



U.S. SMALL BUSINESS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL
AUDITING DIVISION

AUDIT REPORT

Issue Date: November 12, 2010

Number: 11-03

To: Jonathan I. Carver
Chief Financial Officer
/s/ Original Signed

From: Debra S. Ritt
Assistant Inspector General for Auditing

Subject: Audit of SBA's FY 2010 Financial Statements

Pursuant to the Chief Financial Officer's Act of 1990, attached is a copy of the *Independent Auditors' Report* issued by KPMG LLP on the Small Business Administration's financial statements for the fiscal year ended September 30, 2010. The audit was performed under a contract with the Office of Inspector General (OIG) and in accordance with *Generally Accepted Government Auditing Standards*; Office of Management and Budget's (OMB) Bulletin 07-04, *Audit Requirements for Federal Financial Statements*, as amended; the Government Accountability Office (GAO)/President's Council on Integrity and Efficiency (PCIE) *Financial Audit Manual*; and GAO's *Federal Information System Controls Audit Manual*.

The KPMG report concluded that SBA's consolidated financial statements presented fairly, in all material respects, the financial position of SBA as of and for the years ended September 30, 2010 and 2009. It also presented fairly, in all material respects, SBA's net costs, changes in net position, and combined statements of budgetary resources for the years then ended.

With respect to internal controls, KPMG continued to report a significant deficiency related to Information Technology security controls. Details regarding the matters that led to the auditor's conclusion on internal controls are further discussed in Exhibit I of the *Independent Auditors' Report*. KPMG's test for compliance with certain laws, regulations, contracts and grant agreements determined that the Agency did not fully comply with the Debt Collection Improvement Act of 1996 because guidelines regarding referrals of delinquent debt for Treasury cross-servicing and offset were not consistently followed. Details regarding the auditor's conclusion are included in the "Compliance and Other Matters" section of the *Independent Auditors' Report*. The auditors did not report any other instances or matters regarding noncompliance.

We provided a draft of KPMG's report to SBA's Chief Financial Officer (CFO), who concurred with its findings and recommendations and agreed to implement the recommendations. The CFO is delighted that SBA has again received an unqualified

audit opinion and believes these results accurately reflect the quality of the Agency's financial statements and its improved accounting, budgeting and reporting processes.

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 appreciate the cooperation and assistance of SBA and KPMG. Should you or your staff have any questions, please contact me at (202) 205-^[FOIA ex. 2] or Jeffrey R. Brindle, Director, Information Technology and Financial Management Group at (202) 205-^[FOIA ex. 2]

Attachment



KPMG LLP
2001 M Street, NW
Washington, DC 20036-3389

Independent Auditors' Report

Office of Inspector General,
U.S. Small Business Administration:

We have audited the accompanying consolidated balance sheets of the U.S. Small Business Administration (SBA) as of September 30, 2010 and 2009, and the related consolidated statements of net cost and changes in net position, and combined statements of budgetary resources (hereinafter referred to as "consolidated financial statements") for the years then ended. The objective of our audits was to express an opinion on the fair presentation of these consolidated financial statements. In connection with our Fiscal Year (FY) 2010 audit, we also considered SBA's internal control over financial reporting and tested SBA's compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements that could have a direct and material effect on these consolidated financial statements.

Summary

As stated in our opinion on the consolidated financial statements, we concluded that SBA's consolidated financial statements as of and for the years ended September 30, 2010 and 2009, are presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles.

Our consideration of internal control over financial reporting resulted in identifying certain deficiencies that we consider to be a significant deficiency, as defined in the Internal Control Over Financial Reporting section of this report, as follows:

Improvement Needed in Information Technology (IT) Security Controls

We did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses as defined in the Internal Control Over Financial Reporting section of this report.

The results of our tests of compliance with certain provisions of laws, regulations, contracts, and grant agreements disclosed one instance of noncompliance that is required to be reported under *Government Auditing Standards*, issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*, as amended.

