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

Final Report Transmittal
Report Number: 20-04

DATE: November 15, 2019

TO: Christopher M. Pilkerton
Acting Administrator and General Counsel

FROM: Hannibal "Mike" Ware
Inspector General

SUBJECT: Independent Auditors' Report on SBA's FY 2019 Financial Statements

We contracted with the independent certified public accounting firm KPMG LLP (KPMG) to audit the U.S. Small Business Administration's (SBA's) consolidated financial statements as of and for the fiscal year ended September 30, 2019. This audit is an annual requirement of the Chief Financial Officers Act of 1990, as amended, and was conducted in accordance with generally accepted government auditing standards; the Office of Management and Budget Bulletin No. 19-03, Audit Requirements for Federal Financial Statements; and the U.S. Government Accountability Office's Financial Audit Manual and Federal Information System Controls Audit Manual.

The attached independent auditors' report presents an unmodified opinion on SBA's consolidated financial statements for fiscal year 2019. Specifically, KPMG reported that

- the financial statements were fairly presented, in all material respects, in accordance with U.S. generally accepted accounting principles;
- there were no instances in which SBA's financial management systems did not substantially comply with the Federal Financial Management Improvement Act of 1996 (FFMIA);
- there is one material weakness related to internal control over financial reporting where improvement is needed in SBA's risk assessment processes;
- there is a significant deficiency related to disaster loan processing controls; and
- there is also a significant deficiency related to SBA's information technology security controls, which has been identified in the past.

Details regarding KPMG's conclusions are included in attachments I and II to this report. Within 30 days of this report, KPMG expects to issue a separate letter to SBA management regarding other, less significant matters that came to its attention during the audit.

In connection with the contract, we reviewed KPMG's report and related documentation and inquired of its representatives. Our review, as differentiated from an audit of the financial statements in accordance with U.S. generally accepted government auditing standards, was not intended to enable us to express—and we do not express—opinions on SBA's financial statements or internal control over financial reporting or conclusions on whether SBA's financial management systems substantially complied with the three FFMIA requirements, or on compliance with laws and other matters.

KPMG is responsible for the attached auditors' report dated November 15, 2019, and the conclusions expressed therein. However, our review disclosed no instances where KPMG did not comply, in all material respects, with U.S. generally accepted government auditing standards.

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

We appreciate the cooperation and assistance of SBA and KPMG during the audit. Should you or your staff have any questions, please contact me or Andrea Deadwyler, Assistant Inspector General for Audits, at (202) 205-6586.

cc: Dorrice Roth, Acting Financial Officer and Associate Administrator for Performance Management
Maria Roat, Chief Information Officer
James Rivera, Associate Administrator, Disaster Assistance
Martin Conrey, Attorney Advisor, Legislation and Appropriations
Kyong Chae, Acting Director, Office of Internal Controls
Michael Simmons, Attorney Advisor

Attachment

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

Independent Auditors' Report

Inspector General
U.S. Small Business Administration

Acting Administrator
U.S. Small Business Administration

Report on the Financial Statements

We have audited the accompanying consolidated financial statements of the United States (U.S.) Small Business Administration (SBA), which comprise the consolidated balance sheets as of September 30, 2019 and 2018, and the related consolidated statements of net cost, and changes in net position, and combined statements of budgetary resources for the years then ended, and the related notes to the consolidated financial statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these consolidated financial statements in accordance with U.S. generally accepted accounting principles; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of consolidated financial statements that are free from material misstatement, whether due to fraud or error.

Auditors' Responsibility

Our responsibility is to express an opinion on these consolidated financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America, in accordance with the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and in accordance with Office of Management and Budget (OMB) Bulletin No. 19-03, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin No. 19-03 require that we plan and perform the audit to obtain reasonable assurance about whether the consolidated financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the consolidated financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the consolidated financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the consolidated financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the consolidated financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of the U.S. Small Business Administration as of September 30, 2019 and 2018, and its net costs, changes in net position, and budgetary resources for the years then ended in accordance with U.S. generally accepted accounting principles.

