

COVID-19 AND DISASTER ASSISTANCE INFORMATION SYSTEMS SECURITY CONTROLS

REPORT NUMBER 22-19 | SEPTEMBER 27, 2022





EXECUTIVE SUMMARY

Report 22-19

COVID-19 AND DISASTER ASSISTANCE INFORMATION SYSTEMS SECURITY CONTROLS

What OIG Reviewed

This report presents the results of our audit to determine whether the U.S. Small Business Administration (SBA) maintained effective management control activities and monitoring of the design and implementation of third-party operated SBA systems.

Demand for financial assistance because of the economic effects of the Coronavirus Disease 2019 (COVID-19) pandemic required SBA to expand the Economic Injury Disaster Loan (EIDL) and initiate the Paycheck Protection Program (PPP) loan forgiveness programs.

SBA needed information technology systems from third-party service providers that could improve the system efficiency and productivity to process high transaction volumes, transmit data between other information systems, and safeguard the integrity and confidentiality of the personally identifiable information processed by the programs.

The design and related monitoring affects data processed within these third-party systems and impacts the integrity of the agency's system control architecture. These systems feed data to SBA's financial systems and directly impact the effectiveness of cybersecurity controls.

Our objective was to determine what internal controls the organization designed to address system cybersecurity risks caused by COVID-19 and disaster economic relief transactions.

We reviewed whether management effectively designed, implemented, and monitored IT controls, such as authorization to operate procedures, security, privacy, incident response, contract compliance, and system development for three disaster assistance systems.

What OIG Found

We found the agency's entity-level control environment was not designed in accordance with federal guidance at the beginning of the COVID-19 assistance programs. The agency

allowed the third-party systems to be put into service without conducting the baseline assessments. With no baseline, the agency could not perform effective continuous monitoring. Also, we found that control processes did not identify, communicate, and capture privacy and identity risks on an enterprise-wide basis.

We also found that SBA deployed mission-critical systems without full adherence to important SBA security and privacy controls. For example, we found agency assessment and oversight of the third-party systems was incomplete approximately a year after both systems were put into operation. In addition, neither system met the requirement for an independent auditor's evaluation, such as the System and Organization Controls (SOC) 1 report. The SOC 1 report provides assurance that reported financial data is complete and reliable.

Agency management told us their delay in effectively designing entity-level controls and implementing continuous monitoring was caused by the urgency to deliver immediate COVID-19 assistance to small businesses.

OIG Recommendations

We made 10 recommendations to strengthen the agency's entity-level IT control environment. The areas addressed included cybersecurity risk and privacy controls, system development life cycle, continuous monitoring, and the supply chain risk management processes.

Agency Response

SBA management fully agreed with seven recommendations, disagreed with two recommendations, and stated one recommendation was specific to the pandemic and will not likely be repeated. While the agency agreed to implement seven recommendations, management's planned corrective actions did not fully address identified control issues. OIG will seek resolution in accordance with our audit follow-up procedures.




Office of Inspector General

U. S. Small Business Administration

DATE: September 27, 2022

TO: Isabella Casillas Guzman
Administrator

FROM: Hannibal "Mike" Ware 
Inspector General

SUBJECT: Audit of COVID-19 and Disaster Assistance Information Systems Security Controls

This report represents the results of our audit *COVID-19 and Disaster Assistance Information Systems Security Controls*. We considered management comments on the draft of this report when preparing the final. SBA management fully agreed with seven recommendations, disagreed with two recommendations, and stated one recommendation was specific to the pandemic and will not likely be repeated.

We appreciate the courtesies and cooperation extended to us during this audit. If you have any questions, please contact me or Andrea Deadwyler, Assistant Inspector General for Audits, at (202) 205-6586.

cc: Arthur Plews, Chief of Staff
Therese Meers, Acting General Counsel
Michael Simmons, Attorney Advisor
Stephen Kucharski, Acting Chief Information Officer, Office of the Chief Information Officer
Luis Campudoni, Deputy Chief Information Officer, Office of the Chief Information Officer
Francisco Sanchez Jr, Associate Administrator, Office of Disaster Assistance
Patrick Kelley, Associate Administrator, Office of Capital Access
Ron Whalen, Acting Director, Office of Performance and Systems Management
Kate Aaby, Associate Administrator, Office of Performance, Planning, and the Chief Financial Officer
Tonia Butler, Director, Office of Internal Controls
Peggy Delinois Hamilton, Special Counsel for Enterprise Risk, Office of the Administrator

