DATE: November 15, 2024

TO: Isabella Casillas Guzman
Administrator

FROM: Hannibal "Mike" Ware
Inspector General

SUBJECT: Independent Auditors' Report on SBA's Fiscal Year 2024 Financial Statements (Report 25-05)

I am pleased to present the attached independent auditors' report on the U.S. Small Business Administration's (SBA) financial statements for fiscal year (FY) 2024, as required annually by the Chief Financial Officers Act of 1990, as amended.

We contracted with the independent certified public accounting firm KPMG LLP to conduct an audit of SBA's consolidated balance sheets as of September 30, 2024 and 2023 and the related notes to these statements. Our contract with KPMG required that the audit be performed in accordance with auditing standards generally accepted in the United States of America, *Government Auditing Standards* issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin No. 24-02, Audit Requirements for Federal Financial Statements.

KPMG's responsibility was to express an opinion on the consolidated balance sheets based on their audit. KPMG was not engaged to audit the consolidated statements of net cost and changes in net position and combined statements of budgetary resources for the years that ended September 30, 2024 and 2023 and the related notes to these statements.

In the audit, KPMG reported significant matters for which they were unable to obtain sufficient and appropriate audit evidence to provide a basis for an audit opinion on SBA's balance sheet as of September 30, 2024. Accordingly, KPMG issued a disclaimer of opinion on the consolidated balance sheets as of September 30, 2024 and 2023.

The basis for the disclaimer was that due to inadequate processes and controls, SBA was unable to provide adequate evidential matter in support of a significant number of transactions and account balances related to the Paycheck Protection Program, Economic Injury Disaster Loan program, Restaurant Revitalization Fund, and the Shuttered Venue Operators Grant program.

As a result, KPMG was unable to determine whether any adjustments might have been necessary with respect to the following:

- Credit program receivables and related foreclosed property,
- Other than intragovernmental accounts receivable,
- Downward re-estimate payable to Treasury, and
- Loan Guarantee Liabilities and the related notes.

For the period that ended September 30, 2024, KPMG identified seven material weaknesses and two significant deficiencies in internal control over financial reporting. Appendixes I and II of this report describe details of KPMG's conclusions about the material weaknesses and significant deficiencies. Appendix III describes instances of noncompliance with applicable laws or other matters required to be reported under *Government Auditing Standards* or OMB Bulletin No. 24-02.

We reviewed KPMG's report and related documentation and inquired of its representatives. Our oversight protocols included evaluation of major work products, attendance at critical meetings, review of significant findings, and examination of related evidential matter. Our review, as differentiated from an audit of the financial statements in accordance with 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 SBA's compliance with applicable laws and other matters. Our review disclosed no instances where KPMG did not comply in all material respects with auditing standards. KPMG is responsible for the attached auditors' report dated November 15, 2024 and the conclusions expressed. However, the Office of Inspector General provides negative assurance of this audit.

We provided a draft of the KPMG report to SBA's Chief Financial Officer, who concurred with its findings and recommendations and agreed to implement the recommendations. The Chief Financial Officer stated that SBA has undergone tremendous effort to strengthen internal controls, policies, and procedures and will continue remediation efforts in the coming audit year. The Chief Financial Officer's response is included in Appendix IV.

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: Dilawar Syed, Deputy Administrator, Office of the Administrator
Arthur Plews, Chief of Staff, Office of the Administrator
Isabelle James, Deputy Chief of Staff, Office of the Administrator
Katherine Aaby, Associate Administrator and Chief Financial Officer, Office of Performance, Planning, and the Chief Financial Officer
Kathryn Frost, Associate Administrator, Office of Capital Access
John Miller, Deputy Associate Administrator, Office of Capital Access
Francisco Sanchez Jr., Associate Administrator, Office of Disaster Recovery and Resilience
Therese Meers, General Counsel, Office of General Counsel
Michael Simmons, Attorney Advisor, Office of General Counsel
Cynthia Pitts, Director, Office of Administrative Services
Anna Maria Calcagno, Director, Office of Strategic Management and Enterprise Integrity
Tonia Butler, Director, Office of Internal Controls

Attachment

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

Independent Auditors' Report

Inspector General
U.S. Small Business Administration:

Administrator
U.S. Small Business Administration:

Report on the Audit of the Consolidated Financial Statements

Disclaimer of Opinion

We were engaged to audit the consolidated balance sheets of the United States (U.S.) Small Business Administration (SBA) as of September 30, 2024 and 2023, and the related notes to the consolidated balance sheets (the consolidated financial statements).

We do not express an opinion on the accompanying consolidated financial statements of the SBA. Because of the significance of the matter described in the Basis for Disclaimer of Opinion section of our report, we have not been able to obtain sufficient appropriate audit evidence to provide a basis for an audit opinion on the consolidated financial statements.

Basis for Disclaimer of Opinion

The SBA's pandemic relief programs include the Paycheck Protection Program, Economic Injury Disaster Loan program, Restaurant Revitalization Fund program, and Shuttered Venues Operators Grant program, which were authorized by the Coronavirus Aid, Relief, and Economic Security Act of 2020 and related legislations. These programs affect a substantial proportion of SBA's consolidated financial statements. As of the date of our audit report, management was still in the process of designing and implementing corrective actions to remediate control deficiencies identified in the prior and current years. These control deficiencies contributed to SBA's inability to provide relevant and reliable information to support a significant number of transactions and account balances related to these programs. As a result of this matter, we were unable to determine whether any adjustments might have been necessary related to the Credit Program Receivables and Related Foreclosed Property, Net; Other than Intragovernmental Accounts Receivable, Net; Downward Reestimate Payable to Treasury; Loan Guarantee Liabilities; and the related notes.

Other Matters

Report on Certain Fiscal Year 2024 and 2023 Information

We were not engaged to audit the consolidated statements of net cost and changes in net position, and combined statements of budgetary resources for the years ended September 30, 2024 and 2023, and the related notes to these statements. Accordingly, we express no opinion on them.

Interactive Data

Management has elected to reference to information on websites or other forms of interactive data outside the Agency Financial Report to provide additional information for the users of its consolidated financial statements. Such information is not a required part of the 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.

Responsibilities of Management for the Consolidated Financial Statements

Management is responsible for the preparation and fair presentation of the consolidated financial statements in accordance with U.S. generally accepted accounting principles, and for 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' Responsibilities for the Audit of the Consolidated Financial Statements

Our responsibility is to conduct an audit of the SBA's consolidated financial statements in accordance with auditing standards generally accepted in the United States of America (GAAS), Government Auditing Standards, issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin No. 24-02, Audit Requirements for Federal Financial Statements, and to issue an auditors' report. However, because of the matter described in the Basis for Disclaimer of Opinion section of our report, we were not able to obtain sufficient appropriate audit evidence to provide a basis for an audit opinion on these consolidated financial statements.

We are required to be independent of the SBA and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements relating to our audit.

Required Supplementary Information

U.S. generally accepted accounting principles require that the information in the Management's Discussion and Analysis and Required Supplementary Information sections be presented to supplement the basic consolidated financial statements. Such information is the responsibility of management and, 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 were unable to apply certain limited procedures to the required supplementary information in accordance with GAAS because of the significance of the matter described in the Basis for Disclaimer of Opinion paragraph. We do not express an opinion or provide any assurance on the information.

Other Reporting Required by *Government Auditing Standards*

Report on Internal Control Over Financial Reporting

In connection with our engagement to audit the SBA's consolidated financial statements as of September 30, 2024, we considered the SBA's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing an opinion on the consolidated financial statements, but not for the purpose of expressing an opinion on the effectiveness of the SBA's internal control. Accordingly, we do not express an opinion on the effectiveness of the 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 were not identified. However, as described in the accompanying Appendices I and II, we identified certain deficiencies in internal control that we consider to be material weaknesses 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 the accompanying Appendix I to be material weaknesses.

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 the accompanying Appendix II to be significant deficiencies.

