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

**TRANSMITTAL MEMORANDUM**
Report No. 14-04

**DATE:** December 16, 2013

**TO:** Jonathan I. Carver
Chief Financial Officer

**FROM:** Robert A. Westbrooks
Deputy Inspector General

**SUBJECT:** *Independent Auditors' Report* on the SBA's FY 2013 Financial Statements

We contracted with the independent public accounting firm, KPMG LLP (KPMG), to audit the U.S. Small Business Administration's consolidated financial statements as of September 30, 2013, and for the years then ended. The contract required that the audits be conducted in accordance with *Generally Accepted Government Auditing Standards;* the Office of Management and Budget Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*, and the U.S. Government Accountability Office's *Financial Audit Manual and Federal Information System Controls Audit Manual.* This audit is an annual requirement of the Chief Financial Officers Act of 1990.

The results of KPMG's audits are presented in the attached report. The report includes an opinion on SBA's financial statements, internal control over financial reporting, and compliance and other matters that have a direct and material effect on the financial statements. The independent auditor issued an unmodified opinion on SBA's fiscal year 2013 consolidated financial statements. In summary, 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 is a repeat condition.
- There is one instance of noncompliance with laws and regulations related to the Debt Collection Improvement Act of 1996, which is also a repeat condition.

Details regarding KPMG' s conclusions are included in the "Compliance and Other Matters " section, and Exhibit I of *the Independent Auditors' Report.* Within 30 days of this report, KPMG expects to issue a separate letter to 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 the SBA's financial statements, KPMG's conclusions about the effectiveness of internal control, 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 *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 the SBA and KPMG. Should you or your staff have any questions, please contact me at (202) 205-6587 or Jeffrey R. Brindle, Director, Information Technology and Financial Management Group at (202) 205-7490.

Attachment

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

# Independent Auditors' Report

The Inspector General,
U.S. 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, 2013 and 2012, and the related consolidated statements of net cost, and changes in net position, and the 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*

Management is responsible for the preparation and fair presentation of these consolidated financial statements in accordance with U.S. generally accepted accounting principles; 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. 14-02, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin No. 14-02 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, 2013 and 2012, and its net costs, changes in net position, and budgetary resources for the years then ended in accordance with U.S. generally accepted accounting principles.

***Other Matters***

*Required Supplementary Information*

U.S. generally accepted accounting principles require that the information in the Management's Discussion and Analysis, Required Supplementary Information, and Required Supplementary Stewardship Information sections 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 31 to 35 of the *Agency Financial Report*, is presented for purposes of additional analysis and is 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, we considered the 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 the SBA's internal control. Accordingly, we do not express an opinion on the effectiveness of the 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 audit, we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, we did identify a deficiency in internal control, described in Exhibit I, related to information technology security controls, that we consider to be a significant deficiency.

***Compliance and Other Matters***

As part of obtaining reasonable assurance about whether the 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, and certain provisions of other laws and regulations specified in OMB Bulletin No. 14-02. 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. 14-02, and which are described below.

***The Debt Collection Improvement Act of 1996 (DCIA).*** The DCIA assigns the U.S. Department of Treasury (Treasury) the responsibility for collecting delinquent debts, Government-wide. The DCIA requires federal agencies to transfer their nontax debt over 180 days delinquent to Treasury. During our testwork over loan charge-offs, we noted the SBA did not refer obligors (eligible principal borrowers, co-borrowers, and/or guarantors) to the Treasury for offset or cross-servicing at the time of charge-off, as required by DCIA. Similar instances of noncompliance with the DCIA were reported in prior years. These deficiencies were primarily the result of inadequate information technology controls. We recommend the Associate Administrator, Office of Capital Access:

1. Conduct training to educate loan center staff on the proper steps to refer obligors to Treasury and correct errors after the initial referral.

2. Reinforce the importance of retaining identifying information for all obligors.

3. Implement robust, quarterly monitoring reviews to identify and correct all charged-off loans where the automatic referral did not occur.