Noncompliance with the Debt Collection Improvement Act

The following sections discuss our opinion on SBA's consolidated financial statements; our consideration of SBA's internal control over financial reporting; our tests of SBA's compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements; and management's and our responsibilities.



U.S. Small Business Administration
November 12, 2010
Page 2 of 4

Opinion on the Financial Statements

We have audited the accompanying consolidated balance sheets of SBA as of September 30, 2010 and 2009, 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.

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of SBA as of September 30, 2010 and 2009, and its net costs, changes in net position, and budgetary resources for the years then ended, in conformity with U.S. generally accepted accounting principles.

The information in the Management's Discussion and Analysis, Required Supplementary Information, and Required Supplementary Stewardship Information sections is not a required part of the consolidated financial statements, but is supplementary information required by U.S. generally accepted accounting principles. We have applied certain limited procedures, which consisted principally of inquiries of management regarding the methods of measurement and presentation of this information. However, we did not audit this information and, accordingly, we express no opinion on it.

Internal Control Over Financial Reporting

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.

Our consideration of internal control over financial reporting was for the limited purpose described in the Responsibilities section of this report and was not designed to identify all deficiencies in internal control over financial reporting that might be deficiencies, significant deficiencies, or material weaknesses. In our FY 2010 audit, we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses, as defined above. However, we identified a deficiency in internal control over financial reporting described in Exhibit I that we consider to be a significant deficiency in internal control over financial reporting. 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.

Exhibit II presents the status of the prior year material weakness, and Exhibit III presents the status of the prior year significant deficiency.

We noted certain additional matters that we have reported to management of SBA in a separate letter dated November 12, 2010.

Compliance and Other Matters

The results of certain of our tests of compliance as described in the Responsibilities section of this report, exclusive of those referred to in the *Federal Financial Management Improvement Act of 1996* (FFMIA), disclosed one instance of noncompliance that is required to be reported herein under *Government Auditing Standards* or OMB Bulletin No. 07-04, and is described below.



Debt Collection Improvement Act of 1996 (DCIA). During our testwork over loan charge-offs, we noted SBA did not refer loans to Treasury for cross-servicing in accordance with the DCIA. Specifically, we noted ten loan charge-off transactions that were not referred to Treasury for cross-servicing. Two of the ten loans were loan guaranties that were not referred at time of charge-off. The remaining eight loans were not referred due to outdated referral system programming logic which prevented the automatic referral of charged-off loans to Treasury. Through additional research covering the population of Disaster loans charged-off during FY 2010, SBA identified a total of 473 disaster loans that were not referred for cross-servicing. Of the 473 loans identified, 334 loans were not referred due to the referral dates being out of the system range parameter; thus preventing the system from transmitting the loan referrals to Treasury. SBA was unable to determine why the remaining 139 charged-off loans were not referred. According to SBA management, efforts are underway to address the issues noted which caused the system errors. Further, SBA management agreed to perform an analysis of Disaster loans charged-off in prior years to identify and correct potential additional issues of noncompliance. Exhibit IV presents the status of the prior year noncompliance finding.

The results of our other tests of compliance as described in the Responsibilities section of this report, exclusive of those referred to in FFMIA, disclosed no instances of noncompliance or other matters that are required to be reported herein under *Government Auditing Standards* or OMB Bulletin No. 07-04.

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.

* * * * *

Responsibilities

Management's Responsibilities. Management is responsible for the consolidated financial statements; establishing and maintaining effective internal control; and complying with laws, regulations, contracts, and grant agreements applicable to SBA.

Auditors' Responsibilities. Our responsibility is to express an opinion on the FY 2010 and 2009 consolidated financial statements of SBA 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 OMB Bulletin No. 07-04. Those standards and OMB Bulletin No. 07-04 require that we plan and perform the audits to obtain reasonable assurance about whether the consolidated financial statements are free of material misstatement. An audit includes consideration of internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of SBA's internal control over financial reporting. Accordingly, we express no such opinion.



