



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

AUDIT REPORT

Issue Date: November 14, 2008

Number: 9-04

To: Department of Treasury, Financial Management Service

From: Debra S. Ritt
Assistant Inspector General for Auditing

Subject: GFRS for Fiscal Year 2008

Pursuant to OMB Circular A-136, *Financial Reporting Requirements* (Circular A-136) and the *Treasury Financial Manual*, Part 2, Chapter 4700 (TFM 2-4700), attached is the *Independent Auditors' Report* on Special-Purpose Financial Statements, issued by KPMG LLP on the Small Business Administration's (SBA) reclassified balance sheet as of September 2008 and 2007, and the reclassified statements of net costs and changes in net position and Federal trading partner note for the year then ended (hereinafter referred to as the special-purpose financial statements).

The auditor found that the statements, including the Federal trading partner note, present fairly in all material respects, the financial position of SBA as of September 30, 2008 and 2007. Also, the results of operations and the changes in net position for the period then ended are in accordance with U.S. generally accepted accounting principles, and the presentation is in conformance with the requirements of TFM 2-4700. As requested, the following documents are attached:

- (1) reclassified financial statements;
- (2) GF004F Trading Partner Summary Note Report;
- (3) GF003G Closing Package Line Reclassification Summary Report;
- (4) GF006 FR Notes Report;
- (5) GF007 Other Data Report;
- (6) Management Representation Letter on the Closing Package, including the Summary of Unadjusted Misstatement; and
- (7) Closing Package *Independent Auditors' Report*.

We reviewed KPMG's report and related documentation and made necessary inquiries of their representatives. Our review was not intended to enable us to express, and we do not express, an opinion on the SBA's reclassified financial statements or on conclusions about

internal control and the SBA's compliance with laws and regulations. However, our review disclosed no instances where KPMG did not comply, in all materials respects, with *Generally Accepted Government Auditing Standards*.

We appreciate the cooperation and assistance of SBA and KPMG representatives. Should you or your staff have any questions, please contact me at (202) 205-6121 or Jeffrey R. Brindle, Director, Information Technology and Financial Management Group at (202) 205-6121

Attachments

Distribution:

Department of Treasury, Financial Management Services: financial.reports@fms.treas.gov

Government Accountability Office: USCFS@gao.gov

OMB, Office of Federal Financial Management: Statements@omb.eop.gov



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 Closing Package Financial Statement Report – Balance Sheet of the U.S. Small Business Administration (SBA) as of September 30, 2008 and 2007 the related Closing Package Financial Statement Report – Statement of Net Cost and Statement of Changes in Net Position, and the accompanying Financial Report (FR) Notes Report (except for the information contained in the sections entitled “Threshold”) for the years then ended; the accompanying Additional Note No. 27; the accompanying Trading Partner Summary Note Report – Balance Sheet as of September 30, 2008 and 2007 and the related Trading Partner Summary Note Report – Statement of Net Cost and Statement of Changes in Net Position for the years then ended (hereinafter collectively referred to as the special-purpose financial statements). These special-purpose financial statements are the responsibility of SBA’s management. Our responsibility is to express an opinion on these special-purpose 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. 07-04, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin No. 07-04 require that we plan and perform the audits to obtain reasonable assurance about whether the special-purpose 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 special-purpose financial statements and assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall special-purpose financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

The accompanying special-purpose financial statements have been prepared for the purpose of complying with the requirements of Chapter 4700 of the U.S. Department of the Treasury’s *Treasury Financial Manual* (TFM), as described in Additional Note No. 27, solely for the purpose of providing financial information to the U.S. Department of the Treasury and the U.S. Government Accountability Office (GAO) to use in preparing and auditing the *Financial Report of the U.S. Government*, and are not intended to be a complete presentation of SBA’s consolidated financial statements.

In accordance with *TFM Chapter 4700*, SBA prepared FR Notes Report Nos. 1 through 26, except for FR Notes Report Nos. 10A, 16, 21, 23, and 24, which were not applicable to SBA. SBA included Additional Note No. 27, to disclose other data not contained in the special-purpose financial statements, but which is necessary to make the special-purpose financial statements more informative.



In our opinion, the special-purpose 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 and changes in net position for the years then ended in conformity with U.S. generally accepted accounting principles and the presentation pursuant to the requirements of *TFM Chapter 4700*, as described in Additional Note No. 27.

