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

TRANSMITTAL MEMORANDUM
Report No. 13-04

DATE: November 14, 2012

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 2012 Financial Statements

We contracted with the independent public accounting firm, KPMG LLP (KPMG), to audit the U.S. Small Business Administration's consolidated financial statements as of September 30, 2012, 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's audits are presented in the attached report. The report includes an opinion on SBA's financial statements, internal control over financial reporting, and compliance and other matters that have a direct and material effect on the financial statements. The independent auditor issued an unqualified opinion on SBA's fiscal year 2012 consolidated financial statements. In summary, KPMG reported that:

- The financial statements were fairly presented, in all material aspects, in conformity with U.S. generally accepted accounting principles.
- There were no material weaknesses in internal control.
- There is a significant deficiency related to SBA's information technology security controls, which is a repeat condition.
- There is one instance of noncompliance with laws and regulations related to the Debt Collection Improvement Act of 1996, which is also a repeat condition.

The report also includes one other matter related to possible violations of the Federal Acquisition Regulation's documentation retention requirements. Details regarding KPMG' 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's report and related documentation, and made necessary inquiries of their respective representatives. Our review was not intended to enable us to express, and we do not express, an opinion on the SBA's financial statements, KPMG's conclusions about the effectiveness of internal control, or its conclusions about SBA's compliance with laws and regulations. However, our review disclosed no instances where KPMG did not comply, in all material respects, with *Generally Accepted Government Auditing Standards.*

We provided a draft of KPMG's report to SBA's Chief Financial Officer who concurred with its findings and recommendations, and agreed to implement the recommendations. The Chief Financial Officer's comments are attached as Exhibit IV to this report.

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

Attachment

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

Independent Auditors' Report

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, 2012 and 2011, 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 2012 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, 2012 and 2011, are presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles.

As discussed in our opinion on the consolidated financial statements, the SBA changed its presentation for reporting the statement of budgetary resources in fiscal year 2012.

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

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, relating to the *Debt Collection Improvement Act of 1996*, 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.

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 Consolidated Financial Statements

We have audited the accompanying consolidated balance sheets of the SBA as of September 30, 2012 and 2011, 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 the SBA as of September 30, 2012 and 2011, 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 15 to the consolidated financial statements, the SBA changed its presentation for reporting the combined statement of budgetary resources in fiscal year 2012, based on new reporting requirements under OMB Circular No. A-136, *Financial Reporting Requirements*. As a result, the SBA's combined statement of budgetary resources for fiscal year 2011 has been adjusted to conform to the current year presentation.

U.S. generally accepted accounting principles require that the information in the Management's Discussion and Analysis, Required Supplementary Information, and Required Supplementary Stewardship Information sections be presented to supplement the basic financial statements. Such information, although not a part of the basic financial statements, is required by the Federal Accounting Standards Advisory Board who considers it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America, which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic financial statements, and other knowledge we obtained during our audits of the basic financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Our audits were conducted for the purpose of forming an opinion on the basic financial statements as a whole. The information in the Other Information section is presented for the purposes of additional analysis and is not a required part of the basic financial statements. Such information has not been subjected to the auditing procedures applied in the audits of the basic financial statements, and accordingly, we do not express an opinion or provide any assurance 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

fiscal year 2012 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 certain deficiencies in internal control over financial reporting described in Exhibit I, related to information technology security controls, 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 significant deficiency, which was also related to information technology security controls.

We noted certain additional matters that we have reported to management of the SBA in a separate letter dated November 14, 2012.

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). The DCIA assigns the U.S. Department of Treasury (Treasury) the responsibility for collecting delinquent debts (cross servicing) Government-wide. The DCIA requires federal agencies to transfer their nontax debt over 180 days delinquent to Treasury. During our testwork over loan charge-offs, we noted the SBA did not refer obligors (eligible principal borrowers, co-borrowers, and/or guarantors) to Treasury for offset or cross-servicing at the time of charge-off, as required by 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.

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.

Other Matter: 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.

* * * * * * *

Responsibilities

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

Auditors' Responsibilities. Our responsibility is to express an opinion on the fiscal year 2012 and 2011 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.

In planning and performing our fiscal year 2012 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 fiscal year 2012 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.

The SBA's written response to the findings identified in our audit and presented in Exhibit IV was not subjected to the auditing procedures applied in the audit of the SBA's consolidated financial statements and, accordingly, we express no opinion on it.