Other Matters

Interactive Data

Management has elected to reference to information on websites or other forms of interactive data outside the U.S. Small Business Administration's FY 2019 Agency Financial Report to provide additional information for the users of its financial statements. Such information is not a required part of the basic consolidated financial statements or supplementary information required by the Federal Accounting Standards Advisory Board. The information on these websites or the other interactive data has not been subjected to any of our auditing procedures, and accordingly we do not express an opinion or provide any assurance on it.

Required Supplementary Information

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 consolidated financial statements. Such information, although not a part of the basic consolidated 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 consolidated 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 consolidated financial statements, and other knowledge we obtained during our audits of the basic consolidated 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.

Other Information

Our audits were conducted for the purpose of forming an opinion on the basic consolidated financial statements as a whole. The Message from the Acting Administrator, Management's Discussion & Analysis, Other Information, Message from the Acting Chief Financial Officer, and the Appendices in the U.S. Small Business Administration's FY 2019 Agency Financial Report are presented for purposes of additional analysis and are not a required part of the basic consolidated financial statements. Such information has not been subjected to the auditing procedures applied in the audits of the basic consolidated financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

Other Reporting Required by *Government Auditing Standards*

Internal Control over Financial Reporting

In planning and performing our audit of the consolidated financial statements as of and for the fiscal year ended September 30, 2019, we considered SBA's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the consolidated financial statements, but not for the purpose of expressing an opinion on the effectiveness of SBA's internal control. Accordingly, we do not express an opinion on the effectiveness of SBA's internal control. We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982*.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that have not been identified. However, as described in the accompanying Attachments I and II we did identify certain deficiencies in internal control that we consider to be a material weakness and significant deficiencies.

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. We consider the deficiencies described in Attachment I to be a material weakness.

SBA management did not report the material weakness related to the risk assessment process for internal controls over financial reporting in its Management Assurances: FMFIA and FFMIA Assurance Statement for FY 2019, included in the Management's Discussion and Analysis section of the accompanying FY 2019 Agency Financial Report.

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. We consider the deficiencies described in Attachment II to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the SBA's consolidated financial statements as of and for the fiscal year ended September 30, 2019 are free from 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 was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 19-03.

We also performed tests of its compliance with certain provisions referred to in Section 803(a) of the *Federal Financial Management Improvement Act of 1996* (FFMIA). Providing an opinion on compliance with FFMIA was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests 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 U. S. Government Standard General Ledger at the transaction level.

SBA's Responses to Findings

SBA's responses to the findings identified in our audit are described in Attachment III. SBA's responses were not subjected to the auditing procedures applied in the audit of the consolidated financial statements and, accordingly, we express no opinion on the responses.

Our response to SBA's response is included in Attachment IV.

Purpose of the Other Reporting Required by Government Auditing Standards

The purpose of the communication described in the Other Reporting Required by *Government Auditing Standards* section is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of SBA's internal control or compliance. Accordingly, this communication is not suitable for any other purpose.

KPMG LLP

Washington, DC
November 15, 2019

U.S. Small Business Administration

Material Weakness

Risk Assessment

During fiscal year (FY) 2019, we noted that management did not perform an adequate risk assessment to identify, assess, and address relevant risks that could prevent the fair presentation of the consolidated financial statements to be free from material misstatement and be in accordance with U.S. generally accepted accounting principles. We further noted several internal control matters that highlighted the need for SBA management to improve their risk assessment process, particularly in relation to the evaluation of service organization controls and preparation of the financial statement disclosure related to the budget and accrual reconciliation. These matters are considered to be a material weakness in internal control.

Improvements Needed in the Agency's Risk Assessment Process

In FY 2019, SBA represented that a risk assessment related to internal controls was performed prior to initiating their annual testing in accordance with the Office and Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. However, the risk assessment was performed through informal management discussions and was not documented. As such, SBA was not able to demonstrate that a comprehensive risk identification and assessment process was performed to provide reasonable assurance that all significant reporting risks were identified, tested, or appropriately addressed. In addition, SBA did not calculate a materiality threshold to use in determining the sufficient level of internal control activities needed to manage risk related to reporting objectives.

