



IT MODERNIZATION

SBA Urgently Needs to Address Risks on Newly Deployed System

Report to the Ranking Member, Committee on Small Business, House of Representatives

November 2024
GAO-25-106963
United States Government Accountability Office

Accessible Version

GAO Highlights

View [GAO-25-106963](#). For more information, contact Carol C. Harris at (202) 512-4456 or HarrisCC@gao.gov, or Courtney LaFountain at (202) 512-5463 or LaFountainC@gao.gov.

Highlights of [GAO-25-106963](#), a report to the Ranking Member, Committee on Small Business, House of Representatives

November 2024

IT MODERNIZATION

SBA Urgently Needs to Address Risks on Newly Deployed System

Why GAO Did This Study

In fiscal year 2023, the federal government awarded \$178.6 billion in contracts to small businesses. SBA promotes small business participation in federal contracting through a variety of contracting assistance programs. These programs rely on multiple IT systems. However, SBA's past attempts to modernize its IT systems experienced challenges and did not deliver expected results.

GAO was asked to review SBA's Unified Certification Platform project. This report (1) describes the project's plans and status, and (2) evaluates the extent SBA has adopted leading practices for risk management, cybersecurity, and schedule and cost estimation for the project. To do so, GAO summarized and analyzed relevant documentation and compared SBA's risk management, cybersecurity, and schedule and cost estimation efforts to leading practices. GAO also interviewed SBA officials.

What GAO Recommends

GAO is making fourteen recommendations to SBA, including that it should (1) expeditiously address critical risk management issues, (2) expeditiously address critical cybersecurity issues, and (3) consider the probability and impact of accepted risks if deciding to issue a final authorization to operate the system. SBA concurred with three, partially concurred with three, and did not concur with eight recommendations. GAO maintains that the recommendations are warranted.

What GAO Found

In 2023, the Small Business Administration (SBA) started the Unified Certification Platform project. This project is intended to allow small businesses to more efficiently apply for and maintain certifications to SBA's contracting assistance programs, compared to legacy certification systems.

SBA originally anticipated deploying the system in September 2024. In June 2024, SBA announced a pause, effective August 1, 2024, in accepting new applications for certification. GAO expressed concerns regarding the agency's pause in accepting new applications until the certification system is deployed. GAO also noted that SBA triggered questions about risks and available mitigation strategies if full deployment did not occur in September or if there were system performance issues after deployment. The risk of a deployment delay was eventually realized, as SBA delayed UCP deployment to address system issues identified during testing. SBA subsequently deployed the UCP system on October 18, 2024, but work remains to develop additional, more complex functionality, secure the system, and migrate data.

GAO's analyses of SBA's efforts show that leading practices for risk management, cybersecurity, and schedule and cost estimation have not been fully implemented. Accordingly, SBA faces an increased risk of additional delays as it completes remaining work and may face challenges with addressing system issues that arise.

Extent to Which the Small Business Administration (SBA) Met Selected IT Management Areas for the Unified Certification Platform Modernization

IT management area	Overall assessment
Risk Management	Minimally met
Cybersecurity	Partially met
Schedule	Not met
Cost	Minimally met

Source: GAO analysis of SBA data. | GAO-25-106963

GAO identified critical management gaps:

- SBA did not have a project level risk management strategy, a risk mitigation plan, and did not fully identify and document risks.
- SBA did not document plans for managing cybersecurity risks or conduct a traceability analysis to ensure project security requirements had been met. This increases the likelihood of a successful cyberattack.

Further, the project’s schedule and cost estimates were unreliable. SBA did not create an integrated master schedule; instead, it used a “road map” that did not meet the characteristics of a reliable schedule. SBA’s cost estimate largely relied on subject matter expertise instead of supporting data or methodologies.

SBA issued an interim authority to operate for the system in August 2024 while it continues to implement IT security controls. Under schedule pressure, SBA could decide to accept known risks and issue a final authorization to operate with issues not being fully resolved. If taking such an action, consideration of the probability and resulting impact of accepted risks is essential.

Contents

GAO Highlights	ii
Why GAO Did This Study	ii
What GAO Recommends	ii
What GAO Found	ii

Letter	1
Background	2
SBA Unified Certification Platform to Address Shortcomings with Certification Systems; Work is Ongoing Post-Deployment	9
SBA Has Not Fully Implemented Selected Leading IT Management Practices and Faces Increased Risks	13
Conclusions	27
Recommendations for Executive Action	27
Agency Comments and Our Evaluation	29

Appendix I	Objectives, Scope, and Methodology	32
Appendix II	SBA UCP Project Cost Estimate Compared to Leading Practices	35
Appendix III	Comments from the Small Business Administration	37
Appendix IV	GAO Contacts and Staff Acknowledgments	55

Tables	
Extent to Which the Small Business Administration (SBA) Met Selected IT Management Areas for the Unified Certification Platform Modernization	iii
Table 1: Examples of Small Business Administration (SBA) Contracting Assistance Program Reporting	5
Table 2: Unified Certification Platform (UCP) Planned Cost, as of October 2024	12
Table 3: Implementation Status of the Small Business Administration’s (SBA) Unified Certification Platform Project, as of October 2024	13
Table 4: Analysis of the Small Business Administration’s (SBA) Implementation of Selected Leading Risk Management Practices for the Unified Certification Platform (UCP) Project, as of October 2024	15
Table 5: Extent to Which the Small Business Administration (SBA) Adopted Selected Leading Cybersecurity Practices for the Unified Certification Platform (UCP) Project, as of October 2024	19
Table 6: Assessment of Small Business Administration (SBA) Unified Certification Platform (UCP) May 2023 Cost Estimate Compared to Cost Estimating Leading Practices, as of October 2024	24
Table 7: Assessment of the Unified Certification Platform (UCP) Cost Estimate Compared to Leading Practices, as of October 2024	35

Figures

Figure 1: Simplified Overview of the Small Business Administration's (SBA) Contracting Assistance Program Certification Process 4

Figure 2: Examples of Intended Functions of the Small Business Administration's (SBA) Unified Certification Platform (UCP) 11

Abbreviations

- BTIC: Business Technology Investment Council
- CMMI: Capability Maturity Model Integration
- HUBZone: Historically Underutilized Business Zone
- NIST: National Institute of Standards and Technology
- CIO: Chief Information Officer
- OIG: Office of Inspector General
- SBA: Small Business Administration
- UCP: Unified Certification Platform
- VetCert: Veteran Small Business Certification Program
- WOSB: Women-Owned Small Business
- WBS: work breakdown structure

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



November 6, 2024

The Honorable Nydia Velázquez
Ranking Member
Committee on Small Business
House of Representatives
Dear Ms. Velázquez,

The Small Business Administration (SBA) administers contracting assistance programs and promotes small business participation in federal contracting through a variety of programs. In fiscal year 2023, the federal government awarded \$178.6 billion in federal procurement opportunities to small businesses. Approximately \$156.5 billion of those contracting dollars was awarded to small businesses that were disadvantaged, women-owned, service-disabled veteran-owned, or located in historically underutilized business zones.¹

To certify small businesses for eligibility in its contracting assistance programs, SBA relies on multiple IT systems. We and SBA’s Office of Inspector General (OIG) have previously reported that these systems have shortcomings, including issues with reconciling data between systems and limitations in promised functionality.²

To help address these shortcomings, in 2023, SBA initiated the Unified Certification Platform (UCP) modernization project. The UCP project is intended to deploy a new system to allow small businesses to more efficiently apply for and maintain certifications to SBA’s contracting assistance programs.

You asked us to review SBA’s UCP project. Our specific objectives were to (1) describe SBA’s plans for the UCP project and the status of its efforts; and (2) determine to what extent the UCP project has adopted leading IT management practices for risk management, cybersecurity, and schedule and cost estimation.

To address our first objective, we reviewed and summarized relevant UCP project information, such as acquisition plans, solicitation documents, monthly meeting minutes, and schedule and cost documentation. We also interviewed agency officials to verify SBA’s plans for its modernization effort and its current status.

To address our second objective, we assessed the UCP project’s practices for managing risks, cybersecurity, and schedule and cost estimation against selected leading practices. Specifically,

- We selected seven leading practices associated with risk management in ISACA’s Capability Maturity Model Integration (CMMI).³ We then evaluated the UCP project’s documentation, such as risk registers and quality assurance plans, and SBA policies against the selected practices.

¹Government-Wide Performance FY2023 Small Business Procurement Scorecard, available at <https://www.sba.gov/agency-scorecards/scorecard.html?agency=GW&year=2023>.

²GAO, *Small Business Administration: Recent Changes to the 8(a) Program’s Financial Thresholds Need Evaluation*, GAO-22-104512. (Washington, D.C.: Aug 30, 2022); Small Business Administration, Office of Inspector General, *Evaluation of Certify.SBA.Gov*, 20-17 (Washington, D.C.: Jul. 30, 2020).