Table of Contents

| | |
|--|----|
| Introduction..... | 1 |
| Background..... | 1 |
| Disaster Assistance Systems and Security Risk Management..... | 2 |
| Results | 2 |
| Finding 1: SBA’s Entity-level Control Activities Were Not Effectively Designed..... | 3 |
| Perform Entity-wide Security Risk Management Assessments | 3 |
| Update the Agency’s System Development Methodology..... | 4 |
| Obtain and Review System and Organization Controls (SOC) Assurance Reports | 5 |
| Perform Validations on Third-party System Security Functionalities..... | 5 |
| Recommendations..... | 7 |
| Finding 2: SBA’s Entity-level Monitoring Activities Need Improvement..... | 8 |
| Complete Authorization to Operate Procedures Before Launching New Systems..... | 8 |
| Table 1. Completion Timeframes for Required Assessment and Authorization Components in Third-Party Systems Tested..... | 9 |
| Complete Data Sharing Agreements Prior to Operation..... | 9 |
| Enhance Monitoring Capabilities through Automation..... | 10 |
| Recommendations..... | 10 |
| Analysis of Agency Response..... | 11 |
| Summary of Actions Necessary to Close the Recommendations..... | 11 |
| Appendix I: Objective, Scope, and Methodology..... | 16 |
| Use of Computer-Processed Data | 16 |
| Assessment of Internal Controls..... | 16 |
| Prior Audit Coverage..... | 17 |
| Appendix II: Management Comments..... | 18 |

Introduction

This report presents the results of the audit of the U.S. Small Business Administration's (SBA) security controls in information systems used to deliver assistance during the Coronavirus 2019 (COVID-19) pandemic and disaster assistance programs. The objective was to determine what internal controls the agency designed to address system cybersecurity risks caused by COVID-19 and disaster economic relief transactions.

Background

During the past 2 years, SBA modified its systems and program delivery capabilities to provide emergency COVID-19 pandemic relief and ongoing disaster assistance. The volume and scope of agency assistance increased potential fraud and cybersecurity threats.

The SBA Office of Disaster Assistance initially used the Disaster Credit Management System (DCMS) to provide aid under the provisions of the Economic Injury Disaster Loan (EIDL) program. However, the program generated unprecedented transaction volumes that DCMS was unable to process. The agency made DCMS a high-value asset system in September 2020. The DCMS high-value asset designation reflects that the system handles Personally Identifiable Information (PII) and is mission critical. PII refers to information like names, social security numbers, addresses, etc., that can be used to distinguish or trace an individual's identity. Systems that meet the definition of Primary Mission Essential Functions¹ or National Essential Functions² are considered high-value assets.

In March 2020, SBA entered into a contract with a third-party service provider to replace the Office of Disaster Assistance's system and used a cloud-based system for COVID-19 EIDL assistance. Similarly, in June 2020 the SBA Office of Capital Access also adopted a cloud-based system acquired from another third-party service provider to process the acceptance, review, and disposition of PPP loan forgiveness decisions.

The SBA Office of Disaster Assistance reported three security incidents during the past two years. The first related to a data breach in March 2020 that affected the PII of approximately 8,000 applicants because the system did not have the capacity for the volume of transactions. The second security incident in October 2020 related to a brute force attack from a foreign source. The most recent incident in January 2022 related to third parties using stolen identities to access the system.

SBA established an Enterprise Cybersecurity Service to address cybersecurity intelligence, risk management, and incident response. Enterprise Cybersecurity Service is SBA's stated vehicle to meet the initiatives outlined in Presidential Executive Order 14028, Improving the Nation's Cybersecurity, and enables SBA to respond to cyber events. The Office of Chief Information Officer's Information Security Division provides cybersecurity threat briefings to the agency's Enterprise Risk Management Board. As outlined in the Office of

¹ Primary Mission Essential Functions are those mission essential functions that must be continuously performed to support or implement the uninterrupted performance of National Essential Functions.

² National Essential Functions are select functions that are necessary to lead and sustain the nation during a catastrophic emergency.

Management and Budget (OMB) Circular No. A-123, the Enterprise Risk Management Board is responsible for the establishment of a governance structure to oversee a robust risk management and related internal control process. The Federal Information Security Modernization Act (FISMA) of 2014 requires agencies to report the status of their information security programs to OMB. The FY 2020-2022 FISMA reporting metrics measures the agency's ability to provide a centralized, enterprise-wide view of cybersecurity risk management activities (i.e., identify, remediate, etc.) across the organization.

Disaster Assistance Systems and Security Risk Management

The control design and related monitoring affects data processed within third-party and internal systems. It also affects the integrity of the entire agency system control architecture. These disaster systems feed data to SBA's financial systems and directly impact the effectiveness of cybersecurity controls.

This audit addressed SBA's need to securely process high volumes of loan transactions and concurrently deliver prompt financial assistance to small businesses in need due to the pandemic and natural disasters. The cloud-based, third-party systems we reviewed had to concurrently meet emergency needs and process personally identifiable information. OMB Circular No. A-123 and FISMA guidance requires agency management to validate the adequacy of controls by third-party service providers.

In addition, Presidential Executive Order 14028 states the federal government must rapidly improve the security and integrity of critical software supply chains, further reinforcing requirements for federal agencies to exercise due diligence over cybersecurity. OMB Memorandum M-22-01 sets forth the guidance to comply with the Executive Order to improve visibility into and detection of cybersecurity vulnerabilities and threats to the federal government.

Results

The objective was to determine what internal controls the organization designed to address system cybersecurity risks caused by COVID 19 and disaster economic relief transactions. We assessed whether management effectively designed, implemented, and monitored IT controls, such as authorization to operate procedures, security, privacy, incident response, contract compliance, and system development for three disaster assistance systems.