This report is intended solely for the information and use of the SBA's management, the 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, 2012

Exhibit I

U.S. Small Business Administration

Significant Deficiency

The significant deficiency identified in our Fiscal Year (FY) 2012 audit, is summarized below:

Improvement Needed in Information Technology Security Controls

During our prior year, FY 2011, financial statement audit, we identified 18 information technology (IT) control findings, and recommended many corresponding corrective actions. During the FY 2012 financial statement audit, we found that the U.S. Small Business Administration (SBA) implemented corrective actions to remediate 3 of the 18 findings; however, we also identified 9 new IT control findings. Therefore, SBA's IT control environment continues to require improvement.

The IT control deficiencies that we noted during the FY 2012 audit are summarized below and fall under the following general IT control objectives: security access controls, segregation of duties, security management, software configuration management, and contingency planning. We did not provide details on the specific IT control deficiencies in this report due to sensitivity considerations surrounding the information systems. 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 the effectiveness of 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. Our audit found the following control deficiencies:

- Several high- and medium-risk security vulnerabilities affecting various financial systems.
- A weakness in network access controls.
- The SBA was unable to provide evidence that security incidents are analyzed, validated, and resolved.
- Physical access control procedures can be improved for all financial systems managed at SBA Headquarters (HQ) and one financial system hosted by an SBA service provider. In addition, access to the data centers can be improved.
- Several users had unnecessary access to an SBA financial subsystem.
- User accounts were not reviewed in accordance with SBA policy for five of the seven systems we reviewed.
- Complex and unique password configurations were not implemented and/or enforced.
- User accounts were not disabled or removed promptly upon personnel termination.
- Financial system user accounts and remote access authorizations were not properly authorized.
- Weak controls over the monitoring and review of audit logs for four of the seven systems we reviewed.

Recommendations – Security Access Controls:

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

1. Enhance security vulnerability management processes. Specifically, (a) ensure that servers, operating systems, and databases are properly configured and updated on a routine basis; (b) monitor SBA vulnerability reports for required patches; (c) update systems based on risk determination and threats.
2. Develop and implement procedures to ensure mandatory domain authentication for Internet Protocol (IP) address issuance.
3. Fully implement the SBA entity-wide incident management and response program and ensure that procedures are enforced.
4. Ensure that information systems hosted by the SBA and third parties comply with SBA policy and National Institute of Standards and Technology guidance.
5. Develop and implement procedures for user access reviews to ensure that proper access rights are set for financial subsystems.
6. Ensure that all new system users are assigned random passwords and are subsequently required to change their password upon first log-in.
7. Develop and implement procedures for user access termination to ensure that access for terminated or transferred personnel is removed from systems in a timely manner.
8. Develop and enforce procedures for user access approvals, including remote access, and retain the evidence of the approvals.
9. Oversee the review and validation of financial system accounts on a quarterly basis.
10. 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. Our audit found the following control deficiencies:

- An authorized user had conflicting access rights in a key financial system.
- Twenty-eight service accounts were not properly restricted with unique log-ins and passwords.
- Users were authorized with conflicting rights as a database administrator (DBA) and system administrator to a financial application hosted by an SBA service provider.

Recommendations – Segregation of Duties:

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

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

12. 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. Our audit found the following control deficiency:

- The CIO had not fully implemented a mandatory training program for IT security personnel.

Recommendations – Security Management:

We recommend the CIO:

13. Updates the position descriptions for IT security personnel to include minimum annual training requirements.

14. Develops and fully implement a comprehensive security education and training program for all IT security personnel, to include 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. Our audit noted the following control deficiencies:

- The configuration management process is not centralized, and the Enterprise Change Control Board governance processes were not fully implemented across SBA.
- SBA personnel did not provide sufficient evidence to support software change authorizations for one financial system.
- Software changes for one financial subsystem were not tested before being moved to production, which impacted the SBA's compliance with the Debt Collection Improvement Act of 1996 (DCIA). This issue was reported as a noncompliance matter in the Compliance and Other Matters section of our audit report.

Recommendations – Software Configuration Management:

We recommend the CIO:

15. Enforces 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 coordinates with the CFO to:

16. 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. Our audit noted the following control deficiencies:

- Backup tapes necessary to restore system operations were not consistently rotated off-site for four of the seven systems we reviewed.
- Comprehensive contingency plans had not been developed and authorized for one key financial system. In addition, another system's plan was not updated to reflect the current environment.
- Five of the seven contingency plans, which includes the HQ Continuity of Operations Plan (COOP), were documented and approved but were not tested semiannually as prescribed by SBA policy. Two of the plans, which were first authorized in May 2011, had never been tested.
- One key financial system lacked adequate recovery capabilities commensurate with the system's Federal Information Processing Standards Publication 199 categorization.