³ISACA, *CMMI Model V3.0* (Pittsburgh, PA: Apr. 6, 2023). CMMI Model and ISACA© [2021] All rights reserved. Used with permission.

- We selected five leading practices that represented key elements for addressing cybersecurity requirements and needs in an acquisition from the National Institute of Standards and Technology's (NIST) guidance on *Engineering Trustworthy Secure Systems*.⁴ We then evaluated the UCP project's documentation, such as the UCP acquisition plan and performance work statement, against the selected NIST guidance.
- We reviewed documentation supporting SBA's schedule and cost estimates for the UCP project. Specifically, we assessed SBA's efforts to establish a project schedule against leading practices for developing a comprehensive, well-constructed, credible, and controlled schedule, as identified in GAO's *Schedule Assessment Guide*.⁵ In addition, we evaluated documentation supporting the project's cost estimate against the leading practices for developing a comprehensive, accurate, well documented, and credible cost estimate identified in GAO's *Cost Estimating and Assessment Guide*.⁶

For both objectives, we interviewed cognizant agency officials in SBA's Office of Government Contracting and Business Development, as well as SBA's Office of the Chief Information Officer to obtain their views and verify the information provided. Additional details on our objectives, scope, and methodology are provided in appendix I.

We conducted this performance audit from July 2023 to November 2024 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.

Background

SBA was created in 1953 as an independent agency of the federal government with a mission to aid small businesses, preserve free and competitive enterprise, and maintain and strengthen the overall economy of our nation. The agency's Office of Government Contracting and Business Development is responsible for promoting small business participation in federal contracting. The office administers several contracting assistance programs that, among other things, facilitate contract set-asides (i.e. government contracts with competition limited to small businesses in general or those that meet specific eligibility requirements), including the following programs:

- **8(a) Business Development** assists small businesses owned and controlled by socially and economically disadvantaged individuals and entities. The program provides up to 9 years of developmental support, such as business counseling and mentoring, contracting guidance, and access to capital. The program also sets aside federal contracting opportunities for program participants.

⁴National Institute of Standards and Technology, *Engineering Trustworthy Secure Systems*, Special Publication 800-160, Volume 1, Revision 1 (Gaithersburg, Md.: Nov. 16, 2022).

⁵GAO, *Schedule Assessment Guide: Best Practices for Project Schedules*, [GAO-16-89G](#) (Washington, D.C.: Dec. 22, 2015).

⁶GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, [GAO-20-195G](#) (Washington, D.C.: Mar. 12, 2020).

- **Women-Owned Small Business (WOSB)** provides greater access to federal contracting opportunities for women-owned small businesses. Through this program, contracting officers can set aside contracts for eligible WOSBs and economically-disadvantaged women-owned businesses.
- **Historically Underutilized Business Zone (HUBZone)** provides small businesses located in economically distressed areas access to federal contracting set-aside opportunities to promote economic development.
- **Veteran Small Business Certification Program (VetCert)** allows veteran-owned and service-disabled veteran-owned small businesses to compete for federal set-aside contracts.⁷

SBA's Certification Process and Systems for Contracting Assistance Programs

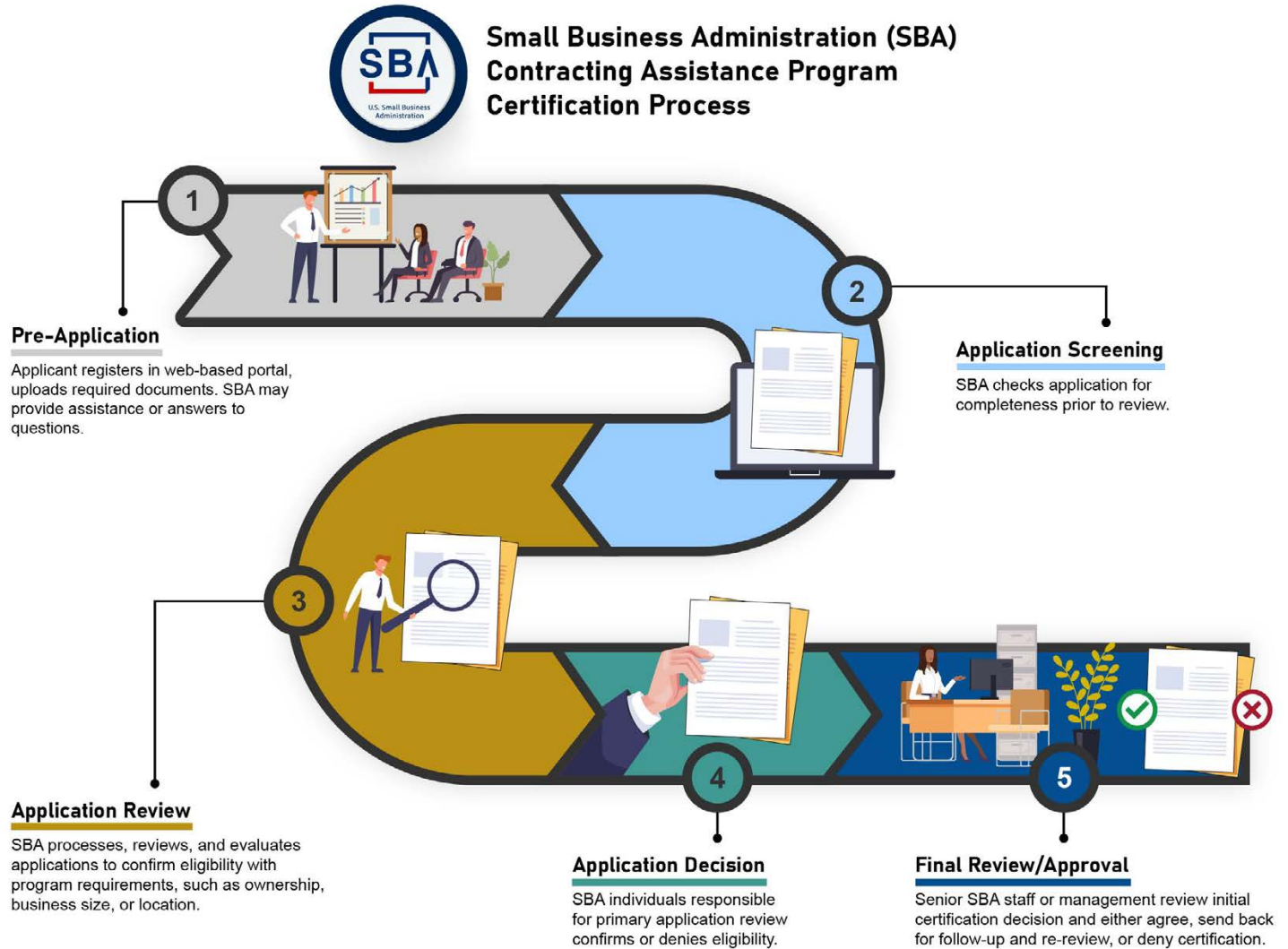
According to SBA, the general initial certification process for the 8(a), WOSB, HUBZone and VetCert programs include a pre-application phase where the applicant registers and uploads required documents to an online portal. During this phase, SBA may provide assistance or answers to questions from prospective applicants. Subsequent phases are;

- an application screening step where SBA staff or contractor support staff check submitted applications for completeness before full review;
- a document processing, application evaluation, and fact review step to confirm eligibility and other program requirements;
- a certification decision recommendation by individuals responsible for the primary review; and
- a final certification review/approval.

Figure 1 provides an overview of SBA's contracting assistance program certification process.

⁷The National Defense Authorization Act for Fiscal Year 2021 provided for the transfer to SBA of the veteran-owned and service-disabled veteran owned small business certification process from the Department of Veterans Affairs. Pub. L. No. 116-283, § 862, 134 Stat. 3388, 3776-3784. In January 2023, SBA began accepting applications to certify new veteran-owned small businesses through its VetCert program. Existing veteran-owned small businesses that were already certified by the Department of Veterans Affairs as of January 1, 2023, were granted a one-time, one-year extension by SBA. Prior to the 2021 act, veteran-owned small businesses would self-certify using the VetCert portal at veterans.certify.sba.gov. The portal allows participants to check their eligibility, apply for certification or re-certify their businesses, access checklists and guides, and search for certified veteran-owned firms.

Figure 1: Simplified Overview of the Small Business Administration’s (SBA) Contracting Assistance Program Certification Process



Sources: GAO analysis of SBA documentation; SBA (logo); Irina/stock.adobe.com (illustrations); TriMaker/stock.adobe.com (colored arrows illustration). | GAO-25-106963

Note: The certification process for some of the contracting assistance programs differ from the general approach depicted above. For example, the Women-Owned Small Business program allows approved third-party certifiers to review applications and make eligibility determinations, subject to SBA oversight. See, e.g., 13 C.F.R. §§ 127.350-356. The 8(a) program also includes a secondary review of the certification decision for applicants.

