

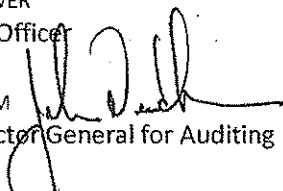


U.S. SMALL BUSINESS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL
WASHINGTON, D.C. 20416

TRANSMITTAL MEMORANDUM
Report No. 12-02

DATE: NOVEMBER 14, 2011

TO: JONATHAN I. CARVER
Chief Financial Officer

FROM: JOHN K. NEEDHAM 
Assistant Inspector General for Auditing

SUBJECT: *Independent Auditors' Report* on the SBA's FY 2011 Financial Statements

We contracted with the independent public accounting firm, KPMG LLP, to audit the U.S. Small Business Administration's consolidated financial statements as of September 30, 2011, 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. 07-04, *Audit Requirements for Federal Financial Statements*, as amended; 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 LLP'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. KPMG LLP issued an unqualified opinion on SBA's fiscal year 2011 consolidated financial statements. In summary, KPMG LLP found 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.

The report also includes one other matter related to possible violations of the Federal Acquisition Regulation's documentation retention requirements. Details regarding the auditor's conclusions are included in the Compliance and Other Matters Section 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 LLP'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 LLP'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 LLP did not comply, in all material respects, with *Generally Accepted Government Auditing Standards*.

We provided a draft of KPMG LLP'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 IV to this report.

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

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, 2011 and 2010, 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) 2011 audit, we also considered the SBA's internal control over financial reporting and tested the 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 the SBA's consolidated financial statements as of and for the years ended September 30, 2011 and 2010, 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 significant deficiencies, as defined in the Internal Control Over Financial Reporting Section of this report, as follows:

Improvement Needed in Information Technology 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 and one other matter 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.

Noncompliance with the Debt Collection Improvement Act of 1996

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

Opinion on the Financial Statements

We have audited the accompanying consolidated balance sheets of the SBA as of September 30, 2011 and 2010, 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.



U.S. Small Business Administration
November 14, 2011
Page 2 of 4

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of the SBA as of September 30, 2011 and 2010, 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.

The information in the Other Accompanying Information section is presented for purposes of additional analysis and is not required as part of the consolidated financial statements. This information has not been subjected to auditing procedures 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 2011 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 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 significant deficiency.

We noted certain additional matters that we have reported to management of the SBA in a separate letter dated November 14, 2011.

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 and one other matter that are required to be reported herein under *Government Auditing Standards* or OMB Bulletin No. 07-04, and are described below.

Debt Collection Improvement Act of 1996 (DCIA). During our testwork over loan charge-offs, we noted the SBA did not refer obligors to the U.S. Department of Treasury (Treasury) for offset or cross-servicing, in accordance with DCIA. Specifically, we noted the SBA did not refer obligors (eligible principal borrowers, co-borrowers, and/or guarantors) associated with 504 delinquent Disaster Assistance loans to the Treasury for offset or cross-servicing at time of charge-off. We also noted in the 7(a), 504, and Disaster programs more than 5,000 eligible co-borrowers and guarantors were not referred for offset or cross-



servicing, in conjunction with the principal borrower at time of loan charge-off. In both conditions, the obligors were not referred to the Treasury for collection during the period under review due to systemic problems with the legacy mainframe system utilized by the SBA to facilitate the referral process. Specifically, certain outdated system edits in the SBA's referral protocol prevented certain loans in charged-off status from being transferred to the Treasury for collection. Also, programmers in the Office of the Chief Information Officer modified the system code (referral protocol) but did not test the program changes during the development phase prior to implementing the changes in production. We noted during the fourth quarter of FY 2011 that the Office of the Chief Information Officer was in the process of implementing actions to address these deficiencies which led to the noncompliance with the DCIA. Exhibit III presents the status of the prior year noncompliance finding, which was also related to DCIA.

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 and one other matter that is required to be reported herein under *Government Auditing Standards* or OMB Bulletin No. 07-04.

A matter has been identified that may be a violation of the Federal Acquisition Regulation documentation retention requirements. This matter is currently under review by SBA management and the Office of Inspector General. The outcome of this matter is not presently known.

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.

* * * * *

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 the SBA.