Recommendations – Contingency Planning:

We recommend the CIO:

17. Enforces existing SBA policies to rotate backups off-site.

18. Conducts a Business Impact Analysis, develop and implement the contingency plans, and establish an alternate processing site.

We recommend the CIO coordinate with the CFO to:

19. Test system-specific plans and the HQ COOP on a frequency consistent with SBA policy.

Exhibit II

U.S. Small Business Administration

Status of Prior Year Significant Deficiency

Fiscal Year 2011 Finding	**Fiscal Year 2012 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 2012, 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.

Exhibit III

U.S. Small Business Administration

Status of Prior Year Noncompliance

Fiscal Year 2011 Finding	**Fiscal Year 2012 Status of Finding**
Debt Collection Improvement Act of 1996 (DCIA) During our Fiscal Year (FY) 2011 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 loans to the 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 2012, we noted instances of noncompliance related to timely referrals of loan charge-offs to Treasury for offset and cross-servicing. We also noted that the approximately 5,000 eligible obligors identified in FY 2011 have not been properly referred to the Treasury as of FY 2012.Therefore, in FY2012, the issue is again presented in the Compliance and Other Matters section of our Independent Auditors' Report. We recommend the Associate Administrator for Capital Access[1]: 20. Conducts training to educate loan center staff on the proper steps to refer obligors to the Treasury through the system and how to correct errors after loans have been referred to Treasury. 21. Considers implementing a process to monitor loans that reach 150 days delinquent to ensure, that at 180 days, the loans are properly referred to the Treasury. 22. Continues to work with the Treasury to refer the more than 5,000 co-borrowers and guarantors that were not referred in FY 2011. 23. Continues to review system protocol to identity any other coding problems which may cause untimely referral of loans. 24. Implements quarterly monitoring reviews to identify all charged-off loans where the automatic referral did not occur.

[1] The recommendations listed in this exhibit were sequenced after the recommendations presented on Exhibit I, *IT Significant Deficiency*, to assist users of this report tracking the number of recommendations presented.

Exhibit IV

CFO Response to Draft Audit Report on FY 2012 Financial Statements

DATE: November 14, 2012

TO: John Needham, Assistant IG for Auditing

FROM: Jonathan Carver, Chief Financial Officer

SUBJECT: Draft Audit Report on FY 2012 Financial Statements

The Small Business Administration has received the draft Independent Auditors' Report from KPMG that includes the auditor's opinion on the financial statements and its review of the Agency's internal control over financial reporting and compliance with laws and regulations. The independent audit of the Agency's financial statements and related processes is a core component of SBA's financial management program.

We are pleased that the SBA has again received an unqualified audit opinion from the independent auditor with no material weaknesses. We believe these results accurately reflect the quality of the Agency's financial statements and our improved accounting, budgeting and reporting processes. As you know, the SBA has worked hard in past years to address the findings from our independent auditor. Our core financial reporting data and processes have further improved, and we are proud that the results of our efforts have been confirmed by the independent auditor.

The audit report includes a continuing significant deficiency in SBA's information technology controls. As the auditor noted in the report on the FY 2012 financial statements, the SBA implemented corrective action this year to remediate 3 of the 18 prior year IT control findings. The auditor, however, identified 9 new IT findings this year and re-issued one NFR related to it. The SBA will continue to work on improvements in IT security. The SBA will track, monitor, and aggressively mitigate vulnerabilities in all Agency systems. Furthermore, the SBA will clarify and strengthen detailed procedures required to ensure security access controls are in place to protect SBA data from unauthorized modification, disclosure, and loss.

The auditor reported again this year that the SBA is not compliant with the Debt Collection Improvement Act of 1996 related to timely referral of charged-off loans to the Department of the Treasury for its tax refund offset and collection programs. Although the SBA made improvements to correct systemic errors identified last year, the auditor again found instances of charged-off loans where co-borrowers and guarantors were not referred to Treasury. The SBA is working on procedures to correct this issue.

The audit report includes one other matter that may be a violation of the Federal Acquisition Regulation documentation retention requirements. This is the second year since the SBA transferred the procurement functions to the Office of the Chief Financial Officer. The FY 2012 review of internal controls over financial reporting revealed that, while there was considerable improvement in the contracting area, more time and resources will be required to resolve all outstanding issues. These include formalizing the acquisition process and related requirements through Agency-wide Standard Operating Procedures, ensuring all contracting documents are signed by appropriate authorized individuals, and ensuring that invoices are reviewed by appropriate parties before payment is disbursed. The Agency takes this matter very seriously and we have already taken steps to make further improvements.

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.