SBA also produces various reports associated with its contracting assistance programs. Table 1 provides a description of each program’s reporting.

Table 1: Examples of Small Business Administration (SBA) Contracting Assistance Program Reporting

Program	Reporting summary
8(a) Business Development	Section 408 of the Business Opportunity Development Reform Act of 1988 requires SBA to develop and implement a process for the systematic collection of data on the 8(a) program. ^a The act also requires SBA to submit an annual report to Congress with information on the program’s costs and benefits, the dollar amount of contracts awarded, and the status of businesses exiting the program, among other things. In addition to this annual report, SBA reports metrics for this program as part of its agencywide annual performance report.
Women-Owned Small Business	SBA reports metrics for this program as part of its agencywide annual performance report.
Historically-Underutilized Business Zone	Section 31 of the Small Business Act as amended requires SBA to annually report performance metrics and program data. ^b In addition, SBA reports metrics for this program as part of its agencywide annual performance report.
Veteran Small Business Certification	SBA reports metrics for this program as part of its agencywide annual performance report.

Source: GAO analysis of SBA documentation. | GAO-25-106963

^aPub. L. No. 100-656, § 408, 102 Stat. 3853, 3877-78 (codified at 15 U.S.C. § 636j(16)).

^b15 U.S.C. § 657a(e).

Each of SBA’s contracting assistance programs are supported by different IT systems. These IT systems use different computer languages, are located on various platforms, and are hosted in cloud computing environments using various technology providers.⁸ According to SBA, in fiscal year 2023, the agency reported spending approximately \$10.86 million to operate and maintain the IT systems environment supporting its contracting assistance programs.

Overview of Leading Practices for IT Modernization

We, ISACA, and NIST have identified leading practices and guidance to assist in ensuring the effective management of IT modernization initiatives. These include the following:

- **Risk management.** ISACA’s CMMI provides guidance for improving an organization’s capabilities and performance when developing or acquiring solutions, including hardware and software, and their related components. ISACA’s CMMI Model Version 3.0, published in April 2023, includes practices to help organizations manage potential risks and reduce the chance of adverse impacts on meeting objectives, among other areas.
- **Cybersecurity.** NIST has issued a suite of information security standards and guidelines that, collectively, provide comprehensive guidance on managing cybersecurity risk to agencies. For example, NIST’s guidance on engineering trustworthy secure systems establishes leading practices for agencies to follow in developing new systems or updating legacy systems.⁹ The guidance is intended to address security issues from a perspective of stakeholder requirements and protection needs and to use established processes to ensure that such requirements and needs are addressed with the appropriate rigor across the life cycle of

⁸According to the National Institute of Standards and Technology (NIST), cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned and released.

⁹National Institute of Standards and Technology, *Engineering Trustworthy Secure Systems*, Special Publication 800-160, Volume 1, Revision 1 (Gaithersburg, Md.: Nov. 16, 2022).

the system. By following the guidelines, agencies can better ensure that the security requirements of the system are defined, among other things.

- **Schedule estimation.** GAO's *Schedule Assessment Guide* presents 10 leading practices for scheduling.¹⁰ Leading practices within this guide show that a well-planned schedule is a fundamental management tool that can help government programs use public funds effectively by specifying when to perform work in the future and measuring program performance against an approved plan. An integrated and reliable schedule can show when major events are expected as well as the completion dates for all activities leading up to them, which can help determine if the program's parameters are realistic and achievable.
- **Cost estimation.** GAO's *Cost Estimating and Assessment Guide* establishes a consistent methodology based on 18 leading practices that can be used across the federal government for developing, managing, and evaluating program cost estimates for acquisitions and development efforts.¹¹ GAO grouped leading practices into the four characteristics of a reliable cost estimate—comprehensive, well-documented, accurate, and credible. The guidance considers an estimate reliable if it substantially or fully meets each of the characteristics of a reliable cost estimate.

GAO and OIG Reports Found Longstanding Challenges with SBA's Prior IT Systems Modernizations, Reporting, and IT Management

Prior IT System Modernizations for Contracting Assistance Programs

From 2011 through 2019, SBA initiated several projects to modernize the IT systems used for its contracting assistance programs but has faced longstanding challenges.

- **OneTrack.** In 2011, SBA began a \$1.9 million contract to develop an IT system, OneTrack, which was intended to improve, streamline, automate, and unify business processes for the 8(a) and HUBZone programs. The intent was to create one portal for businesses to use for the programs, and to provide SBA staff with a shared database of program data to improve productivity and enhance monitoring and reporting capabilities. However, the SBA OIG found in 2014 that the system did not achieve the intended capabilities because the development process did not complete the necessary market research for the project, did not use modular contracting principles, did not maintain contract documentation, and did not monitor or mitigate project risks.¹²

In 2015 we also reported that SBA experienced problems implementing the OneTrack system.¹³ SBA ultimately decided not to deploy the system and instead began development of another replacement IT system.

¹⁰[GAO-16-89G](#).

¹¹[GAO-20-195G](#).

¹²Small Business Administration, Office of Inspector General, *The SBA Did Not Follow Federal Regulations and Guidance in the Acquisition of the OneTrack System*, 14-10 (Washington, D.C.: Feb. 12, 2014).

¹³GAO, *Small Business Administration: Leadership Attention Needed to Overcome Management Challenges*, [GAO-15-347](#) (Washington, D.C.: Sept. 22, 2015). The report made eight recommendations designed, among other things, to improve SBA's oversight of IT investments. SBA implemented all of our recommendations.

- **Certify.sba.gov.** In 2015, SBA approved a contract for Certify.sba.gov, which—like OneTrack—was intended to improve the 8(a), HUBZone, and WOSB programs by creating a single gateway for participating businesses. Certify.sba.gov would also increase efficiency for processing and reviewing applications and enable SBA to report on and analyze the agency’s impact on small businesses. However, from 2015 through 2019, the SBA OIG found that the system’s technical architecture would not meet the needs of 8(a) and HUBZone program processes.¹⁴ In addition, the system was missing critical features such as the ability to prescreen applications and key analytical tools to improve review capabilities. These issues created delays, backlogs, and reliance on manual workarounds.

SBA ultimately stopped development of Certify.sba.gov in 2019 when it was determined that the platform was unsustainable in the long-term due to maintenance and updates required for the open-source platform, and security vulnerabilities were difficult to address. The agency reported to the Office of Management and Budget that the cost for the Certify.sba.gov system between 2015 and 2019 exceeded \$30 million.

- **Beta.Certify.sba.gov.** In 2019, SBA approved plans to redesign Certify.sba.gov on a new platform, called beta.Certify.sba.gov, at a cost of \$3.5 million. Like the original Certify.sba.gov platform, the initial intent of beta.Certify.sba.gov was to unify 8(a), WOSB, and HUBZone under one system and to facilitate improved user experience for applicants as well as to enhance electronic reviews and tracking by SBA staff. Additionally, the platform was intended as a replacement for other obsolete tools, such as business search tools, among other things. According to SBA, the scope of the effort was reduced to provide a platform solely for the WOSB program, and 8(a) and HUBZone remained in their legacy systems. Beta.Certify.sba.gov was launched in 2020 as the WOSB system of record. Subsequently, in a September 2022 report, the SBA OIG found that beta.Certify.sba.gov did not contain accurate WOSB information and was undergoing fixes as program officials discovered issues.¹⁵

Challenges with Contract Assistance Program Reporting

SBA has also faced challenges in meeting the contracting program reporting requirements previously discussed. These challenges were due, in part, to shortcomings in its IT systems. Specifically, we reported in 2022 that SBA identified a number of challenges that led to a delay in required 8(a) program reporting, including

- manual data collection and aggregation processes, such as data on firm owners saved in individual spreadsheets maintained by different analysts;
- IT issues, such as reconciling data between prior IT systems and new systems; and
- limited functionality of the current Certify.sba.gov system, such as the inability to monitoring the business development of 8(a) participants.¹⁶

¹⁴Small Business Administration, Office of Inspector General, *Evaluation of Certify.SBA.Gov*, 20-17 (Washington, D.C.: Jul. 30, 2020).

¹⁵Small Business Administration, Office of Inspector General, *SBA’s Implementation of the Women-Owned Small Business Certification Program*, 22-20 (Washington, D.C.: Sept. 29, 2022). In the September 2022 report the OIG recommended that SBA mitigate or remedy the beta.Certify.sba.gov issues affecting data accuracy. SBA disagreed with the recommendation, stating that SBA already had procedures and guidance in place to identify and address system issues. The OIG noted that those procedures and guidance did not catch the data issues uncovered in the OIG report and that SBA did not provide any information that improvements had been made to address the issues the OIG identified.

