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

Final Report Transmittal
Report Number: 16-02

DATE: November 16, 2015

TO: Maria Contreras-Sweet
Administrator, Small Business Administration

Douglas Kramer
Deputy Administrator, Small Business Administration

Tami Perriello
Chief Financial Officer, Small Business Administration

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

SUBJECT: *Independent Auditors' Report on SBA's FY 2015 Financial Statements*

We contracted with the independent certified public accounting firm KPMG LLP (KPMG) to audit the U.S. Small Business Administration's (SBA) consolidated financial statements for fiscal year (FY) 2015, ending September 30, 2015. This audit is an annual requirement of the Chief Financial Officers' Act of 1990, and was conducted in accordance with the *Generally Accepted Government Auditing Standards*; the Office of Management and Budget Bulletin No. 15-02, *Audit Requirements for Federal Financial Statements*; and the U.S. Government Accountability Office's *Financial Audit Manual* and *Federal Information System Controls Audit Manual.*

The attached independent auditors' report presents an unmodified opinion on SBA's consolidated financial statements for FY 2015. Specifically, KPMG reported that:

- The financial statements were fairly presented in all material aspects in conformity with U.S. generally accepted accounting principles.
- There were no material weaknesses in internal control.
- There is a significant deficiency related to SBA's information technology security controls, which has been identified in the past.
- There is one instance of noncompliance with laws and regulations related to the Debt Collection Improvement Act of 1996, which also has been reported in the past.

KPMG noted that SBA management identified a matter that may be reported as a violation of the Antideficiency Act. The outcome of this matter and any resulting ramifications is not presently known.

Details regarding KPMG's conclusions are included in the "Compliance and Other Matters" section, and Exhibit I to this report. Within 30 days of this report, KPMG expects to issue a separate letter to SBA management regarding other, less significant matters that came to its attention during the audit.

We reviewed a copy of KPMG's report and related documentation and made necessary inquiries of their respective representatives. Our review was not intended to enable us to express—and we do not express—an opinion on SBA's financial statements, KPMG's conclusions about the effectiveness of internal controls, or its conclusions about SBA's compliance with laws and regulations. However, our review disclosed no instances where KPMG did not comply, in all material respects, with the *Generally Accepted Government Auditing Standards*.

We provided a draft of KPMG's report to SBA's Chief Financial Officer, who concurred with its findings and recommendations and agreed to implement the recommendations. The Chief Financial Officer's comments are attached as Exhibit II to this report.

We appreciate the cooperation and assistance of SBA and KPMG. Should you or your staff have any questions, please contact me at (202) 205-7390 or Jeffrey R. Brindle, Director of the Information Technology and Financial Management Group at (202) 205-7490.

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

Attachment

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

Independent Auditors' Report

Inspector General
United States Small Business Administration:

Report on the Financial Statements

We have audited the accompanying consolidated financial statements of the U.S. Small Business Administration (SBA), which comprise the consolidated balance sheets as of September 30, 2015 and 2014, and the related consolidated statements of net cost, and changes in net position, and combined statements of budgetary resources for the years then ended, and the related notes to the consolidated financial statements.

Management's Responsibility for the Financial Statements

SBA's management is responsible for the preparation and fair presentation of these consolidated financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of consolidated financial statements that are free from material misstatement, whether due to fraud or error.

Auditors' Responsibility

Our responsibility is to express an opinion on these consolidated financial statements based on our audits. We conducted our audits 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 Office of Management and Budget (OMB) Bulletin No. 15-02, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin No. 15-02 require that we plan and perform the audit to obtain reasonable assurance about whether the consolidated financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the consolidated financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the consolidated financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the consolidated financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the consolidated financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion on the Financial Statements

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of the U.S. Small Business Administration as of September 30, 2015 and 2014, and its net costs, changes in net position, and budgetary resources for the years then ended in accordance with accounting principles generally accepted in the United States of America.