Report on Compliance and Other Matters

In connection with our engagement to audit the SBA's consolidated financial statement as of September 30, 2024, 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 consolidated financial statement. However, providing an opinion on compliance with those provisions was not an objective of our engagement, and accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 24-02, and which are described in accompanying Appendix III as items A and B.

We also performed tests of the SBA's 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 engagement, and accordingly, we do not express such an opinion. The results of our tests disclosed instances, described in the accompanying Appendix III as item C, in which the SBA's financial management systems did not substantially comply with the (1) Federal financial management systems requirements, and (2) applicable Federal accounting standards. The results of our tests disclosed no instances in which the SBA's financial management systems did not substantially comply with the United States Government Standard General Ledger at the transaction level.

Additionally, if the scope of our work had been sufficient to enable us to express an opinion on the consolidated financial statements, other instances of noncompliance or other matters may have been identified and reported herein.

SBA's Response to Findings

Government Auditing Standards requires the auditor to perform limited procedures on the SBA's response to the findings identified in our engagement and described in the accompanying Appendix IV. The SBA's response was not subjected to the other auditing procedures applied in the engagement to audit the consolidated financial statements and, accordingly, we express no opinion on the response.

Purpose of the Other Reporting Required by Government Auditing Standards

The purpose of the communication described in the Report on Internal Control Over Financial Reporting and the Report on Compliance and Other Matters sections 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 the SBA's internal control or compliance. Accordingly, this communication is not suitable for any other purpose.

KPMG LLP

Washington, DC
November 15, 2024

U.S. Small Business Administration

Material Weaknesses

The following deficiencies are considered to be material weaknesses in internal controls over financial reporting.

1. **Controls over Coronavirus Disease 2019 (COVID-19) Economic Injury Disaster Loans (EIDLs) Need Improvement**
2. **Controls over Paycheck Protection Program (PPP) Loan Guarantees Need Improvement**
3. **Controls over Monitoring of Restaurant Revitalization Fund (RRF) and Shuttered Venues Operators Grant (SVOG) Programs Need Improvement**
4. **Controls over Financial Reporting for Programs Funded by CARES Act and Related Legislation Need Improvement**
5. **Controls over the Evaluation of Service Organizations Need Improvement**
6. **Entity Level Controls Need Improvement**
7. **Controls over General Information Technology Need Improvement**

Background

The COVID-19 EIDLs, PPP, RRF, and SVOG programs were authorized and funded by the Coronavirus Aid, Relief, and Economic Security Act of 2020, the Paycheck Protection Program and Health Care Enhancement Act, the Economic Aid to Hard-Hit Small Businesses, Nonprofits, and Venues Act, and the American Rescue Plan Act. The referenced laws are collectively referred to as the CARES Act and related legislation. The CARES Act and related legislation were passed by Congress to provide emergency assistance in response to the extensive effects of the public health and economic crisis arising from the COVID-19 pandemic. The COVID-19 EIDLs, PPP, RRF, and SVOG programs affect a substantial proportion of the consolidated financial statements.

1. Controls over COVID-19 EIDLs Need Improvement

The COVID-19 EIDLs transactions were approved in fiscal years 2020 through 2022. These loans have a 30-year term, and the originating payment start date was deferred by the SBA for up to 30 months after the loan disbursement. The payment deferral period ended for a significant number of COVID-19 EIDLs beginning in fiscal year 2023 and continued into fiscal year 2024.

We found that management did not design and implement adequate monitoring controls over the COVID-19 EIDLs portfolio to ensure reliable financial reporting as of the end of the fiscal year. Management's review was not appropriately designed to identify a complete and accurate COVID-19 EIDLs population of outstanding loans disbursed to eligible recipients. The review process relied on hold codes in the SBA's loan repository system to identify the COVID-19 EIDLs with eligibility concerns. However, management was not able to provide evidence of the completeness and accuracy of the population of loans with hold codes as of the end of the fiscal year.

Management did not properly design the review controls over loans with existing hold codes. Specifically, management did not document sufficient evidence about the identification, research, and resolution of hold codes to support management's reliance for financial reporting purposes as of the end of the fiscal year.

Further, management did not identify and research COVID-19 EIDLs with unresolved hold codes for loans charged-off, in deferment, repayment, and delinquent stages as of the end of the fiscal year.

During fiscal year 2024, management expanded the Hardship Accommodation Plan (HAP) that is offered to COVID-19 EIDLs borrowers experiencing short-term financial challenges to help bring them into compliance and avoid default. The expansion included allowing COVID-19 EIDLs that were previously charged-off to be reinstated with temporarily modified payment terms. However, management did not design and implement effective controls over the review of reinstated loans resulting from HAP enrollments. Management did not provide sufficient evidence on the completeness and accuracy of the reinstated population as of the fiscal year-end. The COVID-19 EIDLs that were reinstated due to HAP enrollments were not subsequently monitored to ensure those loans continued to meet HAP eligibility. In addition, management did not consistently reinstate loans receivable for COVID-19 EIDLs that were enrolled in a HAP, which were previously charged off, and in certain instances the borrowers were making payments.

The monitoring controls over the servicing and review of the COVID-19 EIDLs portfolio were not adequately documented or updated timely to reflect process changes throughout the fiscal year. Management implemented significant policy changes in fiscal year 2024, however, management did not update the COVID-19 EIDLs servicing manual to reflect the current processes and related controls in operation including the expansion of the HAP and the changes to the charge off process.

These deficiencies were caused by an inadequate risk assessment process to identify and mitigate relevant risks and design appropriate controls at a sufficient level of precision to ensure a complete and accurate population of COVID-19 EIDLs that were disbursed to eligible recipients. In addition, management's information systems were not designed to properly update the loan status of COVID-19 EIDLs which were previously charged-off but that required reinstatement due to HAP enrollments. The monitoring controls over the active HAP population were not designed to ensure COVID-19 EIDLs enrolled in HAP meet the eligibility requirements. Finally, management did not update and review the documentation of existing policies and procedures in a timely manner to ensure the most current operating environment was reflected in its documentation.

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

- GAO's Green Book, Principle 3, Establish Structure, Responsibility, and Authority; Principle 6, Define Objectives and Risk Tolerances; Principle 7, Identify, Analyze, and Respond to Risks; Principle 9, Identify, Analyze, and Respond to Change; Principle 10, Design Control Activities; and Principle 12, Implement Control Activities

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

The deficiencies described above may result in a material misstatement of the Credit Program Receivables and Related Foreclosed Property, Net and Downward Reestimate Payable to Treasury line items, and related elements in the consolidated financial statements.

Recommendations – Controls over COVID-19 EIDLs Need Improvement

We recommend the Administrator coordinate with the Associate Administrator for the Office of Capital Access to:

1. Perform and update the program's internal control risk assessment to identify and respond to changes to risks that may require updates to the design and implementation of effective monitoring controls over the review of the COVID-19 EIDLs portfolio.

2. Design and implement sufficient controls to identify COVID-19 EIDLs disbursed to ineligible recipients and implement an effective funds recovery plan to ensure COVID-19 EIDLs funds

disbursed to ineligible recipients are recovered and reported accurately and in a timely manner. The plan should include an effective process to provide the information necessary to the Office of Planning, Performance, and the Chief Financial Officer to record any required accounting adjustments for accurate and timely financial reporting.

3. Identify all COVID-19 EIDLs with an incorrect status. Research and update the status of the identified COVID-19 EIDLs within the applicable systems of record for loan accounting.

4. Review and update the design, implementation, and operating effectiveness of controls over information technology program changes within the applicable systems of record for loan accounting to ensure changes are appropriate and function as intended.

5. Update existing process and controls documentation over the servicing and review of COVID-19 EIDLs to ensure they are relevant, reliable, and based on implemented policies and procedures. Perform a regular review of implemented processes and controls to ensure they are in line with documented policies and procedures.

2. Controls over PPP Loan Guarantees Need Improvement

A. Forgiveness Review of PPP Loan Guarantees

The PPP program terms, authorized by the CARES Act and related legislation, permitted for the forgiveness of PPP loan guarantees if the borrower met the forgiveness criteria. To request forgiveness, borrowers submit the forgiveness application to the lenders for approval. The lenders will subsequently notify SBA of their forgiveness decision and submit the request to SBA.