¹⁶[GAO-22-104512](#).

We recommended that, among other things, SBA assess the process to systematically collect data and develop a report on the 8(a) program in light of delay-causing challenges. We recommended that the agency identify potential operational efficiencies and develop a plan to assess report delays, such as revising procedures or developing time frames as needed. SBA agreed with this recommendation and has taken steps to address it. In March 2024, SBA stated that the agency had assessed the 8(a) program reporting process to develop revisions that reduce or eliminate reporting delays. As of July 2024, SBA had published the 2023 fiscal year 8(a) program report, however, the agency has not yet published program reports for fiscal years 2019-2022. We will continue to monitor SBA's progress in implementing this recommendation.

Challenges with IT Management

We and the SBA OIG have previously reported on SBA's IT management issues. These included, among other things, a governance board that did not meet to oversee IT investments, not reporting investment performance against established baselines, and not taking corrective actions for underperforming investments.

- In 2015, we reported that, although SBA had taken steps to implement aspects of several key IT management initiatives for managing its IT acquisitions and operations, the agency had not fully completed all of them.¹⁷ For example, the agency had not developed a policy for conducting regular operational analyses of all of its IT investments. We made eight recommendations to SBA, including to improve its IT investment oversight by ensuring that investments are continuing to meet business and customer needs and agency strategic goals. SBA took action to implement all eight of our recommendations.
- In 2017 the OIG found that although SBA had made significant progress improving its oversight of IT investments, the agency had not fully implemented OMB guidance. For example, SBA had not conducted regular reviews of its IT investments and there were IT control issues with SBA's handling of several projects, including Certify.sba.gov.¹⁸ The OIG made six recommendations to SBA, including that SBA ensure that its Business Technology Investment Council (BTIC) sessions review and track all IT investment baselines.¹⁹ The OIG also recommended that the SBA Chief Information Officer (CIO) measure and report on IT project performance against baselines and use updated system development policies that address cloud and agile development, among others. SBA agreed with the recommendations and took actions to address them. For example, in November 2017, SBA's OIG reported that the CIO incorporated all performance baselines for IT investments into BTIC session agendas and ensured that any changes to those performance baselines followed an agency established review process.
- In 2024, the SBA OIG reported that SBA had significant IT investment internal control issues as a result of not having an effective IT governance framework in place.²⁰ For example, SBA's BTIC did not meet regularly to review and evaluate IT investments through their business cases and baselines which consider cost, performance goals, scope, and schedule. In addition, those investments did not have an independent

¹⁷GAO-15-347.

¹⁸Small Business Administration, Office of Inspector General, *Review of SBA's Implementation of the Federal Information Technology Acquisition Reform Act*, 18-06 (Washington, D.C.: Nov. 28, 2017).

¹⁹The Business Technology Investment Council (BTIC) is the agency's principal governance body that oversees the selection, control, and evaluation of SBA's major IT investments.

²⁰Small Business Administration, Office of Inspector General, *SBA's IT Investment Governance Framework*, 24-10 (Washington, D.C.: Mar. 29, 2024).

cost and performance assessment with approvals from the architecture review board and the BTIC.²¹ Further, the OIG also found that business cases were not completed for the investments they sampled. The OIG recommended that SBA ensure that (1) it reviews new investments to confirm compatibility with existing systems, (2) the BTIC approves new investments prior to purchase, and (3) program offices create business cases prior to approval of the investment, as required by SBA policies. SBA agreed with these recommendations.

The OIG also found that SBA did not effectively monitor major IT investments as the projects were being developed to ensure that they continued to meet mission needs at the expected levels of cost and risk and take corrective action if needed. SBA policy requires earned value principles to be used to plan and manage the development activities for major IT investments.²² According to that policy earned value methods should at a minimum, track schedules, incurred costs, and estimates to complete the project. The OIG recommended that the agency update procedures to provide specific guidance on how to use earned value principles to measure investment progress against the approved performance measurement baseline²³ and the original performance measurement baseline²⁴ for all major investments. SBA partially agreed with the recommendation and noted that agency investment managers plan to use earned business value principles to measure investment progress and the agency plans to update its procedures.

SBA Unified Certification Platform to Address Shortcomings with Certification Systems; Work is Ongoing Post-Deployment

SBA initiated the UCP modernization project to help address shortcomings with the systems supporting the certification of small businesses for its contracting assistance programs. According to SBA officials and a 2022 third-party evaluation by the MITRE Corporation, these systems have shortcomings that have led to inefficiencies.²⁵ For example, MITRE's evaluation noted that SBA's certification systems do not interface with each other and the manual process of extracting firm data from multiple databases and storing it in spreadsheets for analysis is time-consuming, inefficient, and inconsistent.

Further, a business applying to multiple programs must have a login for each program and repeatedly upload the same documents to each system. According to SBA officials, an estimated 40 percent of certified small businesses are eligible for multiple certifications; however, many forego additional certifications because the different application processes are administratively burdensome and complicated. Additionally, SBA staff

²¹SBA's architecture review board supports the process of researching, investing, architecting, and implementing IT capabilities and services. The board establishes adequate governance to ensure SBA investments conform to an overarching SBA IT system design.

²²Earned Value Management is a technique to measure program and project performance, allowing PMs and investment managers to reduce program or project risk.

²³A documented baseline approved by the BTIC, along with any approved changes to cost, schedule, or scope from the original baseline.

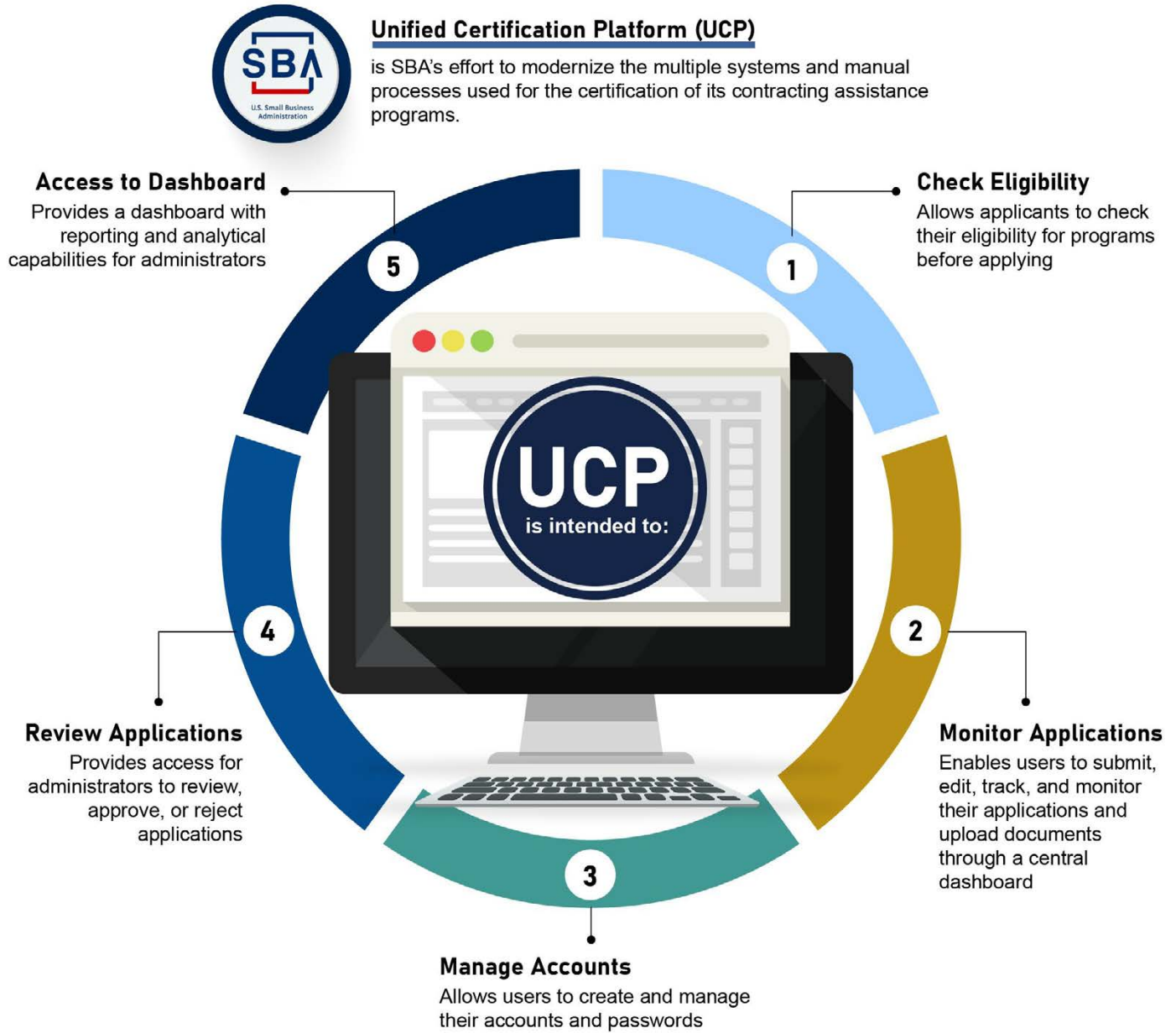
²⁴The original baseline is the baseline approved by the BTIC prior to the addition of the investment to SBA's IT portfolio and submission within the official budget. This baseline includes a cost, schedule, and scope baseline.