The conditions noted were primarily caused by two main factors. First, we were informed that the FY 2019 risk assessment process was not formally documented due to an anticipated update to integrate the FY 2020 risk assessment procedures with the enterprise risk management processes. Second, based on interpretation of the updated Appendix A to OMB Circular No. A-123, *Management of Reporting and Data Integrity Risk*, management did not believe a materiality threshold was required.

Without performing a comprehensive risk identification and assessment process, management did not have reasonable assurance that all significant reporting risks were identified, tested, and appropriately addressed. In addition, by not implementing the guidance in OMB Circular No. A-123 and the updated Appendix A, SBA increases the risk of potential noncompliance with the *Federal Managers' Financial Integrity Act* (FMFIA).

The following criteria were considered with respect to the matter described in the preceding paragraphs:

- The Government Accountability Office's (GAO's) *Standards for Internal Control in the Federal Government* ("Green Book"), Principle 7, *Identify, Analyze, and Respond to Risks*; Principle 8, *Assess Fraud Risk*; and Principle 9, *Identify, Analyze, and Respond to Change*
- OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*
- Section 3512 (c) and (d) of Title 31 of the United States Code (commonly known as FMFIA)

FMFIA provides the statutory basis for management's responsibility for, and assessment of, internal controls. OMB Circular No. A-123 provides a methodology for agency management to assess, document, and report on internal controls over reporting and is guidance to help implement the requirements of FMFIA. The Circular

contains specific guidance requiring agencies to annually identify and assess risk as part of the agency's risk profile. As part of this process, management should determine materiality thresholds to ensure the level of internal control activities needed to provide reasonable assurance for reporting objectives. Management should also determine the risks for which the application of formal internal control activities is the appropriate response.

Recommendations:

We recommend that the Acting Administrator direct the Acting Chief Financial Officer to:

1. Integrate the Office of Chief Financial Officer (OCFO)'s risk identification and assessment process with its enterprise risk management processes.

2. Ensure management personnel document their interpretation with respect to applicability of requirements (e.g., such as the need to determine a materiality threshold in the risk assessment process).

3. Formally document a comprehensive risk assessment process every year, including the determination of materiality thresholds, as applicable under the requirements.

Improvements Needed in the Evaluation of Service Organization Controls

Deficiencies in the risk assessment process, as noted above, could limit management's ability to identify, analyze, and respond to significant changes impacting operations, systems and financial reporting. Specifically, during FY 2019, SBA migrated a system to the cloud using an external cloud service provider. In addition, during the prior year, SBA implemented a new loan origination system which utilizes a different external service provider. Both systems are significant IT environments for SBA's financial reporting. As part of its risk assessment process, SBA could not demonstrate the process used to adequately identify and assess the risks related to financial reporting for these changes to the relevant IT environments affected by the use of service organizations.

The process that SBA followed with respect to assessing the operations at the service organizations, in this instance, was limited to obtaining assurance for the design, implementation, and operation of relevant controls at the service organizations by obtaining a Service Organization Control (SOC) 1 Type 2 report. However, we noted that management's evaluations of the SOC 1 reports were not sufficiently documented or considered in management's assessment of Internal Controls over Financial Reporting (ICOFR) under OMB Circular No. A-123. For example, management's assessment of the SOC 1 Type 2 reports did not:

- Identify instances in which the SOC 1 reports lack sufficient information or did not cover aspects of service organization business processes and controls considered relevant to SBA's ICOFR
- Include consideration of all exceptions noted in the SOC 1 reports, to determine applicability to SBA's ICOFR, the potential impact to SBA's financial statements, and mitigating controls or other considerations made during their risk assessment
- Evaluate SBA's implementation and perform testing over the design and operating effectiveness of the complementary user entity controls (CUECs) identified in the SOC 1 reports
- Evaluate the complementary subservice organization controls (CSOCs) identified with the SOC 1 reports
- Consider an assessment of bridge letters for the period between the report dates and September 30, 2019, to determine whether coverage was provided for the entire year.

