments

Complexity Password Settings not Enabled for an SBA System

Passwords were not configured to meet the standards established in Standard Operating Procedure (SOP) 90 47 3*, Information System Security Program* for an SBA system. Specifically, the system's "password verify function", which enforces the requirements for the minimum password length and password complexity of the system administrators, was not enabled throughout the attestation period from January 1, 2017 to March 31, 2017. As of August 10, 2017, the above condition was addressed by the SBA and is considered closed.

Due to the lack of management oversight, the password complexity requirement was not enabled for the database. The lack of strong passwords increases the risk of access by individuals without the appropriate privileges, compromise of the system, data and the integrity of information produced by the system.

4. We recommend that the Chief Information Officer (CIO) continues to work with SBA program offices to enforce password configurations processes and controls that meet the minimum requirements established in SBA's information technology security policy.

Management's Response

Management concurs with the factual accuracy of this condition.

Inadequate Retention of System Access Modification Records

An SBA system was not configured to retain audit records of user access modifications in accordance with SOP 90 47 3. Specifically, SOP 90 47 3 requires system owners to retain audit records for at least one year; however, one system was only configured to retain audit records for 180 days (six months). This system is a commercial-off-the-shelf software package and as of August 2017, was configured to purge the audit details after 180 days.

The inconsistent implementation of audit log standards throughout the Agency increases the risk that the SBA is unable to perform effective continuous monitoring of systems and security events (e.g., new user additions) that occur in the system. Further, unauthorized events could go undetected and not be investigated and resolved in a timely manner.

5. We recommend that the CIO enhances audit logging retention settings to meet the minimum standards defined by SOP 90 47 3.

Management's Response

Management agrees with the condition that is stated, however the condition omits an acknowledgement that SOP 90 47 4 was issued on September 8, 2017, and the system's configuration is in compliance with the new SOP. As a result, SBA management does not concur with the recommendation and believes this issue should have been closed.

Exhibit II

Access Recertification Controls Need Improvement

An SBA office has not implemented adequate access recertification controls to review all front-end and back-end accounts at least semi-annually in accordance with SOP 90 47 3. Specifically:

a) Application end-user recertification is designed to only identify terminated users that no longer need access, and users that need to be removed completely from the system. However, supervisors do not review the user roles and privileges to ensure that roles continue to be appropriate.

b) All accounts were not reviewed during the February 2017 account recertification.

The following causes were noted for each respective item above:

a) Due to system limitations, the SBA is unable to produce a system generated listing of all active users with their enabled roles. Therefore, the user roles are currently not included in the account listings that are provided to the supervisors for review.

b) According to SBA management, all accounts were not reviewed during the February 2017 account recertification because the accounts are static.

Without effective access recertification controls, the SBA cannot attest to the accuracy of each user's access to its systems, which leads to the risk of inappropriate access and modification to the data processed and stored within the systems.

We recommend that the CIO continues to work with SBA program offices to:

6. Enhance account recertification controls for end-user accounts, application and system accounts, and all administrator accounts to help ensure that all enabled roles are reviewed for appropriateness and accounts are disabled or modified as necessary.

7. Formally document a risk acceptance memo in accordance with SBA's information technology security policy for static accounts that are deemed unnecessary to periodically review and implement compensating controls to monitor the usage of these static accounts.

Management's Response

Management concurs with the factual accuracy of these conditions.