²⁵The MITRE Corporation is a not-for-profit organization chartered to work in the public interest with expertise in system engineering, IT, and enterprise modernization.

sometimes rely on manual processes and spreadsheets for accessing data from these systems. As a result, it can be difficult for SBA staff to leverage data and documents in or across the different systems for analysis.

According to SBA, the UCP project is intended to develop an IT system to streamline and enhance the administration of the 8(a), HUBZone, VetCert, and WOSB programs. With UCP, SBA plans to improve the certification and recertification process for firms by providing a single software solution for all of SBA's contracting assistance programs. The UCP project was approved by SBA's BTIC in March 2024. SBA's Office of Government Contracting and Business Development, in conjunction with the Office of the CIO, is managing the project. Figure 2 describes the functions SBA plans to provide with the UCP system.

Figure 2: Examples of Intended Functions of the Small Business Administration's (SBA) Unified Certification Platform (UCP)



Sources: GAO analysis of SBA documentation; SBA (logo); Vladwel/stock.adobe.com (desktop illustration); Iryna/stock.adobe.com (colored circle illustration). | GAO-25-106963

To develop the UCP system, SBA issued two contracts that, in total, include a 12-month base period beginning in September 2023 followed by two 3-month option periods beginning in September 2024 and December 2024, respectively, and a final 12 -month option period beginning in March 2025.²⁶

According to SBA, the UCP system is expected to cost \$19.14 million for the entire 30-month period. This cost figure includes \$13.5 million for the contract base period, and \$5.64 million for the option periods. However, SBA did not provide the total lifecycle costs of the UCP system. This issue is discussed later in the report. As of October 2024, SBA stated that it had spent approximately \$14.2 million on UCP. See table 2 for an overview of the planned costs for UCP.

Table 2: Unified Certification Platform (UCP) Planned Cost, as of October 2024

Contract period	Dates	Cost (in millions)
Base period (12 months)	September 2023 – September 2024	\$13.50
Additional development and operations and maintenance contract option (3 months)	September 2024 – December 2024	\$1.09
Additional development and operations and maintenance contract option (3 months)	December 2024 – March 2025	\$1.09
Operation and maintenance contract option (12 months)	March 2025 – March 2026	\$3.46
Total		\$19.14

Source: GAO analysis of Small Business Administration documentation. | GAO-25-106963

SBA is implementing UCP using an Agile incremental development approach with two-week development cycles that are intended to result in deployable working software.²⁷ The program manager holds planning sessions with stakeholders prior to the start of the development of the next system release or sprint, as well as review sessions at the end of each release or sprint to evaluate the work produced.

SBA faced a delay in deploying the UCP system. Based on SBA’s July 2024 product road map, the agency initially planned to deploy the UCP system in September 2024.²⁸ According to SBA officials, the agency delayed the deployment of UCP to address system issues identified during testing.

SBA subsequently deployed the UCP system on October 18, 2024, but work remains to develop additional, more complex functionality.²⁹ For example, although small businesses starting new certification applications

²⁶The development, implementation, and operations and maintenance for UCP were split into two concurrent contracts, UCP I and UCP II. The UCP I contract is for the development, implementation, and post-deployment operations and maintenance of technology solutions for the HUBZone, WOSB and the VetCert programs, including certification decisions, certification servicing, oversight, and re-certification functions, associated reporting, websites, and training. The second contract for UCP II is for the development, implementation, and post-deployment operations and maintenance of technology solutions for the 8(a) field functions, including certification servicing and oversight functions, associated reporting, websites, and training, among other things. The 8(a) field functions are SBA’s 68 field offices who oversee and engage with 8A firms.

²⁷Agile software development approach emphasizes early and continuous software delivery, with development broken into iterations called sprints. Each set of sprints is compiled into deployable working software, referred to as a release. Agile uses collaborative teams, and measures progress with working software. GAO, *GAO Agile Assessment Guide: Best Practices for Adoption and Implementation*, [GAO-24-105506](#) (Washington, D.C.: Dec. 15, 2023).

²⁸According to GAO’s Agile Assessment Guide, a product road map is a management plan where capabilities or features for development are laid out in a timeline and planned for future iterations. [GAO-24-105506](#).

²⁹We did not evaluate the performance of the UCP system.

can use the UCP system, those businesses that are managing existing certifications still need to use other systems. As of October 2024, SBA was in the process of performing data migration from prior systems, which is a necessary step to allow the new system to manage existing certifications. SBA was also working to develop additional functionality to enable small businesses to manage existing certifications using the new UCP system. Lastly, SBA was still implementing system security controls, as discussed later in this report. See table 3 for a description of the UCP project activities and their statuses.

Table 3: Implementation Status of the Small Business Administration’s (SBA) Unified Certification Platform Project, as of October 2024

Activity	Start date	Original estimated completion date	Status
Initiate contract	9/2023	9/2023	Completed
Develop user, business, and system requirements	11/2023	12/2023	Completed
Create a product road map ^a for the system development	12/2023	1/2024	Completed
System Development	3/2024	8/2024	In progress
Data migration	4/2024	3/2025	In progress ^b
System deployment	9/2024	9/2024	Delayed, then completed ^c
Additional development, operations, and maintenance (3-month contract option)	9/2024	12/2024	In progress
Additional development, operations, and maintenance (additional 3-month contract option)	12/2024	3/2025	Not started
Operations and maintenance (12 months)	3/2025	4/2026	Not started

Source: GAO analysis of SBA documentation. | GAO-25-106963

^aAccording to GAO’s Agile Assessment Guide, a product road map is a management plan where capabilities or features for development are laid out in a timeline and planned for future iterations. GAO, GAO Agile Assessment Guide: Best Practices for Adoption and Implementation, [GAO-24-105506](#) (Washington, D.C.: Dec. 15, 2023).

^bSBA officials reported that data essential to the system’s functionality will be migrated first and that data migration is expected to continue after deployment.

^cSBA deployed the UCP system on October 18, 2024, but additional work remains to develop additional functionality, secure the system, and migrate data.

SBA Has Not Fully Implemented Selected Leading IT Management Practices and Faces Increased Risks

SBA has not fully implemented leading IT management practices in the planning and implementation of the UCP modernization project. Specifically, SBA partially implemented leading practices related to identifying and managing risks, and cybersecurity. In addition, SBA did not develop an integrated master schedule for the project, and the agency’s cost estimate for UCP was unreliable.

As mentioned previously, SBA deployed the UCP system, but work remains to develop additional, more complex functionality, secure the system, and migrate data. Critical management gaps, including a lack of project-level risk management strategy, risk mitigation plan, and cybersecurity risk management plan increase the risk of additional delays. As SBA completes remaining work, it will increasingly be more difficult to quickly or effectively deal with issues that arise.

SBA Did Not Fully Implement Selected Leading Practices for Identifying and Managing Risks

According to the CMMI model, an effective risk management process identifies potential problems before they occur, so that risk-handling activities may be planned and invoked, as needed, across the life of the project to mitigate adverse impacts on achieving objectives.³⁰ In addition, the model also indicates that risk identification should consider topics such as work tasks, objectives or requirements, technology, staffing, funding, performance, and regulatory constraints, among other things.

Specifically, effective risk management practices at both the organizational and project levels include seven selected leading practices.

1. Determine risk sources and categories such as work activities, resources, regulations and laws, and management or technical uncertainties).
2. Define parameters to analyze and categorize risks such as the severity of risk, likelihood of occurrence, and impact or consequences.
3. Establish and maintain a risk management strategy. That includes potential mitigation techniques and defining when a risk becomes unacceptable to trigger the execution of a mitigation plan. It also includes consideration of the costs and benefits of implementing risk mitigation plans for key risks.
4. Identify and document risks throughout all phases of the development lifecycle, for example, a document that identifies and records risks, including details about context, conditions, and consequences.
5. Evaluate and categorize each identified risk using defined risk categories and parameters and determine its relative priority.
6. Develop a risk mitigation plan in accordance with the risk management strategy. That includes a determination of the thresholds that define when a risk becomes unacceptable and triggers the execution of a risk mitigation plan. It also includes the costs and benefits of implementing the risk mitigation plan for key risks.
7. Monitor the status of each risk periodically and implement the risk mitigation plan as appropriate, to include resource commitments and the schedules for each risk-handling activity.