In addition, we noted that one of the service organization's SOC 1 report contained a qualification in the opinion related to the design of controls in one of the objectives. SBA did not document the consideration of the qualification and its applicability to SBA's ICOFR, potential impact to SBA's financial statements, and whether there were any mitigating controls.

The deficiencies noted above were caused by the lack of a documented policy/procedure requiring the evaluation of relevant SOC 1 reports for service organizations, in support of SBA's ICOFR evaluation. As a result, SBA's annual assessment of internal controls was incomplete because it did not consider all relevant aspects of the SOC 1 reports during its evaluation of ICOFR. The conditions noted above increase the risk that management fails to make key observations regarding the sufficiency of coverage provided by SOC 1 reports and the results that are relevant to SBA's ICOFR. This in turn could result in a failure to identify and obtain an understanding of relevant service organization controls and weaknesses that increase internal control risks that could affect the integrity of SBA's financial statements. Thus, management's assessment of ICOFR is not complete without the sufficient consideration of the adequacy and effectiveness of controls at relevant service organizations.

The following criteria were considered with respect to the matter described in the preceding paragraphs:

- GAO's Green Book, Section 4, *Additional Considerations: Service Organizations*; Principle 10, *Design Control Activities*; and Principle 16, *Perform Monitoring Activities*

- OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*

The Green Book states that management should identify the risks related to the entity and its objectives, including its service organizations, and design control activities to address the identified risks. In addition, OMB Circular No. A-123 states that for service organizations considered significant to the achievement of internal control objectives for reporting, management needs to consider the services provided by the service organization during its risk assessment process.

Recommendation:

We recommend the Acting Administrator require the Chief Information Officer to work with the relevant program offices to:

4. Develop, document, and implement procedures outlining the SOC 1 report evaluation process for relevant service organizations, to ensure reviews are performed in accordance with OMB and GAO guidance. The reviews should document the following considerations:

- SOC 1 reports are sufficiently scoped to address transaction processing and related control activities performed by service organizations on behalf of SBA (e.g., that services, business applications and other information technology, service organization departments and locations, control objectives and activities, and other aspects of scope that are relevant to SBA's ICOFR are included in the scope of SOC 1 reports).
- All exceptions noted in the SOC 1 reports – not just those described in the independent service auditor's report – are evaluated to determine applicability to SBA's ICOFR, the potential impact to SBA's financial statements, and mitigating controls other considerations made during the risk assessment.
- All CUECs described in the SOC 1 reports are evaluated using current information and with consideration to their applicability to SBA's ICOFR.
- Evaluation procedures include an assessment of whether CUECs and other SBA-performed controls were tested on a frequency determined by SBA, and found effective and, if they are not, the impact of such deficiencies on SBA's ICOFR.
- All CSOCs described in SOC 1 reports are evaluated to determine whether they provided services and performed controls considered relevant to SBA's ICOFR and, if relevant subservice organizations were identified, an evaluation is performed to obtain an understanding of the subservice organization(s) and their controls.
- SOC 1 reports are evaluated to determine whether:
    - The reporting periods and corresponding bridge letters provide sufficient coverage to assess impacts on SBA's ICOFR.

- Any matters require additional follow-up by SBA.

Improvements Needed in the Budget and Accrual Reconciliation (BAR) Disclosure

The deficiencies noted above relating to the risk assessment process prevented management from identifying, analyzing, and responding to risks arising from significant changes in financial reporting requirements in FY 2019, such as the implementation of a new accounting standard. Specifically, we noted deficiencies in controls over the preparation and review of the BAR disclosure.

The Statement of Federal Financial Accounting Standards (SFFAS) 53: *Budget and Accrual Reconciliation: Amending SFFAS 7, and 24, and Rescinding SFFAS 22*, is effective for periods beginning after September 30, 2018. The standard requires a budget and accrual reconciliation between budgetary and financial accounting information to be presented in a footnote that replaces the previous reconciliation of net cost of operations to budget footnote. The BAR explains the relationship between the entity's net outlays on a budgetary basis and the net cost of operations during the reporting period. The BAR will start with the net cost of operations and will be adjusted by components of net cost that are not part of net outlays, components of net outlays that are not part of net cost, and other temporary timing differences, which reflect some special adjustments.