Auditors' Responsibilities. Our responsibility is to express an opinion on the FY 2011 and 2010 consolidated financial statements of the 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 the 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; and
- Evaluating the overall consolidated financial statement presentation.

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



U.S. Small Business Administration
November 14, 2011
Page 4 of 4

In planning and performing our FY 2011 audit, we considered the 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, but not for the purpose of expressing an opinion on the effectiveness of the 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. 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 the SBA's FY 2011 consolidated financial statements are free of material misstatement, we performed tests of the 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 the 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 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, 2011

U.S. Small Business Administration**Significant Deficiency**

The significant deficiency identified for the year ended September 30, 2011, is summarized below:

Improvement Needed in Information Technology Security Controls

During the Fiscal Year (FY) 2010 financial statement audit, we identified 20 information technology (IT) control findings and recommended many corresponding corrective actions. During the FY 2011 financial statement audit, we found that the U.S. Small Business Administration (SBA) implemented corrective actions to substantially remediate 10 of the 20 findings; however, we also identified 8 new IT control findings. Therefore, SBA's IT control environment continues to require improvement. The FY 2011 IT control deficiencies fall within the control areas of security access, including configuration and patch management, segregation of duties, and contingency planning. We are not providing details in this report on the specific deficiencies due to sensitivity considerations, but we have provided the details in a separate report to SBA management. Exhibit II of our report discloses the status of prior year IT findings.

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 control deficiencies we identified during the FY 2011 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 and one financial system.
- SBA was unable to provide evidence that security incidents are analyzed, validated, and resolved.
- Physical access control procedures can be improved for a financial system hosted by an SBA service provider. In addition, access to the service provider data center can be improved.
- Several users have unnecessary access to one SBA financial subsystem.
- User accounts are not reviewed in accordance with SBA policy for five of the seven systems we reviewed.
- There are weak controls over the monitoring and review of audit logs for two of the seven systems we reviewed.

Recommendation – Security Access Controls:

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

1. Enhance security vulnerability management processes. Specifically, SBA should: (a) redistribute procedures and train employees on the process for reviewing and mitigating security vulnerabilities, (b) periodically monitor the existence of unnecessary services and protocols running on their servers and network devices, (c) perform vulnerability assessments with administrative credentials and penetration tests on all SBA offices from a centrally managed location with a standardized reporting

U.S. Small Business Administration

Significant Deficiency

mechanism that allows for trending, on a regularly scheduled basis in accordance with National Institute of Standards and Technology (NIST) guidance, (d) develop a more thorough approach to track and mitigate configuration management vulnerabilities identified during monthly scans, and (e) monitor security vulnerability reports for necessary or required configuration changes to their environment.

2. Update the vulnerability assessment team (VAT) procedures, to include: (a) updating the VAT policies and procedures in accordance with NIST, (b) performing technical reviews of the results for critical issues that need immediate action and take timely corrective action, (c) executing procedures to monitor the completion of the patch management deployment across the SBA enterprise, and (d) prioritizing vulnerabilities as part of the ongoing continuous monitoring process.
3. Prevent users from anonymously connecting unauthorized devices by developing and implementing procedures to ensure mandatory domain authentication for Internet Protocol (IP) address issuance.
4. Ensure users' access rights are authorized prior to gaining access to financial systems.
5. Fully implement the SBA entity wide incident management and response program and ensure that procedures are enforced.
6. Ensure that information systems hosted by third parties comply with SBA policy and NIST guidance.
7. Develop and implement procedures for user access reviews to ensure that proper access rights are set for financial subsystems.
8. Oversee the review and validation of financial system accounts on a quarterly basis.
9. 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 2011 SBA financial statement audit follows:

- An authorized user had conflicting access rights in a key financial system.
- Six users were authorized with rights as a database administrator (DBA) and system administrator to a financial application hosted by a SBA service provider.

Recommendations – Segregation of Duties:

We recommend the CIO coordinate with the Chief Financial Officer (CFO) to:

10. Restrict access to software program libraries based on the principle of least privilege, and implement compensating controls over actions where limited resources cause individuals to perform conflicting job functions.

U.S. Small Business Administration

Significant Deficiency

11. Ensure that DBA and system administrator access is restricted through role-based segregation of duties and managed through an effective audit log review process.

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. During the FY 2011 SBA financial statement audit, we found that a mandatory training program for IT security personnel has not been implemented.

