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

AUDIT REPORT
Issue Date: November 14, 2008
Number: 9-03

To: Sandy K. Baruah
Acting Administrator

Jennifer Main
Chief Financial Officer

[FOIA Ex 6 ____]

From: Debra S. Ritt
Assistant Inspector General for Auditing

Subject: Audit of SBA's FY 2008 Financial Statements

Pursuant to the Chief Financial Officer's Act of 1990, attached are *the Independent Auditors' Report* and accompanying reports on internal control and compliance with laws and regulations issued by KPMG LLP for the fiscal year ending September 30, 2008. 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, 2008 and 2007. 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 control over financial reporting, KPMG continued to report a significant deficiency related to Information Technology controls; but did not consider this deficiency to be a material weakness. KPMG noted that SBA made progress in several areas in its efforts to address prior year Information Technology internal control deficiencies. However, despite these improvements, deficiencies continue to exist for security access controls, software program changes, and end-user computing. Details regarding this significant deficiency are discussed more in Exhibit 1 of the *Independent Auditors' Report.*

KPMG's test for compliance with certain laws, regulations, contracts and grant agreements disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards,* and Bulletin 07-04, as amended.

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 with no reported material weaknesses 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 G*enerally 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[ex 2] or Jeffrey R. Brindle, Director, Information Technology and Financial Management Group at (202) 205-[ex 2]

Attachments

KPMG LLP
2001 M Street, NW
Washington, DC 20036

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, 2008 and 2007, and the related consolidated statements of net cost, 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 2008 audit, we also considered SBA's internal controls 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, 2008 and 2007, are presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles.

Our opinion emphasized that the current economic conditions give rise to risks associated with the uncertainty of future events and actual losses to the agency will be dependent upon future economic and market conditions.

Our consideration of internal control over financial reporting resulted in the following condition being identified as a significant deficiency:

- Improvement Needed in Information Technology (IT) Controls

However, we did not consider this significant deficiency to be a material weakness.

The results of our tests of compliance with certain provisions of laws, regulations, contracts, and grant agreements disclosed no instances of noncompliance or other matters that are 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.

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.

KPMG

OPINION ON THE FINANCIAL STATEMENTS

We have audited the accompanying consolidated balance sheets of SBA as of September 30, 2008 and 2007, and the related consolidated statements of net cost, 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, 2008 and 2007, 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.

As discussed in note 17 to SBA's financial statements, SBA continues to evaluate the risks posed by the current market downturn on its direct loan and loan guaranty portfolios, but the impact of such future risks cannot be reasonably estimated at this time. Actual losses, if any, will largely depend on future economic and market conditions and could differ materially from SBA's current estimates.

The information in the Management 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 and OMB Circular No. A-136, *Financial Reporting Requirements*. 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

Our consideration of the internal control over financial reporting was for the limited purpose described in the Responsibilities section of this report and would not necessarily disclose all deficiencies in the internal control over financial reporting that might be significant deficiencies or material weaknesses.

A control deficiency 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 misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects SBA's ability to initiate, authorize, record, process, or report financial data reliably in accordance with U.S. generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of SBA's consolidated financial statements that is more than inconsequential will not be prevented or detected by SBA's internal control over financial reporting. A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by SBA's internal control.

In our fiscal year 2008 audit, we consider the deficiency described in Exhibit I to be a significant deficiency in internal control over financial reporting; however, we do not believe the significant deficiency described in Exhibit I is a material weakness. A summary of the status of the prior year significant deficiency, and management's response to our findings, is included as Exhibits III and IV, respectively.

We also noted certain additional matters that we reported to SBA's management in a separate letter dated November 14, 2008.

COMPLIANCE AND OTHER MATTERS

The results of our tests of compliance described in the Responsibilities section of this report, exclusive of those referred to in the *Federal Financial Management Improvement Act of 1996* (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, as amended.

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 fiscal year 2008 and 2007 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, as amended. Those standards and OMB Bulletin No. 07-04, as amended, 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.

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
- Evaluating the overall consolidated financial statement presentation.

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

In planning and performing our fiscal year 2008 audit, we considered SBA's internal control over financial reporting by obtaining an understanding of the 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. We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982*. The objective of our audit was not to express an opinion on the effectiveness of SBA's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the SBA's internal control over financial reporting.

As part of obtaining reasonable assurance about whether SBA's fiscal year 2008 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 SBA financial statement amounts, and certain provisions of other laws and regulations specified in OMB Bulletin No. 07-04, as amended, 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 report is presented in Exhibit IV. 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 14, 2008

Exhibit I

U.S. Small Business Administration

Significant Deficiency

Introduction

The internal control deficiency discussed in this report and the U.S. Small Business Administration's (SBA) progress toward correcting it are discussed in the context of SBA's organizational structure and its ability to obtain funding to take corrective action. Exhibit I herein describes the control deficiencies, which collectively resulted in the significant deficiency reported below, for the year ended September 30, 2008, and our recommendations thereon. The status of prior year noncompliance and internal control deficiencies are reported in Exhibits II and III, respectively, and SBA management's response is presented in Exhibit IV.