Other Matters

Within the Management's Discussion and Analysis and Other Information, sections of the *Agency Financial Report*, Management has elected to include references to information on websites to provide additional information for the users of its financial statements. Such information is not a required part of the basic consolidated financial statements or supplementary information required by the Federal Accounting Standards Advisory Board. The information on these websites or the other interactive data has not been subjected to any of our auditing procedures, and accordingly we do not express an opinion or provide any assurance on it.

Required Supplementary Information

Accounting principles generally accepted in the United States of America require that the information in Management's Discussion and Analysis, Required Supplementary Information, and Required Supplementary Stewardship Information be presented to supplement the basic consolidated financial statements. Such information, although not a part of the basic consolidated financial statements, is required by the Federal Accounting Standards Advisory Board who considers it to be an essential part of financial reporting for placing the basic consolidated financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America, which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic consolidated financial statements, and other knowledge we obtained during our audits of the basic consolidated financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Other Information

Our audits were conducted for the purpose of forming an opinion on the basic consolidated financial statements as a whole. The Message from the Administrator, Other Information, and the information on pages 41 to 45 of the *Agency Financial Report*, are presented for purposes of additional analysis and are not a required part of the basic consolidated financial statements. Such information has not been subjected to the auditing procedures applied in the audit of the basic consolidated financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

Other Reporting Required by *Government Auditing Standards*

Internal Control Over Financial Reporting

In planning and performing our audit of the consolidated financial statements as of and for the year ended September 30, 2015, we considered SBA's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the consolidated 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. We did not test all internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our fiscal year 2015 audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, we did identify a combination of certain deficiencies in internal control, described in Exhibit I that we consider to be a significant deficiency.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether SBA's consolidated financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 15-02. Specifically, our audit results noted noncompliance with the Debt Collection Improvement Act of 1996 (DCIA or Act) which is described below:

> The DCIA gave the U.S. Department of Treasury (Treasury) significant responsibilities for collecting delinquent debts, Government-wide. The Act requires Federal agencies to transfer their nontax delinquent debt to Treasury. During our test work over loan charge-offs, we noted that SBA did not timely refer obligors (i.e., eligible principal borrowers, co-borrowers, and/or guarantors) to Treasury for offset or cross-servicing as required by DCIA. Similar instances of noncompliance with the Act were reported in prior years. SBA's noncompliance with the DCIA was the result of deficiencies in information technology controls. For additional discussion of the information technology aspects of this finding and the related recommendation, see Exhibit I.

Additionally, management has identified a matter that may be reported as a violation of the Antideficiency Act. The outcome of this matter, and any resulting ramifications, is not presently known.

We also performed tests of SBA's compliance with certain provisions referred to in Section 803(a) of the Federal Financial Management Improvement Act of 1996 (FFMIA). Providing an opinion on compliance with FFMIA was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests of FFMIA disclosed no instances in which SBA's financial management systems did not substantially comply with (1) Federal financial management systems requirements, (2) applicable Federal accounting standards, and (3) the United States Government Standard General Ledger at the transaction level.

SBA's Response to Findings

SBA's response to the findings identified in our audit is described in the accompanying Exhibit II. SBA's response was not subjected to the auditing procedures applied in the audit of the consolidated financial statements and, accordingly, we express no opinion on the response.

Purpose of the Other Reporting Required by Government Auditing Standards

The purpose of the communication described in the Other Reporting Required by *Government Auditing Standards* section is solely to describe the scope of our testing of internal control and compliance and the result of that testing, and not to provide an opinion on the effectiveness of SBA's internal control or compliance. Accordingly, this communication is not suitable for any other purpose.

KPMG LLP

Washington, DC
November 16, 2015

Exhibit I

U.S. Small Business Administration

Significant Deficiency

Improvement Needed in Information Technology Security Controls

During the FY 2015 financial statement audit, we found that the U.S. Small Business Administration (SBA) continued to implement corrective actions on some of the prior year findings; however, a number of conditions persisted in FY 2015 that reduced SBA's ability to effectively manage its information system risks. As a result, collectively, these conditions continue to present a significant deficiency in SBA's internal control environment.