U.S. Small Business Administration
November 12, 2010
Page 4 of 4

An audit also includes:

- Examining, on a test basis, evidence supporting the amounts and disclosures in the consolidated financial statements;
- Assessing the accounting principles used and significant estimates made by management; and
- Evaluating the overall consolidated financial statement presentation.

We believe that our audits provide a reasonable basis for our opinion.

In planning and performing our FY 2010 audit, we considered the SBA's internal control over financial reporting by obtaining an understanding of SBA's internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls as a basis for designing our auditing procedures 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 over financial reporting. Accordingly, we do not express an opinion on the effectiveness of SBA's internal control over financial reporting. We did not test all controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982*.

As part of obtaining reasonable assurance about whether SBA's FY 2010 consolidated financial statements are free of material misstatement, we performed tests of SBA's 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 the consolidated financial statement amounts, and certain provisions of other laws and regulations specified in OMB Bulletin No. 07-04, including the provisions referred to in Section 803(a) of FFMIA. We limited our tests of compliance to the provisions described in the preceding sentence, and we did not test compliance with all laws, regulations, contracts, and grant agreements applicable to SBA. However, providing an opinion on compliance with laws, regulations, contracts, and grant agreements was not an objective of our audit and, accordingly, we do not express such an opinion.

* * * * *

SBA's response to the findings identified in our audit are presented in Exhibit V. We did not audit SBA's response and, accordingly, we express no opinion on it.

This report is intended solely for the information and use of SBA's management, SBA's Office of Inspector General, OMB, the U.S. Government Accountability Office, and the U.S. Congress and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

November 12, 2010

U.S. Small Business Administration

Significant Deficiency

The significant deficiency identified for the year ended September 30, 2010, is summarized below:

(1) Improvement Needed in Information Technology (IT) Security Controls

We made many recommendations to address IT weaknesses identified during the Fiscal Year (FY) 2009 SBA audit. Although SBA has made some progress related to the FY 2009 weaknesses, improvements are still necessary. During FY 2010, we noted additional weaknesses in security access controls, including configuration and patch management, and segregation of duties. We are not providing details in this report on the specific weaknesses due to their sensitivity, but we have provided the details under a separate cover to SBA management.

Security Access Controls

Integral to an organization's security program management efforts, system security access controls should 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.

A summary of the security access weaknesses we identified during the FY 2010 SBA financial statement audit follows:

- We identified several high and medium risk security vulnerabilities affecting various financial systems. We provided the detailed vulnerabilities to SBA management.
- We identified weaknesses in network access controls.
- We noted several high and medium risk security vulnerabilities affecting another key financial system, which is hosted by an SBA service provider. Although the service provider was monitoring the vulnerabilities and a plan to mitigate such weaknesses was developed, it was not implemented at the time of our review.
- We identified system patches that were not applied in a timely manner to a key financial system. Based on review of the Plan of Actions and Milestones (POA&M) for the system, we could not determine whether corrective actions were made timely.
- Password configuration settings for two key financial systems need improvement. We noted that one financial system did not enforce user password history, password complexity or account lockout after a specified number of failed login attempts. Another key financial system did not enforce password history, password complexity, password changes after 90 days, or account lockout after a specified number of failed login attempts. In addition, we found that password length settings are not compliant with SBA Standard Operating Procedure (SOP) 90.47.2, *Automated Information Systems Security Program*.
- Physical access control procedures are not current and have not been implemented at one SBA location.
- Several users have unnecessary access to a SBA financial subsystem.
- User accounts are not periodically reviewed for three key financial systems.
- There are weak controls over the monitoring and review of audit logs for four of seven systems we reviewed.