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

During fiscal year 2008, we noted that SBA made progress in several areas in its efforts to address prior year IT internal control deficiencies. Despite these improvements, we also noted that deficiencies continued to exist in the areas of security access controls, software program changes, and end-user computing.

Security Access Controls

Integral to an organization's security program management efforts, technical security access controls for systems and applications 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 control deficiencies we identified during the fiscal year 2008 SBA financial statement audit follow:

[FOIA Ex 2]

- Neither OCIO nor DCMS officials were able to ensure that security vulnerability scans were consistently performed for two DCMS devices physically located at SBA Headquarters. This issue was identified by the SBA Office of Inspector General (OIG) during the OIG's annual Federal Information Security Management Act (FISMA) evaluation.

[FOIA Ex 2]

- The OCIO does not appropriately control remote access authorizations. Specifically, remote access is not always requested and approved by the employees' supervisor, and can be requested by the employees

themselves. Further, e-mail approvals from supervisors are not retained for all remote access requests. As a result, controls over remote access authorization are more difficult to implement and validate.

- Validation of physical access to the data center at SBA's headquarters is not performed in accordance with SBA Standard Operating Procedure (SOP) 90-47.2, *Automated Information Systems Security Program*, which requires that a listing of authorized personnel for SBA computer facilities (e.g., server rooms) be maintained and access be revalidated at least quarterly.

- OCIO management is unable to provide reasonable assurance that electronic media is sufficiently sanitized prior to disposal, in accordance with SOP 90-47.2. The SOP requires that (1) media must be sanitized prior to disposal by using one of the three approved methods: overwriting, degaussing, or destruction, and (2) a log of who completed the sanitation action must be maintained.

- OCIO management was unable to provide reasonable assurance that access to the Loan Accounting System (LAS) and Local Area Network (LAN)/Wide Area Network (WAN) was periodically validated, in accordance with National Institute of Standards and Technology (NIST) guidance and SOP 90-47.2.

These issues are consistent with findings identified by the OIG in past years. In fact, the OIG has identified IT security as a serious SBA management challenge since at least fiscal year 2000.

Despite these issues, SBA has made significant improvements in recent years in the area of IT security, and there is commitment from the SBA to continue further improvements continue.

Recommendations – Security Access Controls:

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

[FOIA Ex 2]

3. Ensure the completion of more consistent vulnerability assessments to identify and resolve potential vulnerabilities, both within SBA offices and at service providers.

4. Implement procedures to control the process for requesting and granting remote access and implement procedures to retain the appropriate approval evidence for tracking and validation.

5. Implement controls to comply with SOP 90-47.2 regarding the validation of physical access to the data center.

6. Implement controls to comply with SOP 90-47.2 regarding the sanitizing of media prior to disposal.

7. Retain documentation supporting the validation of LAS and LAN/WAN system access in accordance with NIST guidance and SOP 90-47.2.

Software Program Changes

The primary focus of an organization's software change controls (which also encompasses patch management and configuration management efforts) is on controlling the software changes made to systems and applications in operation. 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 software program change control deficiencies we identified during the fiscal year 2008 SBA financial statement audit follow:

- The Office of Disaster Assistance (ODA) was unable to provide evidence that baseline configurations for the DCMS were updated in a timely manner. This issue was also identified in fiscal year 2007, and SBA was still in the process of implementing corrective actions during fiscal year 2008.

- The OCIO was unable to provide evidence that (1) testing was performed for four of eight selected LAS software changes, (2) approvals were made for two of eight selected LAS software changes, and (3) testing and approvals were documented for three selected Electronic Transaction System (E-TRAN) software changes.

- The OCIO was unable to provide evidence that changes to the LAN/WAN were appropriately tracked, approved, and implemented.

- Ineffective software program change controls in the Joint Administrative and Accounting Management System (JAAMS) directly led to duplicate payments in the amount of $11,205,608.

- The Office of the Chief Financial Officer (OCFO) was unable to provide evidence that the software change requests were consistently completed for JAAMS and the Financial Reporting Information System (FRIS).

- The OCIO was unable to provide evidence that baseline configurations for LAS were updated in a timely manner. Documented baseline configurations enable the process of tracking and controlling software changes, especially as system security settings are changed.

- The Office of the Chief Operating Officer (OCOO), in conjunction with SBA program offices, has not documented segregation of duty procedures for LAS. Consequently, we could not validate that incompatible software change duties were appropriately segregated. This issue was also identified in fiscal year 2007, and SBA was still in the process of implementing corrective actions during fiscal year 2008.