In an effort to provide additional clarity to SBA management with respect to the corrective actions required, we enhanced our prior year recommendations where issues persisted in FY 2015, and issued additional recommendations for the new control deficiencies identified. In the sections below, we distinguish between recurring conditions and related recommendations, and those that were newly identified in FY 2015. We have omitted some technical details from the conditions and recommendations due to the sensitivity of the information. These details were communicated to management in Notices of Findings and Recommendations throughout the audit.

We have summarized the Information Technology (IT) control deficiencies that we noted during the FY 2015 audit below, and have organized them by the following general IT control objectives: logical access controls, application change management, system configuration management, and contingency planning.

Logical Access Controls

An integral part of the effectiveness of an organization's security program management efforts should be to ensure that logical access controls provide reasonable assurance that IT resources, such as data files, application programs, and IT-related facilities/equipment, are protected against unauthorized modification, disclosure, loss, or impairment.

Our audit found that the following control deficiencies identified in prior year(s) persisted in FY 2015:

- User accounts were not properly authorized in accordance with SBA policy.
- User accounts were not recertified in accordance with SBA policy.
- The principle of "least privilege" for user/service accounts with administrator privileges was not enforced.
- User accounts were not disabled or promptly removed upon personnel termination.
- The employee exit clearance and contractor off-boarding processes were not standardized to ensure that access to SBA's systems was timely removed upon separation.
- Processes for consistently and effectively reviewing audit logs were not implemented.

U.S. Small Business Administration

Significant Deficiency

Recommendations – Logical Access Controls:

We have issued the following recommendations to address the repeat control deficiencies listed in the section above.

We recommend that the Chief Information Officer (CIO) coordinate with SBA program offices to:

1. 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.
2. 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.
3. 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.
4. Improve SBA's administration of logical system access by taking the following actions:
   - Implement an effective off-boarding process, and periodically verify that controls to remove logical access for separated employees are implemented and operating as designed;
   - Establish a process for the identification and removal of separated contractors to help ensure that access is timely removed upon contractor separation; and
   - Timely remove access to general support systems and major applications (including development and test environments) when employees and contractors are terminated.
5. 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.

Application Change Management

The integrity of information processing is dependent on the controlled management of changes to the software that controls the processing. Software change management is designed to reduce the risk of unauthorized or erroneous changes to software. Our audit found the following control deficiencies remain, that were identified in a prior year:

U.S. Small Business Administration

Significant Deficiency

- The change management process for one system, which includes several applications, did not sufficiently reduce the risk of an unauthorized change being made to the production environment. Specifically, the SBA did not review or compare system code to ensure that only authorized changes had been made, and the audit log review process was not designed to detect unauthorized changes to application software.
- Required software changes for one subsystem were not implemented due to the ongoing code migration project which impacted SBA's compliance with the Debt Collection Improvement Act of 1996 in that system. This issue was reported as a noncompliance matter in the "Compliance and Other Matters" section of our audit report.

In addition to the matters above, we noted the following additional control deficiency during our FY 2015 audit:

- The Security Authorization Package for one system was not updated to reflect control changes resulting from the migration to a new system environment, and the system was not reauthorized in accordance with SBA policy.

<u>Recommendations – Application Change Management:</u>

We have issued the following recommendations to address the repeat control deficiencies listed in the section above, and recommend that the:

6. Associate Administrator, Office of Capital Access (OCA), in coordination with the CIO, design and implement a combination of preventative and detective controls to address the issues and related risks in the condition above, and ensure an auditable trail of software changes is maintained to prevent and detect unauthorized changes to production programs.
7. Associate Administrator, OCA, in conjunction with the CIO, perform a comprehensive review of system protocols to determine if any other coding problems exist that may cause untimely referral of obligors, and address outstanding system protocol issues as identified.