During our initial test work over Note 16, Reconciliation of Net Operating Cost and Net Budgetary Outlays, for the 4th quarter financial statements in SBA's FY 2019 Agency Financial Report (AFR), we identified the following deficiencies:

- Omission of significant balances from the Components of Net Outlays that are Not Part of Net Operating Cost section, including the Effect of the Prior Year Credit Reform Subsidy Reestimates, the Changes in Loans Receivable Before Allowance, the Other Changes in Liability for Loan Guaranties, the Cash Transfer to the Master Reserve Fund, and the Effect of Current Year Downward President's Budget Reestimate Transferred to the General Fund Receipt Account lines;
- Inaccurate balances in the Other Changes in Allowance Before Reestimates and the Other Changes in Liability for Loan Guaranties Before Reestimates lines due to the inclusion of balances that do not belong in the respective category, such as double counting the effect of the current year reestimate and inclusion of components not part of the Net Cost;
- Inaccurate calculation and presentation of the change in Accounts Receivable and Accounts Payable lines;
- Exclusion of the effect of elimination entries between SBA funds;
- Inaccurate captions of section headers and positive and negative signs on balances; and
- Exclusion of the required narrative explaining the purpose, nature, and line items of the reconciliation.

These deficiencies were caused by the lack of a sufficient process to identify and address risks related to the applicability and implementation of new accounting standards and the identification of processes and controls to mitigate such risks. More specifically, there were no specific internal controls over financial reporting to demonstrate how management considered the impact of SBA's transactions and balances in the BAR note, whereby a risk of material misstatement due to error and/or omissions could have been reasonably mitigated. Also, the deficiencies resulted in significant inaccuracies and incomplete presentation of the BAR note until adjusted through our audit. In addition, without performing and documenting a comprehensive analysis of the applicability and implementation of accounting standards, SBA increases the risk of material misstatements or omissions to the consolidated financial statements that would not be in accordance with generally accepted accounting principles.

The following criteria were considered with respect to the matter described in the preceding paragraphs:

- SFFAS 53, Paragraph 2, sub-paragraph 82, and Paragraph 5, including sub-paragraphs 96-100
- GAO's Green Book, Section 1, *Fundamentals Concepts of Internal Control*

- OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*

Recommendations:

We recommend the Acting Administrator require the Acting Chief Financial Officer to:

5. Formally document a comprehensive risk assessment process, including the consideration of the applicability and implementation of new accounting standards.

6. Implement adequate internal controls to prevent or detect and correct material misstatements to the financial statements and footnotes.

Attachment II

U.S. Small Business Administration

Significant Deficiencies

Improvement Needed in Disaster Loan Processing Controls

During the FY 2019 financial statement audit, we identified one disaster loan for which the interest rate per the borrower's modified loan authorization and agreement did not agree to SBA's records within its loan processing and repository system. Specifically, the identified loan was originally obligated at a specified interest rate, then subsequently approved for a lower rate several months later. The modified interest rate was evidenced by a signed loan modification that reduced the interest rate. The loan was then subsequently disbursed; however, there was no documentation supporting the updated interest rate within the system. This ultimately resulted in an overstatement of the loans receivable and interest revenue balances in SBA's financial statements, and the borrower was overcharged.

The deficiency was caused by the Office of Disaster Assistance's (ODA's) lack of a policy/procedure that would require the consistent and timely generation of documentary evidence to support the establishment and modification of loan obligations and related terms in the system. Furthermore, ODA does not have adequate controls to ensure changes to loan terms subsequent to loan obligation are consistently processed within the system. As such, incorrect loan information in the system may lead to under or overcharges to SBA borrowers. As a result of this deficiency, ODA performed an analysis to further determine the impact of this condition on their disaster loan portfolio. ODA determined that 273 other loans had a similar condition as noted above.