U.S. Small Business Administration

Significant Deficiency

Recommendations – Security Access Controls:

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

1. Improve the vulnerability tracking and monitoring process to fully address high and medium risk vulnerabilities for key financial systems. Ensure that the vulnerability reports are reviewed and analyzed on a regular basis. Periodically monitor the existence of necessary services and protocols running on servers and network devices. Develop a more thorough approach to track and mitigate patch management and configuration management vulnerabilities identified during monthly scans.
2. Prevent users from anonymously connecting unauthorized devices by developing and implementing procedures to ensure mandatory domain authentication for IP address issuance.
3. Improve the POA&M review and approval process for key financial systems. In addition, include all unresolved weaknesses on the POA&M (including vulnerabilities identified at service providers).
4. Enforce financial system password controls for System Administrators and Database Administrators (DBAs) and physical access controls in accordance with SBA SOP 90.47.2.
5. Develop and implement procedures for user access reviews to ensure that proper access rights are set for financial subsystems.
6. Oversee the review and validation of financial system accounts on a periodic basis.
7. Implement a process to monitor the audit logs of all financial applications on a regular basis.

Segregation of Duties

The primary focus of an organization's segregation of duties controls is to provide reasonable assurance that incompatible duties are effectively segregated. Without such controls, there is a risk that unauthorized changes could be implemented into the IT environment, and users may have access that is inappropriate for their duties. As a result, the confidentiality, integrity, and availability of financial data are at risk of possible loss, modification, or disclosure.

A summary of the segregation of duties control deficiencies we identified during the FY 2010 SBA financial statement audit follows:

- Application programmers for a key financial system have the ability to make changes and implement the changes into the production environment.
- Access to the development and production libraries of a key financial system is not restricted based on job role/functions or privileges.
- Certain Information Security staff and DBAs have incompatible access privileges for a financial system, which enable them to perform the user administration functions (i.e., grant any role, create user, become user, alter user, or drop user). We determined that compensating IT controls are not in place to mitigate this weakness.

U.S. Small Business Administration

Significant Deficiency

Recommendations – Segregation of Duties:

We recommend the Chief Financial Officer:

8. Implement procedures and conduct audits of financial system software changes to ensure all changes are sufficiently approved and tested.

We also recommend the CIO:

9. Restrict access to software program libraries based on the principle of least privilege, and periodically review access to the libraries.
10. Separate user and data administration functions for financial systems, or implement compensating IT controls such as management review of user administration functions.

Security Management

An entity-wide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. This security management program should establish a framework, and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

A summary of the security management weaknesses we identified during the FY 2010 SBA financial statement audit follows:

- A mandatory training program for IT security personnel has not been implemented.
- We could not obtain sufficient evidence that media was sanitized properly in accordance with SBA policy.
- SBA implemented end-user security policies and procedures in May 2010, but the policies were not implemented during FY 2010.

Recommendations – Security Management:

We recommend the CIO:

11. Develop a comprehensive security education and training program for all IT security personnel and a method for monitoring the training program.
12. Implement and enforce the procedures documented in SOP 90.47.2 for sanitizing media to be disposed and for maintaining a log of employees who sanitize media to validate the appropriateness of the sanitization process.
13. Coordinate with program offices using end-user programs containing sensitive data, such as Personally Identifiable Information and financial data, to implement end-user computing procedures in accordance with the guidance.

U.S. Small Business Administration

Significant Deficiency

Software Configuration Management

The primary focus of an organization's software configuration management process is to control the software changes made to networks and systems. Without such controls, there is a risk that security features could be inadvertently, or deliberately, omitted or turned off, or that processing irregularities or malicious code could be introduced into the IT environment.

A summary of the configuration management weaknesses we identified during the FY 2010 SBA financial statement audit follows:

- The configuration management process is not centralized, and the Enterprise Change Control Board governance processes are not fully implemented across SBA.
- SBA personnel could not provide sufficient evidence to support software change authorizations for several financial systems.

Recommendations – Software Configuration Management:

We recommend the CIO:

14. Enforce an organization-wide configuration management process, to include policies and procedures for maintaining documentation that supports testing and approvals of software changes.