Recommendations – Security Management:

We recommend the CIO:

12. Develop a comprehensive security education and training program for all IT security personnel and a method for monitoring the training program.

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 deficiencies we identified during the FY 2011 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 one financial system.
- For one financial subsystem, loan charge-off software changes were not tested before being moved to production, which impacted the SBA's compliance with the Debt Collection Improvement Act of 1996 (DCIA). Note that these issues were reported as a noncompliance with the DCIA in the Compliance and Other Matters section of our audit report.

Recommendations – Software Configuration Management:

We recommend the CIO:

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

We recommend the CIO coordinate with the CFO to:

U.S. Small Business Administration

Significant Deficiency

14. Implement configuration management policies and procedures for document retention to include supporting evidence to validate the authorization of operating system changes.

Contingency Planning

The focus of an organization's contingency planning program should 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.

A summary of the contingency planning weaknesses we identified during the FY 2011 SBA financial statement audit follows:

- Backup tapes necessary to restore system operations are not consistently rotated off-site for four of the seven systems we reviewed.
- Comprehensive contingency and disaster recovery plans have not been developed, authorized, nor tested for three of the seven systems reviewed. Additionally, we noted that two financial systems and the Headquarters (HQ) Continuity of Operations Plan (COOP) were in place; however, the plans were not tested on a semiannual basis as prescribed by SBA policy.

Recommendations – Contingency Planning:

We recommend the CIO:

15. Enforce existing SBA policies to rotate backups off-site.

We recommend the CIO coordinate with the CFO to:

16. Create, implement, and test system specific and the HQ COOP.

Exhibit II

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

Fiscal Year 2010 Finding	Fiscal Year 2011 Status of Finding
Improvement Needed in Information Technology (IT) Security Controls	During our review of SBA's IT general and application controls, we noted some improvements made to address prior year findings. However, control deficiencies continue to exist. Therefore, in Fiscal Year (FY) 2011, the issue is again presented in Exhibit I. 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 the associated impact on the consolidated financial statements.

U.S. Small Business Administration

Status of Prior Year Noncompliance

Fiscal Year 2010 Finding	Fiscal Year 2011 Status of Finding
<i>Debt Collection Improvement Act of 1996 (DCIA)</i> During our Fiscal Year (FY) 2010 audit, we noted the agency was noncompliant with the DCIA. The noncompliance was due to instances where SBA did not refer a substantial number of charged-off disaster loans to Treasury for cross-servicing.	During our review over SBA's compliance with the DCIA, we noted improvements made in SBA's Treasury cross-servicing referral process. However, during FY 2011, we noted instances of noncompliance related to timely referrals of loan charge-offs to Treasury for offset and cross-servicing. Therefore, in FY 2011, the issue is again presented in the Compliance and Other Matters section of our Independent Auditors' Report.

CFO Response to Draft Audit Report on FY 2011 Financial Statements

DATE: November 14, 2011
TO: John Needham, Assistant IG for Auditing
FROM: Jonathan Carver, Chief Financial Officer
SUBJECT: Draft Audit Report on FY 2011 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 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 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 in past 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 auditor noted in its report on the 2011 financial statements, the SBA implemented corrective action this year to substantially remediate 10 of the 20 prior year IT control findings. The auditor, however, identified 8 new IT findings this year. The SBA will continue to improve the Agency's IT security during the upcoming fiscal year. The SBA will continue to track, monitor, and aggressively mitigate vulnerabilities in all Agency systems. Furthermore, the SBA will continue its work to 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 SBA is not compliant with the Debt Collection Improvement Act of 1996 in the non referral of delinquent and 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 Disaster loans and eligible Business loan co-borrowers and guarantors that were not referred to Treasury. Research by SBA identified the systemic issues that caused this finding and they were rectified this year. In addition, the SBA is currently migrating its Treasury referral system to a new platform in FY 2012.

During the audit, the auditor identified a potential non compliance with Federal Acquisition Regulation requirements for document retention. The SBA had previously recognized the need for improvement to its acquisition process and has taken action to reorganize and improve its processes concerning the acquisition of goods and services. Furthermore, procurement actions during the current year have been conducted in accordance with FAR requirements including file documentation, and the SBA is now working to review and fully document prior year procurement files.

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.