SBA partially met five and did not meet two of seven selected leading practices for risk management. Table 4 lists these practices and provides our assessment of the UCP project's implementation of the practices, as of October 2024.

³⁰ISACA, *Capability Maturity Model Integration, Version 3.0* (Schaumburg, IL: April 2023). CMMI Model and ISACA© [2021] All rights reserved. Used with permission.

Table 4: Analysis of the Small Business Administration’s (SBA) Implementation of Selected Leading Risk Management Practices for the Unified Certification Platform (UCP) Project, as of October 2024

Leading practice	Assessment	Description of assessment
Determine risk sources and categories	partially met	<p>SBA’s enterprise risk management framework, which describes SBA’s high-level approach to risk across the agency, includes information on the different risk categories and descriptions, for use in risk management at various levels.</p> <p>The UCP business requirements document, which lays out the goals and requirements for the UCP project, includes a section that identifies various categories of risks along with short descriptions.</p> <p>As part of the risk determination process, SBA’s IT program manager meets weekly with developers, SBA stakeholders, and SBA management.</p> <p>Additionally, project leadership meets monthly to discuss risks to project objectives, among other things like resources, backlog, and quality assurance metrics.</p> <p>SBA identifies and tracks risks to the UCP development process using a risk register. The UCP risk register includes columns that describe and categorize risks. As of February 2024, SBA identified and categorized eight risks, such as potential communication issues between product teams or managers, contractor staff access to technology tools, delay in policy decisions, and the possibility of government-wide shutdown, among other things.</p> <p>However, the risk register does not include a column for risk sources and does not explicitly state risk sources in the other columns.</p>
Define parameters to analyze and categorize risks	partially met	<p>As described above, SBA’s enterprise risk management framework includes categories and descriptions for use in categorizing risks.</p> <p>Additionally, the framework includes descriptors and definitions for assigning a likelihood rating and impact rating to a risk based on the likelihood of occurrence and potential severity of impact. The framework also includes instructions for calculating an overall risk rating based on the likelihood and impact scores.</p> <p>However, the UCP risk register does not define or describe the parameters to categorize or analyze risks, nor does the document include instructions for how to identify, analyze, and add risks. The IT Program Manager said that the process to add risks to the UCP risk register does not have defined parameters.</p>
Establish and maintain risk management strategy	not met	SBA does not have a project level risk management strategy for UCP.
Identify and document risks throughout development lifecycle	partially met	<p>Risks are identified at the various meetings attended by the IT program manager and are documented in the UCP risk register, as described above.</p> <p>Additionally, the UCP contracts require the contractor to create monthly status reports that include discussion of risks, among other things such as project progress and mitigation actions.</p> <p>However, the identified risks do not include risks associated with critical phases of development, such as system deployment.</p>

Leading practice	Assessment	Description of assessment
Evaluate, categorize, and prioritize risks using defined risk categories and parameters	partially met	SBA evaluated and categorized risks at the various meetings attended by the IT program manager and documented in the UCP risk register. The risk register also provides the capability to prioritize risks using a series of columns that assign likelihood, impact, and total scores for the potential severity of each risk. For example, the risk with the highest total score is delay in policy decisions validated by management, while two other technical risks related to IT infrastructure used in development have the highest individual assigned likelihood and impact scores out of all the identified risks. However, risks were not evaluated, categorized, or prioritized using defined categories or parameters, and officials confirmed there are no procedures or guidance for the process in the context of UCP.
Develop a risk mitigation plan in accordance with risk management strategy	not met	SBA does not have a risk mitigation plan for UCP. Other SBA guidance, such as a standard operating procedure on IT performance management, notes the importance of having a project risk strategy or mitigation plan in addition to the agencywide risk management strategy.
Monitor risks and implement the risk mitigation plan as appropriate	partially met	SBA monitors risks through the various meetings attended by the IT program manager and documents the risks, status, and mitigation actions in the UCP risk register. The risk register has a section for noting mitigation actions connected to each risk, but the information in that section is a mix of mitigation steps already taken, mitigation steps being taken, and mitigation steps to potentially take. For example, the risk register entry for the risk of delay in policy decisions validated by management notes that the concern has been elevated to management and an alternative development approach devised. However, each entry in the mitigation column of the risk register is only one sentence long, and acts as a record of mitigation actions. The mitigations are not connected to any risk mitigation plan or risk strategy. For example, the risk register does not note when the alternative development approach should be implemented, what it entails, or how it relates to other activities or stakeholders.

- Fully met: SBA provided evidence that addressed the entire practice.
- Partially met: SBA provided evidence that addressed one or more of the practice activities, but not all the activities.
- Not met: SBA did not provide evidence that addressed the practice.

Source: GAO analysis of SBA documentation. | GAO-25-106963

The weaknesses in SBA’s implementation of risk management practices are due, in part to a lack of policies and procedures requiring their use. According to SBA’s IT program manager, there are no SBA policies and procedures requiring the use of specific risk management practices on the UCP project. Although SBA has an enterprise-wide risk management strategy, the detailed procedures it lays out are applied at the agency level.

Further, the manager noted that these practices have not been fully implemented at the project level because they consider the UCP risk register to be sufficient for the project’s needs. According to the manager, developing additional documents such as a project-level risk management strategy and project-level risk mitigation plan has been a lower priority compared to other UCP development tasks. Until SBA establishes and implements policies and procedures requiring the use of leading risk management practices on its IT modernization projects, the agency will be limited in its ability to identify potential problems on its projects before they occur and mitigate adverse impacts on achieving objectives.

As previously discussed, SBA originally anticipated deploying the UCP system in September 2024. In June 2024, SBA announced a pause, effective August 1, 2024, in accepting new applications for certification. The agency stated that it would not be accepting new applications until the new system was deployed. In our draft report provided to SBA for comment, we expressed concerns regarding the agency’s pause in accepting new

applications. We noted that SBA triggered questions about risks and available mitigation strategies if full deployment did not occur in September or if there were system performance issues after deployment. These questions included:

- If deployment of the certification system was delayed or there are performance issues after deployment, how long does SBA wait until lifting the pause on accepting certification applications?
- If the pause is lifted due to a delayed deployment or there are performance issues after deployment, can SBA temporarily return to its processes that were in place before August 1, 2024?

This risk of a deployment delay was eventually realized, as SBA delayed UCP deployment to address system issues identified during testing. Although SBA subsequently deployed the system in October 2024 and lifted the pause in accepting new applications, risks remain with SBA's efforts to develop additional, more complex functionality, secure the system, and migrate data.

As mentioned previously, SBA did not provide risk documentation that addressed risks associated with the deployment of the UCP. The most recent version of the UCP risk register—SBA's primary risk assessment and documentation tool—provided to us in February 2024 included eight risks associated with various human and technical risks.³¹ These risks included coordination issues (disconnection between product managers or among product team roles), agency policy issues, developer staff access to digital infrastructure, delays from use of new enterprise tools or services, government shutdown risk, and dependency on legacy technology.

Further, while the UCP risk register included a column for mitigation actions, it did not include the type of detail found in a risk mitigation plan. Specifically, none of the described mitigation actions explained the responsible parties, a breakdown of individual tasks required for the mitigation, resources required for a mitigation, or a timeline for when a mitigation can be considered sufficiently implemented. For example, one mitigation entry in its totality was "elevated concern to leadership, devised alternate development strategy." The entry did not describe what level of leadership the risk was elevated to or by whom, what the alternate development strategy entailed, or what would trigger the alternate strategy.

We have previously reported that federal IT investments too frequently fail to deliver intended capabilities, due in part to lack of effective management in project planning, oversight, and governance.³² In addition, we have previously reported that planning for testing, conducting testing, and resolving software issues discovered during testing is key to avoiding risks of system problems in general.³³

Without a project level risk management plan or risk mitigation plan, SBA is at risk of not being able to quickly or effectively deal with issues that arise that could affect the ability of applicants to submit certification applications. Further, none of SBA's identified risks were related to common software testing or deployment issues (e.g., technical failures, data integrity or availability issues, integration or compatibility issues), including

³¹We provided SBA with the opportunity to produce a more recent risk register and other documentation of the meetings where risks are discussed and documented; however, the agency has not yet provided us with any such documents.

³²GAO, *High Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, [GAO-23-106203](#) (Washington, D.C.: Apr. 20, 2023). We designated the management of IT acquisitions and operations to be a high risk area across the federal government in 2015, a designation that remains.