The following criteria were considered with respect to the matter described in the preceding paragraph:

- GAO's Green Book, Principle 3, *Establish Structure, Responsibility, and Authority*; and Principle 10, *Design Control Activities*
- OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*

Recommendations:

We recommend the Acting Administrator require the Associate Administrator for ODA to:

7. Develop and enforce a policy/procedure that requires the consistent and timely generation of documentary evidence to support the establishment and modification of loan terms subsequent to loan obligation and ensure it is readily available.

8. Implement adequate controls to ensure changes to loan terms subsequent to loan obligation are consistently and timely processed within the loan processing and repository system.

Improvement Needed in Information Technology Security Controls

During the FY 2019 financial statement audit, we found that SBA continued to implement corrective actions on some of the prior year information technology (IT) findings; however, a number of conditions persisted in FY 2019 that limited SBA's ability to effectively manage its information system risks. Collectively, these conditions increase the risk of unauthorized use, modification, or destruction of financial data, which may impact the integrity of information used to prepare the financial statements. As a result, the conditions continue to present a significant deficiency in SBA's internal control environment.

In an effort to provide additional clarity and emphasis to SBA management with respect to the corrective actions required, we continued to provide prior year recommendations where issues persisted in FY 2019 and issued additional recommendations for the new control deficiencies identified. In the sections below, we distinguish between recurring conditions and related recommendations, and those that were newly identified in FY 2019. We have omitted some technical details from the conditions and recommendations due to the sensitivity of the information. These details were communicated to management in Notices of Findings and Recommendations throughout the audit.

The following criteria were considered with respect to the matter described in the preceding paragraph:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- Federal Information Processing Standards Publication (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*
- SBA Standard Operating Procedure (SOP) 90 47 4, *Information Technology Security Policy*

We have summarized the IT control deficiencies that we noted during the FY 2019 audit below and have organized them by the following general IT control objectives: logical access controls and system configuration management.

Logical Access Controls

An integral part of the effectiveness of an organization's security program management efforts should be to ensure that logical access controls 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 that the following control deficiencies identified in prior years persisted in FY 2019:

- For majority of FY 2019, the employee exit clearance and contractor off-boarding processes were not documented to ensure that access to SBA's systems was removed in a timely manner upon separation.
- Audit logs do not include sufficient detail to identify the security events that were reviewed.

Our audit identified the following new control deficiencies in FY 2019:

- Segregation of duties issues for certain developers that also have access to migrate code exist.
- User access forms were not accurately completed to document the appropriate privileges needed by certain users.

Recommendations – Logical Access Controls:

We have issued the following recommendations to address the repeat and new control deficiencies listed in the section above.

We recommend that the Administrator require the Chief Information Officer (CIO) to:

9. Consider creating an Agency-wide working group to provide effective oversight and solutions to address the entity-wide conditions cited and implement streamlined, efficient and effective user access "best practices" currently used by the private sector and other Federal agencies.
10. Develop and document procedures over the separation process that identify the roles and responsibilities for each office.

11. Create a process to identify separated contractors from their respective program office/Contracting Officer, centrally track and monitor for contractor separations, and communicate contractor separations to stakeholders that are required for the timely removal of logical access.
12. Implement a stricter policy for account suspension after inactivity to account for SBA employees who may not have been removed via the manual account removal process.
13. Continue to enhance and strengthen the audit logging and review controls to specify which events were reviewed, who performed the review, and whether issues were identified, escalated, and resolved.
14. Implement segregation of duties and implement mitigating controls to help ensure that personnel with the ability to the develop code, are restricted from migrating code into the production environment.
15. Train personnel who are responsible for the provisioning of accounts to grant access in compliance with SBA policy and procedures.
16. Evaluate and redesign user access forms to remove any redundant or unnecessary data fields.

System Configuration Management

An integral part of the effectiveness of an organization's security program management efforts should be to ensure that application change management controls provide reasonable assurance that program changes implemented to the applications are appropriate and authorized.

Our audit noted that although improvements have been made, the following new control deficiency exists in FY 2019:

- A patch to an operating system was pushed to the production environment before it was tested.