We found the agency's entity-level control environment was not designed in accordance with federal guidance at the beginning of the COVID-19 assistance programs. The agency allowed the-third-party systems to be put into service without conducting the baseline assessments. With no baseline, the agency could not perform effective continuous monitoring. Also, we found that control processes did not identify, communicate, and capture privacy and identity risks on an enterprise-wide basis.

Finding 1: SBA's Entity-level Control Activities Were Not Effectively Designed

Entity-level control is a primary step to ensure the systems of internal controls are operating effectively and are consistently designed. According to the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*, entity-level controls have a pervasive effect on an entity's internal control system and include controls related to the entity's risk assessment process, control environment, service organizations, management override, and monitoring.

We found that SBA ineffectively designed and implemented entity-level controls as they provided quick delivery of disaster assistance during the pandemic. This occurred because SBA did not:

- perform entity-wide security risk management assessments;
- update the agency's system development methodology;
- obtain and review System and Organization Controls (SOC) assurance reports; and
- perform validations on third-party system security functionalities.

GAO standards require agency management to design control activities for appropriate coverage of objectives and risks in operations. Control activities are the actions management establishes through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the agency's information system.

Management designs entity-level control activities so that the agency meets its objectives and addresses related risks, and these activities ensure information technology continues to properly operate.

Perform Entity-wide Security Risk Management Assessments

SBA did not have an effective process for ensuring privacy and identity risks were captured and communicated on an enterprise-wide basis. GAO's *Standards for Internal Control in the Federal Government* states management must identify enterprise risks and develop needed risk responses. Subsequently, management must design control activities to address identified risk responses.

During the period of our review, three security incidents occurred on the Disaster Credit Management System (DCMS) Disaster Loan Application Portal (DLAP), an outward facing, high-value asset system designed to provide disaster assistance. Additional potential privacy and identity internal control weaknesses in other disaster areas were identified and communicated by OIG in memorandums, reports, and recommendations.

The most recent DCMS/DLAP security incident reported in January 2022 showed misappropriation of personal addresses and other PII data. SBA subsequently implemented automated privacy internal controls to ensure PII was accurate, timely, and complete. However, these controls were designed and implemented a year after the system went into production. These areas included privacy risks related to identity theft, misappropriated social security numbers, and modified applicant addresses.

In addition, we were unable to obtain evidence that previously identified privacy and identity risks from other disaster assistance systems were considered for mitigation in control baselines and communicated on an enterprise-wide basis. OMB A-130 states privacy and security controls must be considered before a system is put into production and periodically monitored. A baseline is a set of minimum-security controls defined for an information system. While the agency through the Enterprise Cybersecurity Service responds to security incidents, improvement is needed to ensure identity and privacy risks are fully integrated into the risk management process. This activity will help ensure more effective system control designs are implemented and monitored for all agency systems.

Update the Agency's System Development Methodology

SBA's System Development Methodology document was last updated in 2009 and was not consistent with current federal requirements. Consequently, the methodology provided only limited system design guidance.

The system development methodology sets out the structure for the design, acquisition, development, and maintenance of information technology. The system development methodology is a method used to validate whether controls, such as system requirements, approvals, and processes, have been properly designed and implemented and operate effectively.

The agency's 2009 System Development Methodology document did not provide procedural guidance over supply chain risk-management practices or high-value asset system designation.

We determined supply chain risk management practices, which also include accelerated system acquisition guidance, were not incorporated into the System Development Methodology. Supply chain risk management is a systematic process for managing vulnerabilities throughout the supply chain and developing response strategies to the unique risks presented by third-party suppliers. The agency had a Supply Chain Risk Management Implementation Plan, but it had not been integrated into the System Development Methodology, and it did not provide specific implementation procedures. For example, the plan did not address accelerated system development for new technologies. OMB Circular A-130 requires agencies to consider supply chain security control issues as a part of their resource planning and management activities throughout the system development life cycle to appropriately manage risks.

We also determined the current System Development Methodology did not include guidance to identify, categorize, and prioritize critical systems as high-value assets. We found that the systems used for COVID-19 assistance programs were not identified as high-value assets based on a review of the systems' descriptions in their respective security plans. OMB M-19-03 allows agencies to designate any system whose functionality impacts the organization's ability to perform its mission as a high-value asset. In addition, agencies are required to take a strategic, enterprise-wide view of cyber risk to protect high-value assets against cyber threats.

A high-value asset is a system critical to an organization because the loss or corruption of information could cause a serious impact to the agency's ability to perform its mission.

High-value asset system identification and categorization is a necessary security function that when appropriately designed helps safeguard agency information systems.

When system development methodologies do not include supply chain and high-value asset designation guidance, management may make uninformed decisions about system design, acquisition, and development that could result in the deployment of systems that do not fully meet agency operational and mission goals.