To address the newly identified change management control weakness, we recommend that the:

8. Associate Administrator, OCA, in coordination with the CIO, 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.

System Configuration Management

The primary focus of an organization's system configuration management process should be to control the security configuration of its infrastructure including servers, databases, network equipment, security appliances, and security services. Without such controls, there is a risk that security features could be inadvertently, or deliberately, omitted or turned off, introducing risk into the IT environment.

Our audit noted that the following prior year control deficiency persisted in FY 2015:

- Numerous critical-, high- and medium-risk configuration and patch management vulnerabilities were noted in certain systems.

U.S. Small Business Administration

Significant Deficiency

Recommendation – System Configuration Management:

To address the repeat system configuration management condition above, we recommend that the:

9. CIO coordinate with SBA program offices to address the existing configuration and patch management vulnerabilities noted during our assessment to be in compliance with SBA policy and SBA Information System Vulnerability Management Plan, Version 1.0. In addition, implement procedures to ensure the consistent implementation and monitoring of SBA approved security configuration baselines across SBA's workstations, servers, databases, network devices, and other security relevant appliances.

Contingency Planning

The focus of an organization's contingency planning program should be to provide reasonable assurance that information resources are protected and the risk of unplanned interruptions is minimized. Without such controls, there is a risk that data may be lost or that critical operations may not resume in a timely manner.

Our audit noted that the following prior year control deficiencies persisted in FY 2015:

- Some of the systems were not configured to retain full backups in accordance with SBA Standard Operating Procedure (SOP) 90.47.3, *Information System Security Program*.
- Incremental or full backups for some of the systems were not retained in accordance with SOP 90.47.3.

Recommendation – Contingency Planning:

To address the repeat contingency planning conditions above, we recommend that the:

10. CIO, Chief Financial Officer, and Associate Administrator, OCA, ensure that incremental and full backups for all systems, including related support infrastructure, are configured and retained in accordance with SBA policies.

Exhibit II

CFO Response to Draft Audit Report on FY 2015 Financial Statements

DATE: November 16, 2015

TO: Troy Meyer, Assistant Inspector General for Auditing

FROM: Tami Perriello, Associate Administrator for Performance Management and Chief Financial Officer

Tami Perriello

SUBJECT: Draft Audit Report on FY 2015 Financial Statements

The Small Business Administration has received the draft Independent Auditors' Report from KPMG that includes the auditors' opinion on the financial statements and its review of the Agency's internal control over financial reporting and compliance with laws and regulations. The independent audit of the Agency's financial statements and related processes is a core component of SBA's financial management program.

We are pleased that the SBA has again received an unmodified audit opinion with no material weaknesses from the independent auditor. We believe these results accurately reflect the quality of the Agency's financial statements and our improved accounting, budgeting and reporting processes. As you know, the SBA has worked hard in past years to address the findings from our independent auditor. Our core financial reporting data and processes have further improved, and we are proud that the results of our efforts have been confirmed.

The audit report includes a continuing significant deficiency in SBA's information technology controls. The SBA will continue to work on improvements in IT security, specifically in access controls, change controls and mitigation of vulnerabilities.

The auditor reported again this year that the SBA is not compliant with the Debt Collection Improvement Act of 1996 related to timely referral of charged-off loans to the Department of the Treasury for its tax refund offset and collection programs. Although the SBA made improvements to correct systemic errors identified last year, the auditors again found instances of charged-off loans where co-borrowers and guarantors were not referred to Treasury. The SBA is working on procedures to correct this issue.

The auditor reported that a potential violation of the Antideficiency Act was identified during the year. The SBA has taken appropriate steps to correct the problem identified and is in the process of preparing the reports required under the Act.

We appreciate your efforts and those of your colleagues in the Office of the Inspector General, as well as those of KPMG. The independent audit process continues to provide us with new insights and valuable recommendations that will further enhance SBA's financial management practices. We remain committed to excellence in financial management and look forward to making more progress in the coming year.