Recommendations – Software Program Changes:

We recommend the following:

8. ODA management ensures the consistent application of controls and procedures to document the DCMS baseline configuration.

9. OCIO management consistently apply procedures for documenting software change testing results, testing approvals, and final approvals. Specifically, such procedures and controls need to be consistently applied for LAS, E-TRAN, and LAN/WAN.

10. OCFO management consistently apply procedures for documenting software change testing results, testing approvals, and final approvals for JAAMS and FRIS.

11. OCIO management ensures the consistent application of controls and procedures to document the LAS baseline configuration.

12. OCOO, in conjunction with program offices, document and implement segregation of duty policies and procedures for LAS.

End-User Computing

End-user computing tools/programs (e.g., spreadsheets and other user-developed programs) present the need for a unique set of general control needs within an organization. By its nature, end-user computing brings the development and processing of information systems closer to the user. End-user computing capabilities typically include access to any end-user developed programs or objects, such as spreadsheets that contain critical data/information. Critical data/information could include Personally Identifiable Information (PII) and financial data. While this environment may not typically be subjected to the same level of rigor and structure as an IT general controls environment, policies and procedures in this area are important to the overall IT environment. We noted many SBA program offices, including the OCFO, Office of Capital Access, and Office of Human Capital Management, have not implemented end-user computing policies and procedures set forth and provided by the OCIO to identify, track, and protect end-user programs containing sensitive information.

Recommendations – End-User Computing:

13. We recommend that the OCIO reemphasize the importance to SBA program offices of controlling end-user programs containing sensitive data, such as PII and financial data, in accordance with OCIO policy.

Exhibit II

U.S. Small Business Administration

Status of Prior Year Noncompliance

Fiscal Year 2007 Noncompliance	Fiscal Year 2008 Status of Noncompliance
Debt Collection Improvement Act of 1996 (DCIA) During our audit for fiscal year 2007, we noted that SBA did not consistently follow Treasury guidelines when referring delinquent debts for collection in accordance with DCIA. Specifically, we noted that 47 of 140 delinquent debt referral transactions tested were not referred timely or were coded improperly in SBA's Loan Accounting System. These exceptions prompted SBA to examine if there were additional loans that were improperly referred to Treasury. As a result of this examination, management determined it did not refer approximately 24,000 delinquent debts for Treasury in accordance with DCIA. SBA management believes that the issue stems from outdated standard operating procedures and a lack of clear instructions to field offices regarding the referral of delinquent debt to Treasury. Towards the end of fiscal year 2007, SBA management established revised protocols that provide clear instructions to field offices to ensure compliance with DCIA.	The results of our tests of compliance with DCIA in fiscal year 2008 disclosed no instances in which SBA is in substantial noncompliance with DCIA.

Exhibit III

U.S. Small Business Administration

Status of Prior Year Significant Deficiency

Fiscal Year 2007 Findings	**Fiscal Year 2008 Status of Findings**
1. Improvement needed in management information technology security controls	During our review of SBA's information technology (IT) general and application controls, we noted improvements in formalizing policies and procedures over sanctioning contractors that don't complete annual computer security awareness training, increasing storage space for audit logs and retention of the logs themselves, implementing day-to-day data center employee responsibilities and end-user computing user-level access control policies, and finalizing Change Control Board Charter for enterprise-wide changes. However, we continued to identify opportunities for SBA to improve its internal controls. The control deficiencies that continue to exist are in the following areas: security access controls, software program changes, and end-user computing. Therefore, in fiscal year 2008, 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.

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

CFO Response to Draft Audit Report on FY 2008 Financial Statements

DATE: November 14, 2008

TO: Debra Ritt, Assistant IG for Auditing

FROM: Jennifer Main, Chief Financial Officer [Ex 6]

SUBJECT: Draft Audit Report on FY 2008 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. Additionally, the report found that SBA is in compliance with all applicable laws and regulations again this year. 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 many 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, however, includes a continuing significant deficiency in the SBA's information technology controls. While we appreciate the recognition in the report of the substantial progress the SBA has made in this area, we are nonetheless disappointed that the significant improvements we have made were not sufficient for the auditor to eliminate this finding. During FY 2008, the SBA's Office of the Chief Information Officer instituted several processes to strengthen information security controls and took a multitude of corrective actions to address previous audit findings, closing 24 out of 41 previous findings. In addition, OCIO made significant progress on the SBA's Management Challenges reported by our Inspector General, scoring green on two key critical areas affecting service continuity controls and computer security training. We do, however, recognize that further improvements are needed in SBA's information

technology controls, and the SBA is committed to taking all necessary action to eliminate this significant deficiency in future audit reports.

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.