³³GAO, *Electronic Health Records: VA Has Made Progress in Preparing for New System, but Subsequent Test Findings Will Need to Be Addressed*, [GAO-21-224](#) (Washington, D.C.: Feb. 11, 2021).

the potential for delays which—as previously mentioned—SBA experienced. Lastly, SBA did not develop mitigation strategies to account for possible delays in deployment or system performance issues.

SBA also needs to obtain a final authorization to operate for the system and consider the risks of the system to agency operations.³⁴ SBA issued an interim authority to operate for the UCP system on August 28, 2024, while it continues to implement system security controls. Under schedule pressure, SBA could decide to accept known risks and issue a final authorization to operate with issues not being fully resolved. If taking such an action, consideration of the probability and resulting impact of accepted deployment risks is essential. Without doing so, SBA will have difficulty assessing the potential consequences on the agency’s ability to provide certification services. Later in this report, we discuss additional cybersecurity and schedule risks facing SBA.

SBA Did Not Fully Implement Selected Leading Cybersecurity Practices

NIST guidance on engineering trustworthy secure systems establishes leading practices for agencies to follow in developing new systems or updating legacy systems.³⁵ The guidance is intended to address security issues from a perspective of stakeholder requirements and protection needs and to use established processes to ensure that such requirements and needs are addressed with the appropriate rigor across the life cycle of the system.

The NIST guidelines include the following selected cybersecurity leading practices: (1) define security aspects for conducting the acquisition; (2) include security requirements as part of system requirements; (3) select one or more suppliers that meet the security criteria; (4) develop an agreement that includes security requirements that will be supplied; and (5) identify, acquire, and maintain skilled systems and cybersecurity personnel to staff ongoing projects.

For the five selected leading cybersecurity practices, SBA fully met two, partially met two, and did not meet one. Table 5 provides a summary of the selected leading practices and an assessment of the extent to which SBA adopted them, as of October 2024.

³⁴NIST defines authorization to operate as the official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security and privacy controls.

³⁵National Institute of Standards and Technology, *Engineering Trustworthy Secure Systems*, Special Publication 800-160, Volume 1, Revision 1 (Gaithersburg, Md.: Nov. 16, 2022).

Table 5: Extent to Which the Small Business Administration (SBA) Adopted Selected Leading Cybersecurity Practices for the Unified Certification Platform (UCP) Project, as of October 2024

Leading practice and corresponding activities	Assessment	Description of assessment
<p>Define security aspects for conducting the acquisition.</p> <p>The acquisition strategy should define security aspects, such as how security risks will be mitigated, the schedule of security-relevant milestones, how assets will be protected, and the security-relevant criteria for selecting suppliers.</p>	partially met	<p>SBA's system acquisition plan includes general information on acquisition needs and a list of evaluation criteria, including subfactors like the technical solution and resource plan. Further, SBA's UCP contract solicitation documentation requires that the contractor offer include a detailed description of how the system solution will adhere to SBA's cybersecurity requirements for IT acquisitions.</p> <p>These cybersecurity requirements detail the security-relevant criteria that the contractors must comply with, such as risk mitigation, security milestones, and asset protection. Additionally, the cybersecurity requirements detail key areas that must be included in the contractor's technical proposal.</p> <p>However, the acquisition plan does not include key details on how SBA plans to manage security risks, security milestones, and asset protection at a project level. The plan also does not include specifics on how the contractors will be rated against the security criteria. In June 2024, SBA officials noted that the ongoing cybersecurity risks are managed by the Office of the Chief Information Security Officer at the agency level, however, SBA has not provided any documentation describing how the security risks are managed at the project level.</p>
<p>Include security requirements as part of system requirements.</p> <p>The security requirements should be integrated with and provided as part of the stakeholder requirements or system requirements.</p> <p>A traceability analysis should be documented to ensure that all security requirements are reflected in the design of the IT system.</p>	partially met	<p>SBA's performance work statement, included in the solicitation orders for the UCP contracts, states that the contractor shall comply with all aspects of SBA's cybersecurity requirements provided in the solicitation package. Further, the UCP systems requirements document includes the system security requirements for the system. However, SBA did not document the traceability between the security requirements and how the proposed IT system solution is expected to satisfy the requirements.</p>
<p>Select one or more suppliers that meet the security criteria.</p> <p>Subject matters experts should be involved in the selection process.</p>	not met	<p>As mentioned before, SBA did not specify how suppliers will be rated against the security criteria. In addition, the agency has not provided documentation demonstrating involvement from security-related subject matter experts in the contractor selection process.</p>
<p>Develop an agreement that includes security requirements that will be supplied.</p> <p>The agreement with the supplier should satisfy the security requirements, including the cybersecurity that will be supplied.</p>	fully met	<p>SBA's cybersecurity requirements for IT acquisitions detail key areas that must be included in contractor's technical proposals. These areas are:</p> <ul style="list-style-type: none"> Response to cybersecurity incidents Availability of service Data retention Encryption of data at rest Telecommunication service redundancy <p>Logical and physical data access limited to continental United States.</p> <p>According to SBA, UCP systems requirements document is intended to be the official documentation of service requirements that the contractor has agreed to provide for the project. Among other things, the requirements document lists the services that will be provided by the contractor for system security and data privacy.</p>

Leading practice and corresponding activities	Assessment	Description of assessment
<p>Identify, acquire, and maintain skilled systems and cybersecurity personnel to staff ongoing projects.</p> <p>The organization should identify personnel with security relevant expertise involved in the modernization project.</p> <p>The organization should maintain and manage a pool of skilled cybersecurity and systems engineering personnel.</p>	fully met	<p>SBA provided documentation of their methods to maintain and manage a skilled pool of cybersecurity and systems engineering personnel including:</p> <p>A strategic workforce and succession plan to track metrics for gains and losses from mission critical occupations, including IT management positions.</p> <p>The Fiscal Year 2021-2024 IT Strategic Workforce Plan that establishes the agency approach to ensuring they have the relevant IT workforce for agency needs.</p> <p>A voluntary bi-annual competency assessment for IT staff that assesses foundation, technical, and leadership competencies.</p> <p>A National Recruitment Plan that outlines targeted talent pools. Additionally, SBA reports developing a tech talent recruitment plan to target the cyber workforce.</p> <p>Additionally, SBA identified key security personnel who are involved in the UCP project, including the senior information system security officer.</p>

- Fully met: SBA provided evidence that addressed the entire practice.
- Partially met: SBA provided evidence that addressed one or more of the practice activities, but not all the activities.
- Not met: SBA did not provide evidence that addressed the practice.

Source: GAO analysis of SBA's documentation. | GAO-25-106963

The weaknesses in SBA's implementation of cybersecurity practices are due to, among other things, a lack of policies and procedures requiring their use. SBA project documentation also lacked specific details to address the gaps. For example, SBA stated that a requirements traceability matrix was not developed because the business requirements document achieves the same outcome, however, this document did not provide any detail as to how the contractor had satisfied security requirements during the course of development.

SBA's planning documentation for UCP did not include details for how it plans to manage cybersecurity risks at the project level. Specifically, SBA utilizes a cybersecurity appendix for all acquisition contracts that includes general cybersecurity requirements; however, these requirements were not specifically tailored to the needs of the UCP. Further, SBA did not document traceability between security requirements and how the developed system satisfies those requirements.

Each of these gaps pose significant risks for the UCP system during or after deployment. For example, without tailored security requirements, or traceability between security requirements and the design of the system, SBA cannot ensure that critical cybersecurity safeguards are fully implemented. This increases the risk of a successful cyberattack where malicious actors gain access to confidential information or disrupt the availability of the system.

In addition, for future IT modernization projects, until SBA establishes and implements policies and procedures to require specific plans for how to manage security risks and documents the involvement of security-related subject matter experts in contract selection, SBA will be at risk for expending resources on projects that may not meet the security needs of the agency. Further, until SBA establishes and implements policies and procedures to ensure that a traceability analysis between the security requirements and the proposed IT solution is performed, it faces an increased risk that adequate cybersecurity will not be built into the new system, resulting in a potentially insecure system.

SBA Did Not Develop a Schedule for Its Unified Certification Platform

According to GAO's *Schedule Assessment Guide*, the success of a project depends in part on having an integrated and reliable master schedule that defines when and how long work will occur and how each activity is related to the others.³⁶ The schedule integrates the planned work, the resources necessary to accomplish that work, and the associated budget. This can help determine if the program's parameters are realistic and achievable.

GAO's research has found that a reliable integrated master schedule is one that is comprehensive, well-constructed, credible, and controlled. Management minimizes the risk of schedule overruns and unmet performance targets by ensuring the integrated master schedule reflects the following four characteristics.