We found that management did not design and implement adequate monitoring controls over the work performed by a contractor and the use of its case management system to ensure that the population of PPP loan guarantees identified with eligibility flags was complete and accurate to determine eligibility for forgiveness. Moreover, management did not provide corroborating evidence to demonstrate that an effective control environment exists when the case management system was used to perform the automated screening of the PPP loan guarantees. Also, an independent review of a contractor's work was not performed effectively to determine whether the results of the contractor's screening process of certain loan guarantees was complete and accurate. These loan guarantees included those with no flags identified for eligibility concerns, or those that had flags identified for eligibility concerns but were not reviewed further based on management's policy decision.

Also, management did not design and implement an effective review and monitoring process for the 2021 cohort of PPP loan guarantees, which comprises the majority of the outstanding principal balance of PPP loan guarantees as of September 30, 2024. The case management system contained a comprehensive series of validation checks to identify potential ineligible PPP loan guarantees; however management only used the system to perform a limited number of validation checks against program eligibility requirements for the 2021 cohort of PPP loan guarantees. Further, management did not implement the appropriate monitoring process to ensure that lenders followed established procedures to adequately resolve the eligibility concerns identified by the case management system's limited automated screening.

The design and implementation of monitoring and review controls to determine the accuracy and completeness for the sample of PPP loan guarantee forgiveness transactions were not effective. The review of the sample from the largest subset of PPP loan forgiveness transactions did not address the eligibility for forgiveness and the accuracy of the approved loan guarantee and forgiveness amounts. In addition, management's review process did not include a requirement to follow-up when differences existed between the sample loan approval amount and the loan forgiveness amount within an acceptable variance threshold. As a result, management's sample review process was not properly designed to evaluate and quantify the magnitude of the actual error amounts for the loan guarantee approval and loan guarantee forgiveness variances.

Management did not adequately design and implement the post payment review control to determine the appropriate status and financial reporting impacts of PPP loan guarantees forgiven as of the end of the fiscal year. Management's process and related control activities for funds recovery of PPP loan guarantees that may have been erroneously forgiven is not documented or effectively implemented.

Management did not fully implement a process to update the outstanding principal balance of PPP loan guarantees subsequent to the forgiveness payments in its loan accounting system. Also, management did not document the automated and manual process that was partially implemented. Further, the outstanding principal balance for certain PPP loan guarantees were not accurate because the balances were not updated subsequent to forgiveness payments.

These deficiencies were caused by management's reliance on the contractor's automated and manual loan review processes without adequate monitoring controls to evaluate and assess their work. Also, management placed undue reliance on the lenders' self-certifications prior to the approval of the 2021 cohort of PPP loan guarantees without adequate monitoring controls. An adequate risk assessment process to identify and mitigate relevant risks and design appropriate controls to ensure a complete and accurate portfolio of PPP loan guarantees that were disbursed to eligible recipients was not effectively performed by management. Finally, management did not document or implement an effective process for updating the outstanding principal loan balance for PPP loan guarantees subsequent to forgiveness.

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

- GAO's Green Book, Principle 3, Establish Structure, Responsibility, and Authority; Principle 6, Define Objectives and Risk Tolerances; Principle 7, Identify, Analyze, and Respond to Risks; 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 deficiencies described above may result in a material misstatement to the Loan Guarantee Liabilities and Downward Reestimate Payable to Treasury line items, and other related elements in the consolidated financial statements.

<u>Recommendations – Forgiveness Review of PPP Loan Guarantees</u>

We recommend the Administrator coordinate with the Associate Administrator for the Office of Capital Access to:

6. Perform a thorough review of the outstanding PPP loan guarantees to determine the impact on the outstanding guarantee and eligibility for forgiveness of loans identified to not be in conformance with the related legislation and program's terms.

7. Design, implement, and document an effective PPP forgiveness review process for loan guarantees that were forgiven that addresses both the eligibility and the accuracy of the loan approval and forgiveness amounts.

8. Design and implement an effective funds recovery plan to ensure PPP funds disbursed on behalf of ineligible recipients are recovered and reported accurately in a timely manner. The plan should include an effective process to provide the information necessary to the Office of Performance, Planning, and the Chief Financial Officer to record any required accounting adjustments.

9. Identify the root cause of the erroneous adjustment and design and implement a control to remediate the deficiency.

10. Document, design, and implement an effective process and controls to update the outstanding principal balance for PPP loan guarantees subsequent to forgiveness.

B. Purchases of PPP Loan Guarantees

The PPP program terms, authorized by the CARES Act and related legislation, fully guaranteed the PPP loans disbursed by lenders on behalf of the SBA. Lenders are required to service the PPP loans and continue to report on their status on a monthly basis until the loan is fully forgiven, repaid, or the borrower defaults. In the event of default, the lender may request that SBA honor its full guarantee and purchase the loan.

We found that management did not adequately design and implement controls to ensure that purchase requests of PPP loan guarantees were appropriately reviewed to verify that requesting lenders met the program requirements prior to approving and disbursing the original loan.

The PPP loan guarantee purchases review process relies on the identification of flags indicating that the lender may not have fulfilled the program requirements. The design and implementation of monitoring and review controls to ensure that the completeness and accuracy of flags identified and resolved for outstanding PPP loan guarantees was not adequate. In addition, management added additional flags that require a manual review of PPP purchases at various stages of the program. However, management did not retroactively review PPP loan guarantee purchase requests that were previously automatically approved that subsequently required a manual review.

The PPP loan guarantee purchases review process documentation did not consider all relevant guidance issued to lenders as part of the origination process when determining the subset of flags that would require a manual purchase review. Specifically, management did not include adequate evaluation of flags communicated to lenders in the procedural notices related to the cohort 2021 loan approval requirements.

These deficiencies were caused by an inadequate risk assessment performed to ensure the appropriate controls were designed and implemented for the review of PPP loan guarantee purchase transactions.

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

- GAO's Green Book, Principle 3, Establish Structure, Responsibility, and Authority; Principle 6, Define Objectives and Risk Tolerances; Principle 7, Identify, Analyze, and Respond to Risks; and Principle 10, Design Control Activities

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

The deficiencies described above may result in a material misstatement to the Loan Guarantee Liabilities and Downward Reestimate Payable to Treasury line items, and the related elements in the consolidated financial statements.

Recommendations – Purchases of PPP Loan Guarantees

We recommend the Administrator coordinate with the Associate Administrator for the Office of Capital Access to:

11. Perform a thorough and complete analysis of all requirements communicated to lenders for the PPP program and determine whether lenders met the requirements prior to disbursing a PPP loan. The analysis should include evidence to support the adequacy of management's review process when determining which purchase requests will require additional review.

12. Develop and implement an effective process to review purchase requests for outstanding PPP

loan guarantees and for loans that were previously purchased that address whether the lender met their requirements in accordance with the program requirements.

13. Develop and implement an effective funds recovery plan to ensure funds related to PPP purchases disbursed to ineligible recipients are recovered and reported accurately in a timely manner. The plan should include an effective process to provide the information necessary to the Office of Performance, Planning, and the Chief Financial Officer to record any required accounting adjustments.

3. Controls over Monitoring of RRF and SVOG Programs Need Improvement

A. Monitoring of RRF Awards

The period to use RRF awards for eligible purposes expired in fiscal year 2023. SBA relies on award recipients to submit Post Award Reports to disclose the amount of the award used on eligible purposes prior to expiration. If any amount of the award was not used for eligible purposes before expiration, the unused funds must be returned to SBA.