Obtain and Review System and Organization Controls (SOC) Assurance Reports

We found management did not obtain reasonable assurance of the design, implementation, and operating effectiveness of internal controls of the third-party information systems. Management also did not provide evidence that user entity controls were effectively designed, implemented, and operated as intended. The agency is required to obtain assurance that third-party internal controls function as represented. This independent assurance is the purpose of a SOC 1 Type 2 report. OMB Circular No. A-123 requires management to validate the adequacy of controls by third-party service providers using an independent evaluation such as the SOC 1 Type 2 report. It provides assurance that reported financial data is complete and reliable.

Independent third-party assurance of financial controls minimizes the risk of inaccurate financial reporting through validation of related integrity controls. However, we found billions of federal assistance dollars were being processed through the systems without assurance that the controls were operating as intended. SBA was unable to obtain reasonable assurance regarding the reliability and integrity of reported financial data, which contributed to two disclaimer³ audit opinions for fiscal years 2020 and 2021.

Perform Validations on Third-party System Security Functionalities

SBA did not provide documentation to validate that system functionality and security was included and reviewed in the acquisition contracts. Acquisition controls play a significant role in the effective management of an information system. Effective communication and coordination of activities throughout system development depends on complete and accurate documentation of decisions and activities leading up to decisions. Activities and decisions should not be considered complete until there is tangible documentation of the activity or decision. We found the agency lacked documentation in areas of system development, as follows:

³ A disclaimer of opinion results when an auditor cannot obtain sufficient information to render an opinion on an organization's financial statements.

- The acquisition contract for one of the two systems we audited did not include required acceptance criteria. The contract was signed without explicit expectations of the minimum desired acceptable system functionality. Acceptance criteria specify the minimum desired functionality acceptable for a system to be put into operation as a usable platform despite known risks and uncertainties. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev.) 5 recommends acquisition contracts to define user acceptance criteria.
- SBA did not independently verify the system specifications using a requirements traceability matrix and test plans for either information system although SBA policy requires a traceability matrix. Requirements traceability validates that the system specifications are carried through to the design, build, and evaluation stages to ensure the system operates as intended. The requirements traceability matrix is an essential reference for the system specifications, test strategy, and allocation of requirements to acceptance criteria.
- The Office of the Chief Information Officer did not provide evidence that they reviewed the third-party service provider contracts in coordination with the system owners and the contracting office. OMB Circular A-130 and Standard Operating Procedure (SOP) 90 47 6 require the Office of the Chief Information Officer to ensure that the terms and conditions in contracts involving the collection, use, and processing of federal information incorporate security and privacy requirements⁴ to protect federal information. Security and privacy requirements in the contract provide reasonable assurance that security can be enforced, including activities performed by third-party service providers.

The agency's priority to provide economic assistance as quickly as possible resulted in management not following all the applicable requirements for systems development, such as developing traceability matrixes, acceptance criteria, and documenting contract review of security requirements.

Management cannot validate that acceptance criteria has been met and all system specifications have been tested and verified without a requirements traceability matrix. In addition, management cannot enforce security controls that are not specified in third-party contracts and validated by the Office of the Chief Information Officer. In such cases, the information systems may not achieve the intended purposes and could prevent the agency from achieving its mission to provide timely disaster assistance and ensure program eligibility requirements are maintained. In addition, these controls are essential to ensure protections are in place over applicants' personally identifiable information and other sensitive data.

⁴ All applicable NIST SP 800-53 controls should be put on contract for all contractor and outsourced operations.

Recommendations

We recommend the Administrator direct the Office of the Chief Information Officer to do the following:

1. Ensure the existing SBA System Development Methodology is updated to include supply chain risk-management practices as required by OMB Circular A-130 and high-value asset system designation guidance. Also, ensure high-value asset system risks are incorporated into the enterprise risk management framework, as recommended by OMB M-19-03 and SBA SOP 90 47 6.
2. Communicate and enforce the SBA System Development Methodology in which a traceability matrix is used to ensure that system requirements can be tested and demonstrated in the operational system. Ensure all requirements are aligned with the contractual acceptance criteria.
3. Implement in updated agency guidance, the requirements of OMB Circular No. A-123 that stipulate a SOC 1 Type 2 report is needed for all new and existing financial systems. This guidance should also require confirmation at least annually that the controls are functioning as designed.
4. Enforce the requirement to establish and implement internal controls to ensure appropriate program officials perform and document contract reviews to ensure that information security is appropriately addressed in the contracting language, as required by OMB Circular A-130 and SBA SOP 90 47 6.
5. In conjunction with the Enterprise Risk Management Board, implement enterprise-wide privacy risk mitigation practices that can be assimilated into new and existing system program designs.

Finding 2: SBA’s Entity-level Monitoring Activities Need Improvement

We determined SBA was unable to continuously monitor system security because of inconsistently established baselines for third-party information systems. The baseline consists of issues and deficiencies initially identified in an entity’s internal control system. *GAO Standards for Internal Control in the Federal Government* requires agencies to establish a baseline to continuously monitor the internal control system.

Continuous monitoring activities offer the organization better visibility into the state of security for its information systems. Continuous monitoring means maintaining ongoing awareness of information security, vulnerabilities, threats, and incidents to support agency risk management decisions.