Recommendation – System Configuration Management:

To address the system configuration management condition above, we recommend that the Acting Administrator require the Associate Administrator for the Office of Capital Access (OCA) to:

17. Periodically train personnel involved with the implementation of operating system patches to follow the requirements of the patch management process in accordance with SBA and OCA policy.

CFO Response to Audit Report on FY 2019 Financial Statements

DATE: November 15, 2019

TO: Hannibal M. Ware, Inspector General

FROM: Dorrice C. Roth, Acting Chief Financial Officer and Administrator for Performance Management

SUBJECT: FY 2019 Financial Statement Audit

The Small Business Administration has reviewed the Independent Auditors' Report from KPMG that includes the auditors' 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 unmodified audit opinion from the independent auditor. We believe these results accurately reflect the quality of the Agency's financial statements and our continued efforts to further improve our budgeting, accounting, and reporting processes.

The auditors identified a material weakness related to the risk assessment process for internal control over financial reporting in the following three areas: evaluation of Service Organization Control (SOC) 1 Reports of two external service organizations, documentation of risk assessments performed for planning of internal control reviews application, and implementation of the new accounting standard for the Budget and Accrual Reconciliation (BAR) footnote.

The SBA does not agree with the assessment on the implementation of the new accounting standard and the subsequent classification of the combined audit findings as a material weakness. The SBA participated in the FASAB task force on the development of the standard. Subsequently, the SBA assisted the U.S. Department of Treasury's working group in the development of the BAR crosswalk requirements in which SBA's financial statement data was utilized. The resulting template was utilized by 24 CFO Act agencies. The SBA also collaborated with other agencies affected by the Federal Credit Reform Act (FCRA) in developing the BAR footnote to ensure consistency across the Federal Government. The SBA reiterates that it has proper internal controls over financial reporting and has been a leader in FCRA accounting within the Federal Government. The SBA will formalize the SOC 1 report review process and will document the internal control risk assessment process.

The auditors identified a significant deficiency related to information technology security controls, and a significant deficiency related to the controls between the Disaster Credit Management System and the electronic loan repository system. The SBA will work to address the significant deficiency related to IT security controls through its Chief Information Officer and the significant deficiency with the Disaster Credit Management System through its Associate Administrator for Disaster Assistance.

We appreciate 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 directly support our efforts to further enhance SBA's financial management practices. We remain committed to excellence in financial management and look forward to making more progress in the coming year.

Auditors' Response to Management's Response

We appreciate SBA management's response to our report, presented in Attachment III, recognize their commitment to accountability and transparency, and acknowledge management's efforts. We note that management does not concur with the classification of the Budget and Accrual Reconciliation (BAR) issue presented in Attachment I as a component of the material weakness.

SBA management initially presented the BAR footnote that was prepared based on their interpretation of the new accounting standard using the BAR crosswalk which was developed by the Treasury Working Group, as referenced in management's response. The crosswalk states at the top: "This crosswalk serves as a guide and is NOT all inclusive. While it presents the most common scenarios, agencies should use their discretionary and professional judgement for agency specific cases when preparing the reconciliation." In addition, there are lines within the crosswalk that state no account mapping is available. These lines are significant for SBA's Credit Reform activity. Furthermore, it is important to recognize that the crosswalk guide is a less authoritative source for generally accepted accounting principles as defined in the SFFAS 34, *The Hierarchy of Generally Accepted Accounting Principles, Including the Application of Standards Issued by the Financial Accounting Standards Board*, than the FASAB standards.

Therefore, we assessed the BAR footnote against the requirements of SFFAS 53, *Budget and Accrual Reconciliation*, and noted material misstatements, as described in Attachment I. The material misstatements were subsequently corrected by SBA management in the accompanying FY 2019 consolidated financial statements. As a result of the material misstatements that we identified during our audit, we assessed the control deficiency as a material weakness, which by definition indicates that there is a reasonable possibility that a material misstatement of the entity's financial statements (which include footnote disclosures) will not be prevented, or detected and corrected, on a timely basis.