Management did not design and implement the appropriate monitoring controls over RRF awards to ensure that the funds were used in accordance with the CARES Act and related legislation and accurate financial reporting as of the end of the fiscal year. Specifically, a Post Award Report was not submitted for a significant number of awards as of September 30, 2024. While management performed follow-up procedures to ensure the outstanding Post Award Reports were submitted by the remaining recipients, the procedures were not substantial enough to support the completeness and accuracy of financial reporting as of the end of the fiscal year. During the fiscal year, management selected a sample of RRF awards for review to determine the accuracy of submitted Post Award Reports. However, management did not initiate or fully complete reviews for a significant number of samples to ensure accurate financial reporting as of the end of the fiscal year. Further, management's process for funds recovery was not fully implemented for RRF awards that had eligibility concerns.

These deficiencies were caused by an inadequate risk assessment process to identify and mitigate relevant risks and design appropriate monitoring controls to ensure funds were spent on eligible expenses to be relied upon for financial reporting.

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

- GAO's Green Book, Principle 10, Design Control Activities; Principle 12, Implement Control Activities; and Principle 13, Use Quality Information

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

The deficiencies described above may result in a material misstatement to the Other than Intragovernmental Accounts Receivable, Net, line item and the related elements in the consolidated financial statements.

<u>Recommendations – Monitoring of RRF Awards</u>

We recommend the Administrator coordinate with the Associate Administrator for the Office of Capital Access to:

14. Continue to perform and update the program's internal control assessment to identify changes to risks that may require the design and implementation of effective monitoring controls and review processes of RRF awards to identify recipients that may not have been eligible to receive awards or that may have spent awards on ineligible expenses in accordance with the program's terms.

15. Design and implement effective follow-up procedures for RRF award recipients that are not complying with the program's terms and to ensure complete, accurate, and timely reporting for the use of the award.

16. Design and implement an effective funds recovery plan and controls to ensure RRF awards disbursed to ineligible recipients or spent on ineligible expenses are recovered and reported accurately and in a timely manner. In conjunction with the Office of Planning, Performance, and the Chief Financial Officer, design and implement an effective process to provide the information necessary to record any required accounting adjustments.

B. Monitoring of SVOG Awards

The time period to use SVOG funds for eligible purposes expired for all SVOG awards. The SBA relies on award recipients to submit an Expense Report and Standard Form (SF) 425, Federal Financial Report, to disclose the amount of the award used for eligible purposes prior to expiration. If any amount of the award was not used for eligible purposes before expiration, the unused funds must be returned to SBA.

Management did not design and implement appropriate monitoring controls over SVOG awards to ensure that the funds were used in accordance with the CARES Act and related legislation and accurate financial reporting as of the end of the fiscal year. Specifically, as of September 30, 2024, an Expense Report or SF-425 was not submitted for certain awards. In addition, management selected samples of SVOG awards to review the accuracy of report submissions and eligibility of award recipients. However, management did not initiate or fully complete the sample reviews for a significant number of samples.

Management's process for funds recovery was not fully implemented for SVOG awards that had identified eligibility concerns. Additionally, management's process to review the recipients' single audit reports was not complete by the end of the fiscal year. Therefore, management could not determine the impact of potential control and compliance deficiencies noted in the single audit reports over the use of SVOG awards.

These deficiencies were caused by an inadequate risk assessment process to identify and mitigate relevant risks and design appropriate monitoring controls to ensure funds were spent on eligible expenses to be relied upon for financial reporting.

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

- GAO's Green Book, Principle 10, Design Control Activities; Principle 12, Implement Control Activities; and Principle 13, Use Quality Information

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

The deficiencies described above may result in a material misstatement to the Other than Intragovernmental Accounts Receivable, Net, line item and the related elements in the consolidated financial statements.

<u>Recommendations – Monitoring of SVOG Awards</u>

We recommend the Administrator coordinate with the Associate Administrator for the Office of Disaster, Recovery, and Resilience to:

17. Continue to implement effective monitoring controls and review processes of SVOG awards to identify recipients that may not have been eligible to receive awards or that may have spent awards on ineligible expenses in accordance with the program's terms.

18. Design and implement effective follow-up procedures for SVOG award recipients that are not complying with the program's terms and to ensure complete, accurate, and timely reporting for the use of the award.

19. Design and implement an effective funds recovery plan and controls to ensure SVOG awards disbursed to ineligible recipients or spent on ineligible expenses are recovered and reported accurately and in a timely manner. In conjunction with the Office of Planning, Performance, and the Chief Financial Officer, design and implement an effective process to provide the information necessary to record any required accounting adjustments.

4. Controls over Financial Reporting for Programs Funded by CARES Act and Related Legislation Need Improvement

A. Accounting for Funds Recovery

The PPP, COVID-19 EIDLs, RRF, and SVOG programs affect a significant proportion of SBA's consolidated financial statements. As these programs are either in the servicing, post payment review or post award phases, SBA began the process to recover funds or identify funds that need to be recovered.

Management did not adequately design and implement controls to account for the recovery of funds related to these programs. Management did not provide evidence of implemented and documented accounting policies and procedures for the recovery of funds related to the RRF and SVOG programs and the recording of the related accounts receivable and allowance for estimated uncollectible amounts. For example, management was not able to demonstrate the application of the accounts receivable recognition criteria for the determination of a claim to cash or other assets due to recovery of funds for each program. Also, management did not maintain adequate documentation supporting the estimation methodology used to determine the accounts receivables and the related allowance for estimated uncollectible amounts based on the status of the awards in the post award review stage or how the post award review sample results would be utilized. Moreover, management did not fully develop and implement the financial reporting considerations related to the recovery of funds for the RRF and SVOG programs including the respective accounting entries.

The accounting policies for the recovery of funds related to the COVID-19 EIDLs and PPP loan programs were not determined by management and documented as of the end of the fiscal year. Further, management did not have adequate documentation to support an analysis of the appropriate accounting treatment with the respective accounting entries in accordance with generally accepted accounting principles, for each step of the recovery life cycle once loan forgiveness and charge-off transactions have been determined to be improper and recovery efforts are initiated. Also, management did not fully complete the evaluation of when the charge-off of a loan should occur.

These deficiencies were caused by an inadequate risk assessment to identify and mitigate relevant financial reporting risks. Also, management did not develop the appropriate policies and procedures for considerations related to the recovery of funds through the applicable programs' lifecycle including the servicing and post payment review phases.

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

- 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

The deficiencies identified above may result in a material misstatement to the Other than Intragovernmental Accounts Receivable, Net, Credit Program Receivables and Related Foreclosed

Property, Net, Loan Guarantee Liabilities, and Downward Reestimate Payable to Treasury line items, and related elements in the consolidated financial statements.

<u>Recommendations – Accounting for Funds Recovery</u>

We recommend the Administrator coordinate with the Chief Financial Officer to:

20. Develop, document, and implement the accounting policies and procedures for the recovery of funds, the accounts receivable, and the allowance for estimated uncollectible amounts related to the programs created or expanded by the CARES Act and related legislation.

21. Inquire and continue to obtain guidance from standard setting bodies to confirm the appropriate accounting treatment for COVID-19 EIDLs and the PPP loans that have been improperly forgiven or charged-off and for which recovery has been initiated. Memorialize the response by updating management's documented policies and procedures including the respective accounting entries under generally accepted accounting principles for all applicable scenarios.

22. Design and implement effective controls and communication processes to timely obtain the information necessary from program offices to record any required accounting adjustments for programs created or expanded by the CARES Act and related legislation.

B. Subsidy Reestimate

Statement of Federal Financial Accounting Standards Number 2, *Accounting for Direct Loans and Loan Guarantees*, requires that direct loans and loan guarantees committed after September 30, 1991, be recorded on a present value basis consistent with the intent of the Federal Credit Reform Act of 1990. As such, SBA developed an estimation methodology to reestimate the future net cash inflows and outflows for the COVID-19 EIDLs and PPP loan portfolios as of the end of the fiscal year.

We found that management did not design and implement adequate review controls over the data inputs used in the PPP subsidy reestimate. Specifically, management did not adequately design and implement controls to ensure the data inputs used in the PPP subsidy reestimate methodology that are derived from the forgiveness and purchases processes are complete and accurate.