Complete Authorization to Operate Procedures Before Launching New Systems

The agency did not fully implement a robust control baseline that addressed the need for essential security controls and continuous monitoring. SBA’s capability to implement continuous monitoring requirements is essential to ensure integration with the agency’s existing systems and prevent loss or corruption of data. According to SBA officials, this capability was adversely affected because of the agency’s priority to provide urgent economic assistance during the COVID-19 pandemic. The vehicles used to establish and monitor these baseline activities include the development of an assessment and authorization package;⁵ monitoring efforts that include updates to this package; and periodic evaluations of the effectiveness of controls through the vehicles such as the Plans of Action & Milestone (POA&M) process.

We found these control activities were not effectively performed in accordance with SBA SOP 90 47 6. Specifically, the agency did not perform a complete assessment and authorization when these systems were put into operation (see Table 1). We also found the agency did not update the authorization package annually as part of the information system continuous monitoring program. The agency also did not perform continuous monitoring of system weaknesses because the POA&Ms were not documented until 10 and 13 months after the two information systems were put into operation (see Table 1 – Plan of Action and Milestones).

In addition, any probable high-value asset POA&Ms rated critical or high were not remediated within 30 days as required by policy because they were not identified for 10 or 13 months. POA&M information is used to allocate risk mitigation resources for system weaknesses and deficiencies. POA&Ms are supposed to be updated quarterly as part of the

⁵ The assessment and authorization process is a baseline analysis of security and privacy controls. It is used to evaluate the internal control system, support information system risk management, and monitor security controls for effectiveness. At a minimum, the assessment and authorization package includes the following components: information system security plan, privacy plan, security control assessments, privacy control assessments, and Plans of Action and Milestones.

continuous monitoring program as required by agency policy and the Federal Information Security Management Act.

Table 1. Completion Timeframes for Required Assessment and Authorization Components in Third-Party Systems Tested

| Required Component | Months Completed After Operation for System 1 | Months Completed After Operation for System 2 |
|-------------------------------------|---|---|
| System Security Plan | 14 months | 9 months |
| Security and Risk Assessment Report | Incomplete | Incomplete |
| Security Assessment Plan | 13 months | 10 months |
| Privacy Impact Assessment | 14 months | Completed |
| Privacy Threshold Analysis | 14 months | Completed |
| Plan of Action and Milestones | 13 months | 10 months |
| Executive Summary | Incomplete | Incomplete |
| Authority To Operate Letter | 11 months | Completed |

Source: OIG analysis prepared as of June 4, 2021

OMB Circular No. A-130 requires agencies to conduct and document initial assessments and authorizations prior to systems being put into operation. Without performing initial or ongoing assessments and authorization, management may not be able to make informed decisions about the security and privacy controls that must be implemented to ensure mission-critical systems are designed and operate effectively in a highly dynamic environment.

Complete Data Sharing Agreements Prior to Operation

We found data-sharing agreements for the two third-party systems under review were completed 6 and 10 months after they were put into operation. Data sharing agreements ensure controls are in place when data is exchanged between external systems or other federal systems to ensure the proper protection and use of mission-critical, sensitive data. Data sharing agreements are used to plan, manage, and execute information exchange procedures.

Data sharing agreements were not completed at the time of operation due to the priority of delivering assistance to small business applicants. SBA SOP 90 47 6 requires that a written management agreement for system interconnections be obtained prior to connecting to a system and reviewed annually per the SBA Information System Continuous Monitoring Plan.

Because SBA did not have a completed data sharing agreement, there was no assurance the data used in data sharing agreements with contractors was protected because there was nothing binding parties to the requirements to address security controls that protect the confidentiality, integrity, and availability of the data transmissions used to process COVID-19 disaster assistance and loan forgiveness.

Enhance Monitoring Capabilities through Automation

The agency was unable to provide evidence they have automated configuration management monitoring capabilities as specified in FISMA guidance. FISMA criteria states an effective level of security includes the use of automated tools to improve the accuracy, consistency, and availability of configuration baseline information.

Agency management manually recorded changes (e.g., system enhancements, fixes, etc.) to one of the three systems in the audit scope. Managing the numerous configurations found within information systems has become almost impossible using manual methods. Automated solutions help lower the cost of configuration management efforts while enhancing efficiency and improving reliability.

Agency management accepted a manual tool to track configuration management. NIST SP 800-53 Rev. 5 Configuration Management-3 states “The organization documents configuration change decisions associated with the information system.” Manual records are insufficient to verify configuration testing and acceptance protocols because it is possible all changes to the system may not be captured or fully authorized.

Recommendations

We recommend that the Administrator direct the Office of the Chief Information Officer and the Office of Capital Access collaborate with program officials to:

6. Complete an initial assessment and authorization for each information system and all agency-designated common controls before operation.
7. Transition information systems and common controls to an ongoing authorization process (when eligible for such a process) with the formal approval of the respective authorizing officials or reauthorize information systems and common controls as needed, on a time or event-driven basis in accordance with agency risk tolerance, as required by OMB Circular No. A-130 and SOP 90 47 6.
8. Review and update POA&Ms at least quarterly as required by SOP 90 47 6.
9. Ensure data-sharing agreements are reviewed annually as required by SBA SOP 90 47 6.
10. Implement an automated process to document and monitor system changes as recommended by NIST SP 800-53 Rev. 5.