U.S. Small Business Administration
 Status of Prior Year Material Weakness

Fiscal Year 2009 Finding	Fiscal Year 2010 Status of Finding
<p>During Fiscal Year (FY) 2009, we reported a material weakness in internal control related to SBA’s financial reporting.</p>	<p>During FY 2010, SBA made significant operational improvements over the controls surrounding the year-end financial reporting process. These improvements included automating previously manual processes and increasing the level of financial statement review performed by personnel within the Office of the Chief Financial Officer. In addition, our testwork did not identify any significant misstatements in FY 2010.</p> <p>Therefore, in FY 2010, this matter is closed.</p>

U.S. Small Business Administration
Status of Prior Year Significant Deficiency

Fiscal Year 2009 Finding	Fiscal Year 2010 Status of Finding
Improvement Needed In Information Technology (IT) Security Controls	<p>During our review of SBA's IT general and application controls, we noted minimal improvements made to address prior year findings. Therefore, control deficiencies continue to exist.</p> <p>Therefore, in fiscal year 2010, the presentation of the issue was modified to reflect current year operations, and we continue to report a significant deficiency in internal controls as it relates to IT systems and their impact on the consolidated financial statements. See Exhibit I for additional information.</p>

U.S. Small Business Administration

Status of Prior Year Noncompliance

Fiscal Year 2009 Finding	Fiscal Year 2010 Status of Finding
<p><i>Debt Collection Improvement Act of 1996 (DCIA)</i></p> <p>During our Fiscal Year (FY) 2009 audit, as stated in its <i>Federal Managers' Financial Integrity Act (FMFIA)</i> Assurance Statement, SBA management reported the agency was noncompliant with the DCIA in FY 2009. The noncompliance was due to instances where SBA did not refer a substantial number of charged off loans to Treasury for offset and cross servicing.</p>	<p>During our review over SBA's compliance with the DCIA, we noted improvements made in SBA's Treasury offset and cross-servicing referral process. However, during FY 2010 we noted instances of noncompliance related to timely referrals of loan charge-offs to Treasury for cross-servicing.</p> <p>Therefore, in FY 2010, the issue is again presented in the Compliance and Other Matters section of our Independent Auditors' Report.</p>



U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, D.C. 20416

DATE: November 12, 2010

TO: Debra Ritt, Assistant IG for Auditing
[FOIA ex. 6]

FROM: Jonathan Carver, Chief Financial Officer

SUBJECT: Draft Audit Report on FY 2010 Financial Statements

The Small Business Administration is in receipt of the draft Independent Auditors' Report from KPMG that includes the auditor's opinion on the financial statements and 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 delighted that the SBA has again received an unqualified audit opinion from the independent auditor with no reported 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 over the past several years to address the findings from our independent auditors. Our core financial reporting data and processes have improved substantially, 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. As the auditors noted in their report on the 2010 financial statements, the SBA made substantial progress in resolving IT deficiencies. The SBA will continue to improve the Agency's IT security during the upcoming fiscal year. The SBA is developing plans to 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 audit report identified one instance of non-compliance with applicable laws and regulations as of September 30, 2010. Due to a system error, 473 of 8,229 charged off disaster loans, or 5.7 percent, were not referred to Treasury for cross-servicing and for the Treasury offset as required by the Debt Collection Improvement Act. This represents \$11.3 million of the \$247.5 million disaster loans written-off in FY 2010, or 4.6 percent. The system issue has been identified and is in the process of being remedied, and a mitigation plan has been developed to ensure that this issue will not recur. All loans eligible for Treasury referral will be referred within the next six months. In FY2009, through the SBA's self-assessment process it was identified that the agency was not referring non-disaster loans for the Treasury off-set program; this was corrected in FY2010. There were no issues identified in the testing of the improved internal controls over non-disaster loans by both our independent auditors and our OMB A-123 team in the current year, and we anticipate the same successful resolution for the disaster loans in FY 2011.

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.