Also, management did not design and implement adequate review controls over the data inputs used for COVID-19 EIDLs subsidy reestimate. The reviews were in process as of the end of the fiscal year and not appropriately designed to identify a complete and accurate COVID-19 EIDLs population of outstanding loans disbursed to eligible recipients.

The loan-level projection datasets included projected cash flows for loans that were charged-off without an outstanding loan receivable balance as of September 30, 2024, for various programs' subsidy reestimates. The projected cash flows for these charged-off loans inappropriately affected the allowance for subsidy balances without the related recognition of the gross loans receivable.

Management did not fully document the considerations made for potential impacts to the estimation methodology for the COVID-19 EIDLs subsidy reestimates due to significant program changes that occurred during the fiscal year. Specifically, the Hardship Accommodation Plan was expanded in fiscal year 2024 resulting in a significant increase in enrollments and loan reinstatements. Discussions were held with the program office related to this change and included in the model documentation where the changes impacted implemented model enhancements. However, management did not fully document the assessment performed to determine if any enhancements should be made to the estimation methodology.

These deficiencies were caused by an inadequate entity wide control environment related to the design, implementation, and operating effectiveness of controls related to the review of the loan portfolio at a precision level necessary to ensure the data inputs used for the reestimate models are complete and accurate. In addition, the deficiencies were caused by the implementation and development of subsidy reestimate models for programs that do not have a significant volume of historical data or precedence. The deficiencies were caused by the inadequate design and implementation of review controls to ensure the impact of significant program changes on the reestimate were adequately documented. Also, there were inadequate accounting policies and procedures to assess the appropriate timing of loan charge-off to ensure the reestimate output and resulting financial reporting impact complied with applicable accounting standards for charged-off loans.

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

- GAO's Green Book, Principle 3, Establish Structure, Responsibility, and Authority; Principle 10, Design Control Activities; and Principle 13, Use Quality Information

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

The deficiencies described above may result in a material misstatement to the Credit Program Receivables and Related Foreclosed Property (Net), Downward Reestimate Payable to Treasury, and Loan Guarantee Liabilities line items, and the related elements in the consolidated financial statements.

<u>Recommendations – Subsidy Reestimate</u>

We recommend the Administrator coordinate with the Chief Financial Officer to:

23. Continue implementing review controls in collaboration with relevant program offices for the PPP and COVID-19 EIDLs portfolios to accumulate relevant, complete, and accurate data on which to base the subsidy reestimate.

24. Design and implement adequate review and approval controls over the reestimate for the PPP and COVID-19 EIDLs portfolios by appropriate levels of management, and to coordinate with relevant program offices to assess the integrity of relevant data inputs used in the development of assumptions, and reasonableness for the selected assumptions used and the resulting estimates.

25. Refine existing review and approval controls to ensure the documentation of the impact of significant program changes is adequate.

26. Inquire and continue to obtain guidance from standard setting bodies to confirm the appropriate accounting and financial reporting treatment for projected cash flows of charged-off loans in the reestimates. Memorialize the responses as part of a documented policy.

5. Controls over the Evaluation and Monitoring of Service Organizations Need Improvement

A. Service Organizations Used for Loan Guarantee Programs

Management did not obtain reasonable assurance on the operating effectiveness of internal controls in multiple service organizations' control environments relevant to the 7(a) loan guarantee program fiscal transfer agent, the financial service providers for the 7(a) and 504 loan guarantee programs, and the PPP forgiveness and purchases platform. With regards to the financial service providers for the 7(a) and 504 loan guarantee programs, the relevant control environments include the facilitation, maintenance, and reporting of the account balances for the respective secondary market programs. With regards to the PPP forgiveness and purchases platform, the relevant control environment includes the operation of the PPP loan forgiveness and PPP loan purchase modules, the data transmissions over the internet between the relevant modules and SBA systems used in the configured checks, the cloud-based infrastructure hosting provider, and the application controls within the application intake platform.

In addition, management did not provide evidence of adequate monitoring activities performed over the relevant internal control environment for certain subservice organizations identified in the service organization control (SOC) 1 Type 2 report.

Management did not provide evidence of adequate monitoring and evaluation activities performed for the complementary user entity controls identified in the service organization control (SOC) 1 Type 2 reports obtained for the 504 loan guarantee program central servicing agent and the financial service provider. In addition, the evaluations of the complementary user entity controls and control objectives were not complete.

These deficiencies identified above were caused by inadequate monitoring controls over the relevant service organizations for their assigned internal control responsibilities to obtain reasonable assurance on the operating effectiveness of internal controls in the service organizations' control environments. Management made an incorrect determination that the sub-service organization's controls were included and evaluated by an independent auditor, however the controls were carved out (i.e. not inclusive).

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

- GAO's Green Book, Section 4, Additional Considerations: Service Organizations; Principle 5, Enforce Accountability; 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 deficiencies described above prevent SBA from obtaining an understanding of relevant service organization controls and their operating effectiveness to identify all relevant control gaps and deficiencies that require a complementary user control to mitigate the risk of error to the Loan Guarantee Liabilities line item and related elements in the consolidated financial statements.

<u>Recommendations – Service Organizations Used for Loan Guarantee Programs</u>

We recommend the Administrator coordinate with the Associate Administrator for the Office of Capital Access to:

27. Assess the risk posed by the service organizations' control environments and obtain sufficient assurance over the operating effectiveness of relevant and significant controls to ensure the integrity of transactions processed on behalf of and recorded by management. To achieve this, consider obtaining and assessing SOC 1 reports for the relevant control environments at the service organizations to determine that:

    - SOC 1 reports are sufficiently scoped to address transaction processing and related control activities performed by the service organizations on behalf of management.

    - 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 management's internal controls over financial reporting, the potential impact to management's financial statements, and mitigating controls considerations made during their risk assessment.

    - All complementary user entity controls described in the SOC 1 reports are evaluated using current information and with consideration to their applicability to SBA's internal controls over financial reporting.

    - Evaluation of controls to document the results that include an assessment about whether all relevant complementary user entity controls and other management-performed controls were tested on a frequency determined by management and found operating effectively and, if they are not, assess the impact of such deficiencies on management's internal controls over financial reporting.

- All complementary subservice organization controls described in SOC 1 reports are evaluated to determine whether they provided services and performed controls considered relevant to management's internal controls over financial reporting 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 their reporting periods and corresponding gap letters provide sufficient coverage to assess impacts on management's internal controls over financial reporting and include matters requiring additional follow up by management.

B. Service Organization Used for the SVOG Program

Management did not obtain reasonable assurance on the operating effectiveness of internal controls in the control environments of the subservice organizations utilized by the service organization for the SVOG platform in monitoring the status of awards.

Management did not provide evidence of adequate monitoring and evaluation activities performed for the complementary subservice organization controls listed in the service organization's SOC 1 report. Also, management did not provide evidence of adequate monitoring and evaluation activities performed for the complementary user entity controls and complementary subservice organization controls listed in the SOC 1 reports of the subservice organizations. Specifically, the evaluation of complementary user entity controls and complementary subservice organization controls was not complete as there was not documentation of the significance and relevance of each control to SBA's internal controls over financial reporting. In addition, management did not evaluate whether the complementary user entity controls and complementary subservice organization controls were designed, implemented, and operating effectively. For one subservice organization, management did not obtain and review the SOC 1 report in a timely manner as of fiscal year-end.

These deficiencies were caused by management not implementing effective monitoring of the effectiveness of internal control over the assigned processes performed by the relevant service organization.

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

- GAO's Green Book, Section 4, Additional Considerations: Service Organizations; Principle 5, Enforce Accountability; 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 deficiencies described above prevented SBA from obtaining an understanding of relevant service and subservice organizations' controls and their operating effectiveness to identify all relevant control gaps and deficiencies that require a complementary user control to mitigate the risk of error to the Other than Intragovernmental Accounts Receivable, Net line item and related elements in the consolidated financial statements.