Analysis of Agency Response

Management provided formal comments, included in Appendix II. SBA management fully agreed with seven recommendations, disagreed with two recommendations, and stated one recommendation was specific to the pandemic and will not likely be repeated. While the agency agreed to implement seven recommendations, management's planned corrective actions did not fully address identified control issues.

In the recommendations where SBA disagreed with the findings, the identified issues were related to implementation of controls established in federal guidance. These recommendations convey the need for the agency to establish robust control baselines to ensure essential security controls are in place and effective. Federal guidance reinforces this need through SOP 90 47 6, which states that an assessment and authorization must be completed prior to a system being placed into production, or if there is a significant change in the system. Also, GAO's *Standards for Internal Control in the Federal Government* states that agency management holds third-party applications responsible for internal controls and ensures that those controls are effective.

In addition, SBA's management response did not fully address control issues identified in each recommendation or provide a final action target date. As a result, we consider all the recommendations as unresolved. In accordance with our audit follow-up policy, the proposed resolution steps and final action dates will be provided by the agency in subsequent correspondence. If management and OIG do not reach agreement on unresolved recommendations within 60 days after the date of this final report, OIG will notify the audit follow-up official of the disputed issue(s).

Summary of Actions Necessary to Close the Recommendations

The following list explains the status of each of our recommendations in the report and the actions we deem necessary to close them:

Recommendation 1: Ensure the existing SBA System Development Methodology is updated to include supply chain risk management practices as required by OMB Circular A-130 and high-value asset system designation guidance. Also, ensure high-value asset system risks are incorporated into the enterprise risk management framework, as recommended by OMB M-19-03 and SBA SOP 90 47 6.

Status: Unresolved

SBA management agreed with this recommendation and stated SBA will endeavor to improve its System Development Methodology and underlying principles, to include testing for core application functionality. Management's comments were not fully responsive to the recommendation because they did not address the risks identified, such as the need to provide procedural guidance over supply chain risk management practices or high-value asset systems designation.

This recommendation can be closed when management provides evidence that SBA revised its System Development Methodology document with procedural guidance over supply chain risk management practices and high-value asset system designation. Management

will also need to provide evidence that the agency has incorporated high-value asset systems risks into the enterprise risk management framework.

Recommendation 2: Communicate and enforce the SBA System Development Methodology in which a traceability matrix is used to ensure that system requirements can be tested and demonstrated in the operational system. Ensure all requirements are aligned with the contractual acceptance criteria.

Status: Unresolved

SBA management agreed and stated they will endeavor to improve its System Development Methodology and underlying principles, to include testing for core application functionality. Management's comments were not responsive to the recommendation because they did not address the need to provide procedural guidance over the use of a traceability matrix to ensure system requirements can be delivered.

This recommendation can be closed when the Office of the Chief Information Officer provides evidence that the agency has issued updated systems development guidance that includes the use of a traceability matrix to ensure system requirements can be tested. The agency will also need to provide evidence that they have established the requirement for design and testing of system controls prior to putting applications into production.

Recommendation 3: Implement in updated agency guidance, the requirements of OMB Circular No. A-123 that stipulate a SOC 1 Type 2 report is needed for all new and existing financial systems. This guidance should also require confirmation at least annually that the controls are functioning as designed.

Status: Unresolved

SBA management did not state agreement or disagreement with this recommendation. They stated that the exigent circumstances caused by the COVID-19 pandemic, reinforced by legislative requirements, did not permit sufficient time for such a formalized third-party audit as recommended. SBA further believes that this condition has been overcome by events.

The agency's comments did not fully address the recommendation. Specifically, A-123 requires the agency to obtain an independent evaluation of third-party financial systems. These evaluations allow agency managers to meet A-123 requirements to continuously monitor, assess, and improve the effectiveness of internal controls. The agency needs to update its guidance to ensure the independent control assessments are performed annually or as required.

This recommendation can be closed when management provides evidence that it has implemented updated guidance in accordance with A-123. The updated policy should require management to validate the adequacy of controls by third-party service providers using an independent evaluation, such as the SOC 1 Type 2 report. This updated policy applies to existing and future contracts for third-party IT financial systems.

Recommendation 4: Enforce the requirement to establish and implement internal controls to ensure appropriate program officials perform and document contract reviews

to ensure that information security is appropriately addressed in the contracting language, as required by OMB Circular A-130 and SBA SOP 90 47 6.

Status: Unresolved

SBA management agreed with this recommendation and stated they will consider updates to its mandatory cybersecurity language for IT acquisitions. SBA management comments were not responsive to the recommendation. The agency's response did not definitively state that they would include requirements to conduct contract document reviews in accordance with OMB A-130. This criteria requires the Office of the Chief Information Officer to ensure that the terms and conditions in contracts incorporate security and privacy control guidance to protect federal information.