For additional discussion of the information technology aspects of this finding, see Exhibit I.

We also performed tests of its 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 the SBA's financial management systems did not substantially comply with the (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***

The SBA's response to the findings identified in our audit is described in Exhibit II. The 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 the SBA's internal control or compliance. Accordingly, this communication is not suitable for any other purpose.

KPMG LLP

December 16, 2013

**Exhibit I**

**U.S. Small Business Administration**

Significant Deficiency

***Improvement Needed in Information Technology Security Controls***

During our Fiscal Year (FY) 2012 financial statement audit, we identified information technology (IT) control findings and issued 19 recommendations for corrective actions. During the FY 2013 financial statement audit, we found that the U.S. Small Business Administration (SBA) implemented corrective actions on some of the findings noted; however, a number of conditions persisted in FY 2013 that reduced SBA's ability to effectively manage its information system risk. As a result, collectively, these conditions 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 2013, and issued additional recommendations for the new control weaknesses identified. In the sections below, we distinguish between recurring conditions and related recommendations, and those that were newly identified in FY 2013. We have omitted some technical details from the conditions and recommendations due to the sensitivity of the information. These details were communicated to management through Notices of Findings and Recommendations (NFRs).

We have summarized the IT control deficiencies that we noted during the FY 2013 audit below, and have organized them by the following general IT control objectives: logical and physical access controls, application change management, system configuration management, and contingency planning.

*Logical and Physical Access Controls*

An integral part of the effectiveness of an organization's security program management efforts should be to ensure that logical and physical 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 the prior year persisted in FY 2013:

- User accounts to the network and some financial systems were not disabled or removed promptly upon personnel termination.
- User accounts to the network and some financial systems were not recertified in accordance with SBA policy.
- User accounts to one financial system and SBA's network were not properly authorized.
- A process for consistently and effectively reviewing audit logs for the network and financial systems was not implemented.
- A security incident response standard operating procedure had not been finalized.
- Responsibilities for approving, administering, and reviewing physical access to the Head Quarters (HQ) data center had not been defined.
- Numerous high- and medium-risk security vulnerabilities were noted in the network and infrastructure supporting certain financial systems.
- Port-based network security had not been implemented across SBA program offices.

In addition to the matters above, we noted the following additional control weaknesses during our FY 2013 audit:

- Remote access to SBA information systems was not configured and provisioned in accordance with SBA policy.
- Network administrative rights were not properly restricted and security settings were not enforced across all parts of the network.

Recommendations – Logical and Physical Access Controls:

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

We recommend that the Chief Information Officer (CIO) coordinate with SBA program offices to[1]:

4. Improve SBA's administration of logical system access by taking the following actions:
   - 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;
   - Establish a process for the identification and removal of separated contractors in order to help ensure that access is timely removed upon contractor separation; and
   - Remove access to the general support systems and major applications (including development and test environments) timely when terminated employees and contractors are identified.
5. 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.
6. 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.
7. Enforce a network access security baseline(s) across the network, consistent with SBA security policy, Office of Management and Budget directives, and United States Government Configuration Baseline requirements.
8. 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, and their ability to implement effective and sustainable continuous monitoring;
   - Implement and enforce consistent and effective creation of audit records, capturing of relevant auditable events, auditing (i.e., manual or automated review of audit records) for specified

[1] The recommendations listed in this exhibit were sequenced after the recommendations presented in the *Independent Auditors' Report*, to assist users of this report in tracking the number of recommendations presented.

events, and automated alerting on specified events across SBA's infrastructure using a risk-based approach; and

- Develop an agency-wide plan and schedule for implementation of the above recommendations.

9. Finalize, implement, and monitor its entity-wide Incident Response Policy or Standard Operating Procedure.
10. Review the list of individuals with HQ data center access permissions periodically, to ensure that only authorized personnel retain access to the HQ data center.
11. Implement port-based network access controls across SBA's network.
12. Address the vulnerabilities noted during the FY 2013 audit, to be in compliance with SBA policy and SBA Vulnerability Assessment Team (VAT) Internal Operating Procedures, Version 1.4. In addition, implement procedures to ensure the consistent identification, tracking, and resolution of security vulnerabilities across SBA's workstations, servers, databases, network devices, and other security relevant appliances.