<u>Recommendations – Service Organizations Used for the SVOG Program</u>

We recommend the Administrator coordinate with the Associate Administrator for the Office of Disaster, Recovery, and Resilience to:

28. Assess the risk posed by the service organizations' and subservice organizations' control environments to determine which subservice organization controls are relevant to SBA and

obtain sufficient assurance over the operating effectiveness to determine the integrity of SVOG program transactions processed on behalf of and recorded by SBA. To achieve this, obtain a SOC 1 report for the relevant control environments at the service organizations, and perform and document the following:

- Verify that the SOC 1 report is sufficiently scoped to cover transaction processing and related control activities performed by the service organizations on behalf of SBA.

- Evaluate all exceptions noted in the SOC 1 report – not just those described in the independent service auditor's report – to determine applicability to SBA's internal controls over financial reporting, the potential impact to SBA's financial statements, and mitigating controls considerations made during their risk assessment.

- Evaluate all complementary user entity controls described in the SOC 1 reports using current information and with consideration to their applicability to SBA's internal controls over financial reporting.

- Evaluate controls and clearly document the results that include an assessment over whether all complementary user entity controls and other SBA-performed controls were tested on a frequency determined by SBA and operating effectively. Assess the impact of such deficiencies on SBA's internal controls over financial reporting.

- Evaluate all complementary subservice organization controls described in SOC 1 reports to determine whether they provided services and performed controls considered relevant to SBA's internal controls over financial reporting and, if relevant subservice organizations were identified, an evaluation is performed to obtain an understanding of the subservice organization(s) and their controls.

- Verify that the SOC 1 reports cover the appropriate period or corresponding gap letters provide sufficient coverage to assess impacts on SBA's internal controls over financial reporting.

C. Service Organizations Used for Payroll and Personnel

Management did not implement a process to annually review the SOC 1 reports over its payroll and personnel systems to determine the reliability of information produced by the system. The SOC 1 reports are not monitored and reviewed to assess whether complementary user entity controls that users of the service organization (e.g., management) should have in place are designed, implemented, and operating effectively to supplement the service organization's internal controls.

These deficiencies were caused by management not evaluating the standard operating procedures over the review and assessment of SOCs to determine the required procedures related to systems and reports utilized by management.

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

- GAO's Green Book, Section 13, Use Quality Information; and Principle 16, Perform Monitoring Activities

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

By not monitoring services provided by third-party service providers, this increases the risk that management may be unaware of control failures that could impact the reliability of those systems and accuracy of data used to prepare the consolidated financial statements.

Recommendations – Service Organizations Used for populations of Separated Users

We recommend the Office of Human Resources Solutions to:

29. Assess the risk posed by the service organization's control environments to identify the relevant significant controls, including determining the relevant of any subservice organizations.

30. Implement procedures to review the SOC 1 report for the service organization's control environment in accordance with management's standard operating procedures. Additionally, evaluate the effectiveness of complementary user entity controls to determine the reliability of controls and reports provided by the service organization.

6. Entity Level Controls Need Improvement

Management faced challenges in maintaining an adequate entity level controls system that produces reliable and accurate financial reporting. The significance of the internal control matters indicated weaknesses across several entity level control categories. The following conditions were identified.

A. Control Environment and Risk Assessment

Management did not establish an effective control environment and did not perform effective risk assessment processes. The following deficiencies were identified across the SBA:

- Management did not adequately develop and document the materiality threshold considered and applied by program offices when key decisions regarding controls and review processes were implemented. The controls within the relevant offices were not designed, implemented, and operating effectively to a sufficient precision level to ensure the reporting objective of preparing the financial statements free of material misstatement could be achieved. For example, the COVID-19 EIDLs and PPP loan review processes were not designed to ensure the reviews performed were to a sufficient level of precision to ensure the related balances were free of material misstatement.

- Management did not implement adequate risk assessment processes to identify, analyze, and respond to relevant risks for FY2024. For example, management did not adequately respond to the increased risk of noncompliance with applicable laws (e.g., DCIA) due to the large volume of COVID-19 EIDLs entering delinquency and subsequent charge off in FY2024. Additionally, management did not evaluate the risks related to the mass reestablishment of COVID-19 EIDLs due to the increased enrollment in the Hardship Accommodation Plan (HAP).

B. Monitoring

Management did not design and implement effective monitoring processes. Management did not have adequate or effective monitoring controls related to:

- PPP lenders.

- Internal control over processes performed by service organizations.

- RRF and SVOG program award recipients.

- The COVID-19 EIDLs portfolio to identify a complete and accurate population of loans disbursed to eligible recipients for financial reporting purposes as of fiscal year-end.

These deficiencies were caused by the prioritization of the continued execution and servicing of the CARES Act and related legislation programs over internal control processes and related remediation of prior year control deficiencies. In addition, these deficiencies were caused by the lack of available resources needed to perform an adequate risk assessment, appropriately remediate prior year control deficiencies, implement, and monitor the operating effectiveness of controls, and operationally service large-scale programs effectively.

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

- GAO's Green Book, Principle 6, Define Objectives and Risk Tolerances; Principle 7, Identify, Analyze, and Respond to Risks; Principle 9, Identify, Analyze, and Respond to Change; Principle 10, Design Control Activities; Principle 12, Implement Control Activities; Principle 16, Perform Monitoring Activities; Principle 17, Evaluate Issues and Remediate Deficiencies

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

As a result of the deficiencies described above, we noted that without the proper level of entity level controls in place and operating effectively, there is an increased risk that a material misstatement in the consolidated financial statements, and noncompliance with the relevant laws and regulations would neither be prevented or detected and corrected in a timely manner.

Recommendations – Entity Level Controls Need Improvement

We recommend that the Administrator coordinate with the Associate Administrator of the Office of Capital Access and the Associate Administrator of the Office of Disaster Recovery and Resilience to:

31. In conjunction with the Office of the Chief Financial Officer, review and evaluate the completed internal control risk assessments for programs that have a material impact on the financial statements at a process level. Develop a plan to respond in a timely manner, including the consideration of whether entity level controls, manual controls, general information technology controls, and system application controls are designed, implemented, and are operating at a sufficient precision level in accordance with management's materiality threshold and will be sufficient for financial reporting purposes.

32. Design, implement, and monitor the operating effectiveness of key controls that respond to significant risks of material misstatements and compliance with relevant laws and regulations.

7. Controls over General Information Technology Need Improvement

Management had control deficiencies that limited SBA's ability to effectively manage its information system risks. Collectively, these deficiencies 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. In the sections below, we have omitted some technical details from the conditions and recommendations due to the sensitivity of the information. These details were communicated to management through other written communications.

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

- GAO's Green Book, Principle 7, Identify, Analyze, and Respond to Risks; Principle 10, Design Control Activities; Principle 11, Design Activities for the Information System; and Principle 12, Implement Control Activities

- National Institute of Standards and Technology Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations

Management did not effectively design, implement, and operate access controls for applications, databases, operating systems, and tools, particularly those related to the authorization, provisioning, monitoring, and deactivation of user accounts. Specifically, management did not have adequate controls designed, implemented, and operating effectively for the timely removal of access to SBA systems for separated employees and contractors. Management also did not consistently implement and enforce controls across multiple systems regarding the configuration of application password security, and authentication to the SBA network and applications.

Management did not properly design and implement a process for recertifying user accounts that required validation by an independent individual with the necessary knowledge and authority to recertify access. Further, user recertifications did not always contain sufficient user identifier information, preventing reviewers from associating accounts with individuals and assessing the appropriateness of their access based on their roles and responsibilities.

These deficiencies were caused by several factors: a lack of enforcement of account management controls for the authorization, provisioning, monitoring, and deprovisioning of user accounts; inadequate implementation of password, and authentication controls; insufficient monitoring and accountability of individuals performing control responsibilities; inconsistent validation of the continued operating effectiveness of controls ensuring data is completely and accurately captured and recorded; and an inadequate risk assessment process to identify and mitigate the risk of inappropriate access.

The deficiencies described above increases the risk that unauthorized users may retain access to the system resulting in unauthorized modification, destruction, or exposure to SBA systems and data, including manipulation of financial transactions and erroneous financial reporting.