This recommendation can be closed when SBA management provides evidence system functionalities are validated and security provisions are reviewed and included in contract language in accordance with OMB A-130.

Recommendation 5: In conjunction with the Enterprise Risk Management Board, implement enterprise-wide privacy risk mitigation practices that can be assimilated into new and existing system program designs.

Status: Unresolved

SBA management agreed and stated they are in the process of establishing more granular and frequent interfacing with the Enterprise Risk Management Board with regard to privacy and cybersecurity risk. Management's comments were not responsive to the recommendation because they did not definitively state that management would establish a process to update control designs related to PII incidents in a timely manner and ensure updated controls are considered for all other SBA systems.

GAO's Standards for Internal Control in the Federal Government requires management to design the entity's information system to obtain and process information to meet each operational process's information requirements and to respond to the entity's objectives and risks. Our report found that more security oversight is needed because the frequency of security incidents on outward facing systems increases the potential of compromising PII data.

This recommendation can be closed when the Office of the Chief Information Officer provides evidence that SBA has an effective process to ensure privacy and identity risks are captured and communicated across the agency.

Recommendation 6: Complete an initial assessment and authorization for each information system and all agency designated common controls before operation.

Status: Unresolved

SBA management disagreed with this recommendation. SBA stated that there is not always a cause-effect relationship, as inferred from the draft report, between the risk management and assessment activities conducted on a particular IT environment and the subsequent improper use of that same IT environment after authorization. The agency's response did not acknowledge that these initial and ongoing assessments and authorizations are needed to provide assurance that security and privacy controls perform as intended. OMB Circular

No. A-130 requires agencies to conduct and document initial assessments and authorizations prior to systems being put into operation.

This recommendation can be closed when the Office of the Chief Information Officer provides evidence management has implemented a process for conducting an initial assessment and authorization for each information system and all agency designated common controls before operation, and documentation to demonstrate that the process is occurring.

Recommendation 7: Transition information systems and common controls to an ongoing authorization process (when eligible for such a process) with the formal approval of the respective authorizing officials or reauthorize information systems and common controls as needed, on a time or event-driven basis in accordance with agency risk tolerance, as required by OMB Circular No. A-130 and SOP 90 47 6.

Status: Unresolved

Management disagreed with this recommendation stating that the specific type of authorization received by a particular IT environment, point-in-time authorization or ongoing authorization, was not a factor in the use or misuse of SBA's pandemic response IT systems implementations. The agency's response does not acknowledge that this control oversight was essential during the pandemic and would be problematic in response to future events. SBA's responsibilities are mandated by OMB Circular A-130 and SOP 90 47 6. These policies require agency-wide risk mitigation controls that prevent loss or corruption of data, as well as address potential identity and privacy risks.

This recommendation can be closed when SBA provides evidence that the agency performs timely authorizations for new and existing systems in accordance with OMB A-130 and SOP 90 47 6.

Recommendation 8: Review and update Plan of Action & Milestones (POA&M) at least quarterly as required by SOP 90 47 6.

Status: Unresolved

SBA management agreed with this recommendation but stated they believe that the condition has been overcome by events. We disagree that the conditions are overcome by events because we found the agency was non-compliant with the Federal Information Security Management Act which requires quarterly review and remediation of all systems through POA&Ms.

This recommendation can be closed when the Office of the Chief Information Officer provides evidence that all SBA's systems are monitored in accordance with FISMA POA&M guidance and SOP 90 47 6. This guidance further requires information be used to allocate risk mitigation resources for system weaknesses and deficiencies.

Recommendation 9: Ensure data sharing agreements are reviewed annually as required by SBA SOP 90 47 6.

Status: Unresolved

SBA management agreed with this recommendation but stated they believe that the condition has been overcome by events. OIG disagrees that the conditions are overcome by events because SBA has existing data sharing agreements and will continue to enter into agreements. The agreements must be reviewed annually in accordance with SOP 90 47 6.

This recommendation can be closed when the Office of the Chief Information Officer provides evidence data sharing agreements are completed at the time of operation and annually thereafter in accordance SBA SOP 90 47 6.

Recommendation 10: Implement an automated process to document and monitor system changes as recommended by NIST SP 800-53 Rev. 5.

Status: Unresolved

SBA management agreed with this recommendation and stated they will evaluate options for automating its change management process for IT systems and applications. SBA management comments were not responsive to the recommendation because they did not provide an implementation plan for this automated configuration capability.

This recommendation can be closed when the agency provides evidence it has automated configuration management monitoring capabilities for third-party applications as recommended by NIST SP 800-53 Rev. 5.

Appendix I: Objective, Scope, and Methodology

Our objective was to determine what internal controls the organization designed to address third-party contractor system cybersecurity risks caused by COVID and disaster economic relief transactions. The scope of the audit included SBA's management of control activities and monitoring of the third-party service provider information systems. We also considered organizational control activities related to the design of a disaster assistance delivery system that incurred a security incident in January 2022.