To address the newly identified logical and physical access control weakness, we are issuing the following recommendations.

We recommend that the CIO coordinate with SBA program offices to:

13. 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.
14. Improve SBA's remote access program, by taking the following actions:
    - Incorporate security requirements into the Teleworking SOP, to be consistent with NIST 800-46 Rev 1;
    - Ensure employees acknowledge compliance with security requirements prior to establishing a remote connection to SBA's network when Teleworking or otherwise connecting remotely to SBA systems; and
    - Monitor compliance with the revised SOP 90.47.3 and the updated Teleworking SOP.

*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 of software. Our audit found the following control deficiencies:

- The change management process for some financial 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 only authorized changes had been made, and the audit log review process was not designed to detect unauthorized changes to application software.
- Detective controls to mitigate the risk of a known segregation of duties issue did not operate for the full fiscal year.

- Required software changes for one financial subsystem were not implemented due to the ongoing code migration project which impacted SBA's compliance with the *Debt Collection Improvement Act of 1996* (DCIA) in that system. This issue was reported as a noncompliance matter in the Compliance and Other Matters section of our audit report.

Recommendations – Application Change Management:

In our prior year report, we issued the following recommendation to address issues with respect to SBA's compliance with the DCIA. We are reissuing that recommendation to address the condition identified above:

15. We recommend that the 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.

In addition, we are issuing the following recommendations to address the additional application change management conditions identified in FY 2013:

16. We recommend that the Chief Financial Officer (CFO) continues to perform the mitigating controls implemented during FY 2013 to ensure that the risks associated with privileged access remain mitigated.
17. We recommend that the Associate Administrator, OCA, in conjunction with the CIO continues to review system protocols to determine if any other coding problems exist that may cause untimely referral of loans, and address outstanding system protocol issues from prior years.

*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 2013:

- Numerous high- and medium-risk configuration management vulnerabilities were noted in the network and infrastructure supporting certain financial systems.

We also identified the following new control weakness as a result of our FY 2013 audit procedures:

- The SBA did not perform periodic, authenticated vulnerability scans for all financial systems.

Recommendations – System Configuration Management:

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

18. The CIO coordinate 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 (VAT) 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's workstations, servers, databases, network devices, and other security relevant appliances.

In addition, we recommend that:

19. The CFO and the Associate Administrator, Office of Disaster Assistance, implement scans of financial systems in its production environment using privileged access authorization.

*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 2013:

- HQ backup tapes necessary to restore system operations were not rotated off-site in accordance with SBA policy.
- An alternate processing site for some financial systems and related support infrastructure had not been established.

Recommendations – Contingency Planning:

We recommend that the CIO:

20. Designs and implements procedures and controls to ensure HQ backup tapes are rotated on a periodic basis in accordance with SBA policies and plans.
21. Designs and implements procedures, resources, and controls to ensure the timely recovery of resources and systems hosted by SBA HQ.

Exhibit II

## CFO Response to Draft Audit Report on FY 2013 Financial Statements

**DATE:** December 16, 2013

**TO:** Robert A. Westbrooks, Deputy Inspector General

**FROM:** Jonathan I. Carver, Chief Financial Officer

**SUBJECT:** Draft Audit Report on FY 2013 Financial Statements

The Small Business Administration has received the draft Independent Auditors' Report from KPMG that includes the auditor's 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 from the independent auditor with no material weaknesses. 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 by the independent auditor.

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. The SBA will track, monitor, and aggressively mitigate vulnerabilities in all Agency systems. Furthermore, the SBA will clarify and strengthen detailed procedures required to ensure security access controls are in place to protect SBA data from unauthorized modification, disclosure, and loss.

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 auditor 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.

We appreciate all of 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 continue to be committed to excellence in financial management and look forward to making more progress in the coming year.