<u>Recommendations – Logical Access Controls</u>

We recommend the Administrator coordinate with the Acting Chief Information Officer to:

33. Implement procedures to validate that SBA network access for separated users, per the authoritative source listings, is removed within the required timeframes.

34. Establish a plan to implement multi-factor authentication for non-privileged users.

35. Implement a process to track compliance with the plan to implement multi-factor authentication requirements.

We recommend the Administrator coordinate with the Chief Financial Officer to:

36. Document within the system security plan the control implementation for all tools and layers within the authorization boundary.

37. Develop and provide training to the control operators to reinforce the existing policies and procedures for requesting, approving, and provisioning new or modified user access.

38. Establish a backup for the individual responsible for operating system account management to remove single points of failure.

39. Revise the account recertification script so data is retrieved from the correct fields.

40. Update the account review and recertification procedures to include quality control steps to validate that complete and accurate account listings are used for all user accounts within the authorization boundary, including the operating system servers.

41. Update the user access review control to include an attribute to ensure that the reviewer has the knowledge, authority, and independence to conduct the review. Additionally, formalize these procedures within the existing account management policies and procedures.

42. Improve controls over personnel actions to ensure timely separation of employees and removal of system access privileges.

43. Provide training to control operators to reinforce the existing policies and procedures for requesting and approving user access for employees dependent upon their employment status (e.g. temporary employee, full-time employee and contractor).

44. Implement separation of duties between roles and functions within the organization to prevent circumvention of controls.

Appendix II

U.S. Small Business Administration

Significant Deficiencies

The following deficiencies are considered to be significant deficiencies in internal controls over financial reporting.

1. **Controls over Payments for Covered Loans under the Debt Relief Program Need Improvement**
2. **Controls over Reporting of Contingencies Need Improvement**

1. Controls over Payments for Covered Loans under the Debt Relief Program Need Improvement

The CARES Act and related legislation authorized the Debt Relief Program that allowed SBA to make payments on behalf of certain loans in the 7(a) and 504 loan guarantee programs and the Microloan program.

Management did not design and implement effective controls over the Debt Relief Program post payment review process. A contractor was used to develop and perform a risk-based methodology to identify the payments for covered loans that may have a higher risk for overpayments and would require further review. However, management did not provide evidence of an effective review over the accuracy of the inputs, appropriateness of significant assumptions, and the application of the methodology.

Further, management did not provide evidence of an effective review of the other alternative methodologies considered and a documented approved basis for the selected risk-based methodology. The documentation evidencing a risk assessment for the impact of the payments that were not considered, determined to be of lower risk, and the application of variance thresholds was not provided by management. Despite the high rate of false positive loan payments that were identified for review by the methodology, management did not provide documentation considering whether the applied methodology was still appropriate.

These deficiencies were caused by management's reliance on the contractor's work without adequate monitoring controls. Also, management did not perform an adequate risk assessment to identify and mitigate relevant risks and design appropriate controls to ensure an effective post payment review of payments for covered loans under the Debt Relief Program caused the deficiency identified above.

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

- GAO's Green Book, Principle 3, Establish Structure, Responsibility, and Authority; Principle 6, Define Objectives and Risk Tolerances; Principle 10, Design Control Activities; Principle 12, Implement Control Activities and Principle 16, Perform Monitoring Activities

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

The deficiencies described above may result in misstatements of the Loan Guarantee Liabilities line item and related elements in the consolidated financial statements.

<u>Recommendations – Payments for Covered Loans under the Debt Relief Program</u>

We recommend the Administrator coordinate with the Acting Associate Administrator for the Office of Capital Access to:

45. Design and implement controls that require oversight over contractors, including maintenance of documentation, that provides evidence over the adequate review and validation of the contractor's work product.

46. Perform and document a thorough risk assessment of the payments for covered loans under the Debt Relief Program.
47. Design and implement the appropriate review controls to identify payments that may have been improper or inaccurate. Implement an effective funds recovery plan that includes an effective process to provide the information necessary to record any required accounting adjustments for accurate and timely financial reporting based on the results of the risk assessment.

2. Controls over Reporting of Contingencies Need Improvement

Statement of Federal Financial Accounting Standards Number 5, *Accounting for Liabilities of the Federal Government*, establishes the accounting and financial reporting requirements for contingencies. A contingency is an existing condition, situation, or set of circumstances involving uncertainty as to possible gain or loss that will ultimately be resolved when one or more future events occur or fail to occur. Contingencies should be recognized as a liability when a past transaction or event has occurred, a future outflow or other sacrifice of resources is probable, and the related future outflow or sacrifice of resources is measurable. Contingencies should be disclosed if any of the conditions for liability recognition are not met and there is a reasonable possibility that a loss or an additional loss may have been incurred.

Management did not design and implement monitoring controls to ensure the timely and complete recognition and disclosure of contingent liabilities. A detailed listing of pending or threatened litigation and unasserted claims against the SBA was not obtained or maintained by the office responsible for financial reporting. The office responsible for financial reporting received a summary of cases by program; however, the information did not include the name and description of each case, the amount claimed, likelihood of loss, and estimated amount or range of potential loss. The information and communication process between the office responsible for communicating the legal matters did not provide the necessary information to those responsible for the financial reporting to perform a complete assessment of the financial reporting impact.

Also, management did not report the summary of cases in accordance with a newly implemented materiality policy. Further, management did not document the quantitative and qualitative evaluation performed to determine that recognition or disclosure was not warranted in accordance with its policy.

The deficiency was caused by the lack of an effective communication and information process between the offices responsible for providing all relevant information regarding legal matters to the respective office responsible for the financial reporting to perform the appropriate assessment of legal matters and the impact to SBA consolidated financial statements. Also, management did not adequately implement the new materiality policy.

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

- GAO’s Green Book, Principle 3, Establish Structure, Responsibility, and Authority; Principle 10, Design Control Activities; Principle 13, Use Quality Information; and Principle 14, Communicate Internally
- OMB Circular No. A-123, Management’s Responsibility for Enterprise Risk Management and Internal Control

The deficiency described above may result in misstatements or omissions to the Other than Intragovernmental Liabilities line item and the Commitments and Contingencies disclosure and other related elements in the consolidated financial statements.

Recommendations – Reporting of Contingencies

We recommend the Administrator coordinate with the Chief Financial Officer to:

48. Design and implement effective communication processes with the Office of General Counsel to obtain relevant and complete information to ensure complete, accurate, and timely recognition and disclosure of contingencies.

49. Update the new materiality policy to specify the application criteria and design and implement controls to ensure that the application of the policy is effective and documented.

U.S. Small Business Administration

Compliance and Other Matters

A. Debt Collection Improvement Act of 1996, as amended (DCIA)

Certain provisions of the DCIA require agencies to notify and refer debts that are delinquent by 120 days or more, for purposes of administrative offset and centralized collection, to the U.S. Department of Treasury (Treasury).

Management did not refer delinquent loans to the Treasury for collection within the required timeframe. Management identified and communicated that approximately 755,725 COVID-EIDLs and 363,863 PPP loans were noncompliant with DCIA requirements for the fiscal year ended September 30, 2024.

In addition, management did not design and implement effective controls to identify a complete population of delinquent loans that meet the criteria for referral to Treasury to ensure compliance with DCIA requirements.

The conditions identified were caused by inadequate design and implementation of risk assessment and monitoring processes that enable management to identify, analyze, and respond to the relevant risks of noncompliance and to ensure delinquent loans were identified and referred to Treasury within the required timeframe. Also, the deficiencies were caused by inadequate system infrastructure in place to understand and respond to the root causes of noncompliance.

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

- DCIA
- GAO's Green Book, Principle 9, Identify, Analyze, and Respond to Change; and Principle 10, Design Control Activities

As a result of delays and absence of referrals of delinquent borrowers and guarantors to Treasury, SBA did not comply with DCIA requirements.