We assessed whether management effectively designed and implemented third-party oversight controls to address security, privacy, incident response, contract compliance, system development, and assessment and authorization controls. Additionally, we considered the findings and conclusions developed by the Fiscal Years 2020 and 2021 Independent Public Accountant because it also addressed third-party oversight controls for the two systems in this audit scope. The period of review was March 20, 2020 through March 31, 2022.

We reviewed agency policies, procedures, practices, and organizational structures designed to provide a reasonable assurance that business objectives will be achieved and that undesired events will be prevented, detected, and corrected.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Use of Computer-Processed Data

We used computer-processed data as a part of our audit procedures. We determined the use of computer-processed data did not materially affect our audit findings, conclusions, or recommendations and the risk of using such data without an assessment was deemed acceptable.

We relied on information used for widely accepted purposes and obtained from sources generally recognized as appropriate, such as data obtained from the Independent Public Accountant. Consequently, we did not need to establish the accuracy, completeness, and validity of the data. As a result, we did not perform an assessment of data produced by the information systems because these procedures were deemed to be out of scope.

Our opinion is solely based on the result of our testing of sampled items selected for review. We believe the data is sufficiently reliable to support our conclusions.

Assessment of Internal Controls

OMB Circular No. A-123 provides the specific requirements for how to perform evaluations and report on internal controls in the federal government.

OMB Circular No. A-123 requires federal government agencies to implement a comprehensive system of internal controls that provides reasonable assurance that agency

programs are designed, implemented, and operating as intended; and to evaluate the effectiveness of internal controls. It also requires agencies to integrate risk management and internal control functions. The Circular also establishes an assessment process based on the Government Accountability Office’s (GAO) Standards for Internal Control in the Federal Government (known as the Green Book) that management must implement the following five components of internal control framework:

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information
5. Communication and Monitoring

Management is also required to assess the design, implementation, and operating effectiveness of the entity’s internal controls to determine if an internal control system is effective.

We identified control activities, monitoring, and the associated principles as material or significant internal control components of this audit. We found the agency ineffectively designed control activities and monitoring as detailed in our audit findings and made recommendations that address the identified issues.

Prior Audit Coverage

| Report Title | Report Number | Final Report Date |
|---|---------------|-------------------|
| <i>Inspection of Small Business Administration’s Initial Disaster Assistance Response to the Coronavirus Pandemic</i> | 21-02 | October 28, 2020 |
| <i>Independent Auditors’ Report on SBA’s FY 2020 Financial Statements</i> | 21-04 | December 18, 2020 |
| <i>SBA’S Handling of Identity Theft in the COVID-19 Economic Injury Disaster Loan Program</i> | 21-15 | May 6, 2021 |
| <i>Weaknesses Identified During the FY 2020 Federal Information Security Modernization Act Review</i> | 21-17 | July 6, 2021 |
| <i>Independent Auditors’ Report on SBA’s FY 2021 Financial Statements</i> | 22-05 | November 15, 2021 |

Appendix II: Management Comments

SBA RESPONSE TO AUDIT REPORT



U.S. Small Business
Administration

Memo for: Hannibal Ware
Inspector General

From: Stephen Kucharski
Acting Chief Information Officer

Francisco Sanchez Jr.
Associate Administrator, Office of Disaster Assistance

Subject: Management Response:
Draft Report on COVID-19 and Disaster Assistance
Information Systems Security Controls
Project 20020

Date: August 18, 2022

We appreciate the opportunity to review the document entitled “Draft Report on COVID-19 and Disaster Assistance Information Systems Security Controls.” While we feel that the draft report reflects work done in earnest and with noble intentions, we feel that the report pays inadequate consideration to key facts regarding the significant restrictions mandated upon the SBA by pandemic response legislation, causing management to significantly deviate from its established processes.

The SBA has the following comments with respect to the recommendations:

Recommendations 1 and 2: The SBA agrees. The SBA will endeavor to improve its System Development Methodology (SDM) and underlying principles, to include testing for core application functionality

Recommendation 3: The SBA believes that the exigent circumstances caused by the COVID-19 pandemic, reinforced by legislative requirements, did not permit sufficient time for such a formalized third-party audit as recommended. The SBA further believes that this condition has been overcome by events.

Recommendation 4: The SBA agrees. The SBA will consider updates to its mandatory cybersecurity language for IT acquisitions.

Recommendation 5: The SBA agrees. The SBA is in the process of establishing more granular and more frequent interfacing with the ERM Board with regard to privacy and cybersecurity risk.

Recommendation 6: The SBA does not agree. The SBA believes that there is not always a cause-effect relationship, as is inferred from the draft report, between the risk management and assessment activities conducted on a particular IT environment, and the subsequent improper use of that same IT environment after authorization.



U.S. Small Business
Administration

Recommendation 7: The SBA does not agree. The SBA feels that the specific type of authorization received by a particular IT environment, point-in-time authorization or ongoing authorization, was not a factor in the use or misuse of the SBA's pandemic response IT systems implementations.

Recommendation 8 and 9: The SBA agrees; however, the SBA believes that these conditions have been overcome by events.

Recommendation 10: The SBA agrees. The SBA will evaluate options for automating its change management process for IT systems and applications.