SBA also prepared Other Data Report Nos. 1 through 17, except for Other Data Report Nos. 3 through 8, and 11 through 14, which were not applicable to SBA. The information included in the Other Data Report Nos. 9 (except for the information in the section entitled "Threshold"), 10, 15, 16, and 17 is presented for the purpose of additional analysis and is not a required part of the special-purpose financial statements, but is supplementary information required by U.S. generally accepted accounting principles and the *TFM Chapter 4700*. 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 supplementary information, and accordingly, we express no opinion on it.

Our audits were conducted for the purpose of forming an opinion on the special-purpose financial statements taken as a whole. The information included in the Other Data Report Nos. 1 and 2 is presented for purposes of additional analysis and is not a required part of the special-purpose financial statements. This information has been subjected to the auditing procedures applied in the audits of the special-purpose financial statements and, in our opinion, is fairly stated in all material respects in relation to the special-purpose financial statements taken as a whole.

The information entitled "Threshold" in Other Data Report No. 9 and the information in the sections entitled "Threshold" in FR Notes Data Report Nos. 2, 3, 4A, 9, 15, and 19; the information in the Closing Package Line Reclassification Summary Report – Balance Sheet; and the information in the Closing Package Line Reclassification Summary Report – Statement of Net Cost, and Changes in Net Position are presented for purposes of additional analysis and are not a required part of the special-purpose financial statements. This information has not been subjected to the auditing procedures applied in the audits of the special-purpose financial statements, and accordingly, we express no opinion on it.

The *TFM Chapter 4700* requires agencies to use the Governmentwide Financial Reporting System to input certain data as described in Additional Note No. 27. Except as discussed in this report, we express no opinion on information maintained in that system.

In accordance with *Government Auditing Standards* and OMB Bulletin No. 07-04, we have also issued our reports dated November 14, 2008 on our consideration of SBA's internal controls over financial reporting and the results of our tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, and other matters that are required to be reported under *Government Auditing Standards*. Those reports are an integral part of the audits of the consolidated balance sheets of SBA as of September 30, 2008 and 2007, and the related consolidated statements of net cost, and changes in net position, and combined statements of budgetary resources (hereinafter collectively referred to as consolidated financial statements) for the years then ended, performed in accordance with *Government Auditing Standards* and OMB Bulletin No. 07-04, and should be read in conjunction with this report in considering the results of our audits of the special-purpose financial statements. Our audit of the consolidated financial statements of SBA as of and for the year ended September 30, 2008 disclosed one significant deficiency as described more fully in Exhibit I. Exhibit II contains management's response. We did not audit management's response, and accordingly, we express no opinion on it.

Management is responsible for establishing and maintaining effective internal control. In planning and performing our audit of the fiscal year 2008 special-purpose financial statements, we also considered SBA's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing our opinion on the special-purpose 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.

Our consideration of internal control over financial reporting for special-purpose financial statements was for the limited purpose described in the preceding paragraph of this section and would not necessarily identify all deficiencies in the internal control over financial reporting for special-purpose financial statements 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 special-purpose financial statements that is more than inconsequential will not be prevented or detected by SBA's internal control. 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 special-purpose financial statements will not be prevented or detected by SBA's internal control.

In our fiscal year 2008 audit, we did not identify any deficiencies in internal control over financial reporting for the special-purpose financial statements that we consider to be material weaknesses as defined above.

Management is responsible for complying with laws, regulations (including *TFM Chapter 4700*), contracts, and grant agreements applicable to SBA. As part of obtaining reasonable assurance about whether SBA's fiscal year 2008 special-purpose financial statements are free of 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 or on compliance with *TFM Chapter 4700* requirements was not an objective of our fiscal year 2008 audit of the special-purpose financial statements, and accordingly, we do not express such an opinion.

The results of our tests of compliance with *TFM Chapter 4700* disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 07-04.

This report is intended solely for the information and use of SBA's management, SBA's Office of Inspector General, U.S. Department of the Treasury, OMB, and GAO, in connection with the preparation and audit of the *Financial Report of the U.S. Government*, and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

November 14, 2008

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

U.S. Small Business Administration

Significant Deficiency

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.

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.

U.S. Small Business Administration

Significant Deficiency

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.

U.S. Small Business Administration

Significant Deficiency

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.



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 Office [EAL] *[Handwritten initials]*
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.