<u>Recommendations – DCIA</u>

We recommend the Administrator coordinate with the Associate Administrator for the Office of Capital Access to:

50. Perform a regular review and risk assessment of the implemented policies to ensure they are responding to relevant risks of noncompliance for the current fiscal year.
51. Design, implement, and document appropriate monitoring controls to address compliance with DCIA.
52. Reevaluate the operational infrastructure and system controls to address relevant risks of noncompliance and ensure that borrowers are notified timely of delinquency, and if applicable, subsequently referred to Treasury timely.

B. Federal Managers' Financial Integrity Act of 1982 (FMFIA)

Management performed an internal control assessment as required under FMFIA. However, management's assessment did not substantially comply with FMFIA and the related OMB Circular No. A-123 requirements. Specifically, management did not:

- Thoroughly document a comprehensive evaluation of internal control over financial reporting regarding current programs while giving consideration to relevant risks during the fiscal year.
- For the risks significant to financial reporting, consistently document financial statement risks and assertions covered, testing procedures performed, extent of sampling performed, testing results, corrective action plans to respond to deficiencies identified, and provide evidence of management review.
- Ensure their own assurance process was sufficient to identify material weaknesses that existed during the fiscal year in addition to those identified by external auditors.

Management did not substantially meet FMFIA requirements due to the urgent need to implement the provisions of the CARES Act and related legislation as quickly and efficiently as possible, the lack of historical precedence, and other inherent challenges faced in implementing and expanding programs. In addition, management did not consider all FMFIA and OMB Circular No. A-123 requirements when performing their evaluation over internal controls.

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

- Section 2 of FMFIA
- OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

Management did not substantially comply with FMFIA and the related OMB Circular No. A-123 requirements, which may lead to not identifying the appropriate risks and key controls, and not detecting internal control or compliance deficiencies. The risk of not detecting and correcting control deficiencies could result in misstatements to the consolidated financial statements.

Recommendations – FMFIA

We recommend the Administrator coordinate with the Chief Financial Officer to:

53. In conjunction with relevant program offices, perform and document a comprehensive internal control evaluation over all programs. This should include entity level controls, manual controls, general information technology controls, and system application controls covering key financial statement line items and risks.
54. Work with relevant program office management to communicate and respond to control testing results and update corrective action plans to remediate control deficiencies identified.
55. Update the existing policy and implement adequate controls to ensure that the statement of assurances provided by the program offices are adequately documented and reviewed for completeness and accuracy to provide a sufficient basis to support the Administrator's statement of assurance.

C. Federal Financial Management Improvement Act of 1996 (FFMIA)

Management did not establish and maintain financial management systems that substantially comply with the following FFMIA requirements:

- Federal Financial Management Systems Requirements. As discussed in Appendix I – Material Weaknesses, control deficiencies over transactions arising from the implementation of the CARES Act and related legislation do not enable reliable and accurate financial reporting, do not ensure compliance objectives are met, and do not ensure budgetary resources are safeguarded against waste, loss, and misuse.

- Federal Accounting Standards. The deficiencies identified and reported in Appendix I – Material Weaknesses, provide an indication that SBA's financial management systems were substantially noncompliant with applicable federal accounting standards. Specifically, management was unable to provide evidence that the accounting treatment and financial reporting of the recovery of funds related to the RRF, SVOG, COVID-19 EIDLs, and PPP programs were in accordance with U.S. generally accepted accounting principles.

Management did not substantially meet FFMIA requirements because of the reasons discussed in Appendix I – Material Weaknesses and due to an inadequate entity wide control environment to implement the provisions of the CARES Act and related legislation with sufficiently designed and implemented controls.

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

- Section 803(a) of FFMIA

- GAO's Green Book, Section 2, Establishing an Effective Internal Control System

- Appendix D to OMB Circular No. A-123, Compliance with the Federal Financial Management Improvement Act of 1996

Management did not substantially comply with FFMIA increasing the risk that transactions are incorrectly recorded to the general ledger, impacting the completeness, existence, and accuracy of the balances in the consolidated financial statements.

<u>Recommendations – FFMIA</u>

We recommend the Administrator coordinate with the Chief Financial Officer to:

56. Address the control deficiencies over transactions arising from the implementation of the CARES Act and related legislation by working with the Office of Capital Access and the Office of Disaster Recovery and Resilience to implement the recommendations in Appendix I – Material Weaknesses.

CFO Response to Audit Report on FY 2024 Financial Statements

DATE: November 15, 2024

TO: Hannibal M. Ware, Inspector General

FROM: Kate Aaby, Associate Administrator for Performance, Planning and the Chief Financial Officer

SUBJECT: FY 2024 Financial Statement Audit

The Small Business Administration has reviewed the Independent Auditors' Report from KPMG that includes the auditors' disclaimer of opinion on the Agency's FY 2024 and FY 2023 Consolidated Balance Sheets. The independent audit of the Agency's financial statements and related processes is a core component of SBA's financial management program, and we are concerned by this result.

The FY 2024 Agency Financial Report includes pandemic relief programs: the Paycheck Protection Program, the COVID-19 Economic Injury Disaster Loan program, the Restaurant Revitalization Fund program, and the Shuttered Venue Operators Grant program, which were authorized by the Coronavirus Aid, Relief, and Economic Security Act of 2020, the Economic Aid Act, the American Rescue Plan Act, and related legislations. As in FY 2023, the management of these programs during prolonged unprecedented times continued to emphasize the importance of serving small businesses as they navigate extraordinary circumstances.

The SBA has continued making tremendous progress strengthening internal controls for pandemic-focused programs and is dedicated to accountability and transparency to the American public. In FY 2024, SBA hired a Chief Risk Officer (CRO) and established a new Office of Enterprise Integrity (OEI) to evaluate and consolidate audit management, internal controls, improper payments, fraud risk management and Enterprise Risk Management (ERM). SBA's Fraud Risk Management Board (FRMB) mitigates, manages, and monitors fraud risks aligned with GAO's Fraud Risk Management Framework. The FRMB is co-chaired by the CFO and CRO and members include Deputy Associate Administrators of key program offices, who are supported by an advisory team of SBA leaders with subject matter expertise across cybersecurity, data, systems, learning and development, and more.

In FY 2024, SBA implemented a more centralized financial statement audit management structure to provide the Agency additional support and oversight to improve financial statement audit posture, improving partnerships across SBA and providing more proactive considerations to strengthen SBA's confidence of its financial standing. The CFO and key SBA program offices have partnered in the development and implementation of corrective actions that will strengthen internal controls as well as address audit identified deficiencies. This was all accomplished and prioritized within existing resources.

The SBA Senior Management Council (SMC) which is chaired by the CRO and comprised of SBA managers from program and support offices, actively plans and executes the Agency's internal control activities that include assessing and improving compliance, monitoring and remediation of identified deficiencies and communicating results of reviews to senior management.

The auditors identified material weaknesses related to the internal controls over seven areas: COVID-19 Economic Injury Disaster Loans, Paycheck Protection Program Loan Guarantees, the Restaurant Revitalization Fund and Shuttered Venue Operators Grant Program, Financial reporting for programs funded by CARES Act and related legislation, Evaluation of Service Organizations, Entity Level Controls, and General Information Technology Controls. The SBA has undergone tremendous efforts to strengthen internal controls, policies and procedures and will continue remediation efforts in the coming audit year.

In FY 2024, SBA re-engaged the Federal Accounting Standards Advisory Board (FASAB) to obtain clarification on the appropriate accounting treatment for various scenarios within the COVID-19 Economic Injury Disaster and Paycheck Protection Program loan portfolios. Due to the unique programs and scope of the standards, FASAB has redirected our inquiry to Treasury and OMB. These discussions will occur in FY 2025 and will be a critical milestone in SBA's remediation.

In addition, SBA implemented Single Sign-On for the Financial Management System in FY 2024. This streamlined multi-factor authentication process enhanced the efficiency, security, and user experience associated with accessing the Financial Management System.

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 beneficial recommendations that support our efforts to further enhance the SBA's financial management practices. We remain committed to excellence in financial management and look forward to furthering progress in the coming year.