- **Comprehensive.** A comprehensive schedule includes all activities for both the government and its contractors necessary to accomplish a program's objectives as defined in the program's work breakdown structure (WBS). The schedule includes the labor, materials, travel, facilities, equipment, and the like needed to do the work and depicts when those resources are needed and when they will be available. It realistically reflects how long each activity will take and allows for discrete progress measurement.
- **Well-constructed.** A schedule is well-constructed if all its activities are logically sequenced with the most straightforward logic possible. Unusual or complicated logic techniques are used judiciously and justified in the schedule documentation. The schedule's critical path represents a true model of the activities that drive the program's earliest completion date, and total float accurately depicts schedule flexibility.
- **Credible.** A schedule is credible if it reflects the order of events necessary to achieve products or outcomes. It should also reflect activities in varying levels of the schedule that relate to one another.
- **Controlled.** A schedule is controlled if it is updated regularly to reflect actual progress and changes. Updates to the schedule are accompanied by a schedule narrative that describes salient changes to the work. The current schedule is compared against a designated baseline schedule to measure, monitor, and report the program's progress. The baseline schedule is accompanied by a basis document that explains the overall approach to the program, defines ground rules and assumptions, and describes the unique features of the schedule. The baseline schedule and current schedule are subjected to configuration management control.

Instead of an integrated master schedule, the project relied on a "product road map" that is not a schedule. According to SBA officials, the agency created a UCP product road map as part of their Agile development framework and aligned it with the two-week sprint cycle process the product teams follow.

The UCP road map covers calendar year 2024 and contains a section for certain milestones, such as data migration from the prior systems to UCP and the deployment of an internal user dashboard. These milestones are overlaid on time-bounded tasks for the various product teams. However, the road map does not include milestones for important system cybersecurity tasks, such as when the security requirements will be finalized and when security testing will be complete. The lack of security milestones is also discussed later in this report. In addition, the road map does not include relationships or dependencies between the tasks, nor does it identify resources for any given activity. Lastly, although SBA officials stated that they meet with staff to ensure

³⁶[GAO-16-89G](#).

communication between product teams, they do not rely on an integrated master schedule to track and plan tasks.

The lack of an integrated master schedule is due, in part, to shortcomings in SBA's policies and procedures. Although SBA policy requires a schedule for new acquisitions, it does not provide procedures and guidance on how to develop reliable schedule estimates.

According to SBA, its guidance on system development methodology lays out requirements for project scheduling. However, the guidance only states that a project management plan should have a road map as part of the project management plan. It does not describe specific requirements for what the road map should include, such as how each activity is related to others or required resources.

Further, SBA officials stated that the Agile methodology does not require a project schedule equivalent to an integrated master schedule, because the process results in specific software features being released during specific time blocks (i.e., individual sprints). According to program officials, critical path milestones are plotted on the road map, and very few milestones are truly critical. Officials said the product road map is sufficient to get the work done in lieu of a master schedule.

However, as explained in GAO's *Agile Assessment Guide*, Agile methodologies still require planning, documentation, and a schedule baseline.³⁷ Specifically, the guide notes that the adaptive and iterative nature does not preclude the need for planning and documentation for the phases of Agile development, how those phases relate to each other, and updates over the life of the development as new information becomes available. Additionally, the guide states that the Agile goal of delivering features at defined intervals still requires the development of a schedule baseline. According to the guide, the baseline should contain enough detail to enable collaborative agreement between product owners and developers. It should be updated with actual data and revisions as progress is made. It should also provide a record of trends and deviations from the baseline to understand whether program execution is on track or requires changes.

The road map provided by SBA does not convey the information available in a reliable integrated master schedule. As a result, it cannot be used to forecast completion dates, help teams plan work based on knowledge of receivables and deliverables, or identify problems that may occur and their effects on downstream work.

Until SBA establishes and implements policies and procedures to require the use of an integrated master schedule that reflects GAO's schedule estimation guidance, the agency faces an increased risk of uncertainty in determining the duration on future IT modernization projects. Such uncertainty can cause schedule slippages, increased project costs, and hinder the ability of agency leadership to make informed decisions.

³⁷[GAO-24-105506](#).

SBA Cost Estimate for the Unified Certification Platform Was Unreliable

According to GAO's *Cost Estimating and Assessment Guide*, reliable cost estimates are critical for successfully delivering IT programs.³⁸ Such estimates provide the basis for informed decision making, realistic budget formulation, meaningful progress measurement, and accountability for results.

GAO's research has found that a reliable cost estimate is one that is comprehensive, well-documented, accurate, and credible. Management minimizes the risk of cost overruns and unmet performance targets by ensuring cost estimates reflect these four characteristics.

- **Comprehensive.** Cost estimates completely define the program and reflect the current schedule and technical baseline. They are structured with sufficient detail to ensure that cost elements are neither omitted nor double-counted. Where information is limited and judgments must be made, assumptions and exclusions on which the estimate is based are reasonable, clearly identified, explained, and documented.
- **Well-documented.** Cost estimates can easily be repeated or updated and can be traced to original sources through auditing. Thorough documentation explicitly identifies the primary methods, calculations, results, rationales or assumptions, and sources of the data used to generate each cost element's estimate.
- **Accurate.** Cost estimates are developed by estimating each cost element using the best methodology from the data collected. Accurate estimates are based on appropriate adjustments for inflation. Their underlying mathematical formulas, databases, and inputs are validated, and the resulting estimates contain few, if any, minor mathematical mistakes. Accurate estimates are based on a historical record of cost estimating and actual experiences from comparable programs. Finally, they are updated regularly to reflect significant changes in the program. Any variances between estimated and actual costs are documented, explained, and reviewed.
- **Credible.** Cost estimates discuss and document any limitations of the analysis, including uncertainty or bias surrounding source data and assumptions. The estimate's major assumptions are varied to determine how sensitive it is to changes. Credible cost estimates include a risk and uncertainty analysis that determines the level of confidence associated with the estimate. In addition, high-value cost elements are cross-checked with alternative estimating methodologies to validate results. Finally, the estimate is compared with an independent cost estimate conducted by a group outside the acquiring organization.

The May 2023 SBA cost estimate of approximately \$19 million for its UCP project was unreliable. This was reflected primarily by a lack of evidence supporting the methodology used to develop the estimate. Although the estimate was mathematically sound and followed a logical structure, we could not trace it back to requirements and had no insight into the validity of the approach used to create the estimate. Our findings below summarize the analysis of the cost estimate.

Specifically, SBA's cost estimate partially met two (comprehensive, accurate), minimally met one (well-documented), and did not meet one of the four characteristics (credible). Table 6 summarizes our assessment of SBA's UCP project cost estimate compared to these characteristics, as of October 2024. Appendix II provides additional information on our cost assessment.

³⁸[GAO-20-195G](#).

Table 6: Assessment of Small Business Administration (SBA) Unified Certification Platform (UCP) May 2023 Cost Estimate Compared to Cost Estimating Leading Practices, as of October 2024

Characteristic	Assessment	Leading practice	Description of assessment
Comprehensive	partially met	The cost estimate includes all life cycle costs.	The cost estimate considers work identified in the contractor's performance work statements, for development and one year of operations and maintenance, but it does not include government and system operations costs. When a cost estimate is missing cost elements, the total cost will be underestimated.
Comprehensive	partially met	The cost estimate is based on a technical baseline description that completely defines the program, reflects the current schedule, and is technically reasonable.	The estimate is the product of estimated hours and rates of pay across various categories. However, it fails to show how SBA traced the estimate to a technical baseline description. Without explicit documentation of the technical baseline of a program's estimates, it will be difficult to update the cost estimate and provide a verifiable trace to a new cost baseline as key assumptions change during the project's life.
Comprehensive	partially met	The cost estimate is based on a work breakdown structure that is product-oriented, traceable to the statement of work, and at an appropriate level of detail to ensure that cost elements are neither omitted nor double-counted.	The estimate relies on a work breakdown structure for the work identified in the contractor's performance work statements.
Comprehensive	partially met	The cost estimate documents all cost-influencing ground rules and assumptions.	Although it includes general scope assumptions for the contract, the cost estimate does not consider how ground rules (agreed-upon standards that minimize conflicts in definitions) and assumptions impact the estimate. Without analyzing the effects of changing ground rules and assumptions on the estimated cost and schedule of a program, cost estimators and management will not have a full understanding of their effect and of any limits to their validity.
Well documented	minimally met	The cost estimate documentation shows the source data used, the reliability of the data, and the estimating methodology used to derive each element's cost.	The cost estimate relies on expert judgment and does not include supporting documentation that explains the estimate. Unless the estimate is fully documented, it will not support an effective independent review, hindering the understanding of any differences between the proposed estimate and the review. This in turn limits the ability of decision-makers to make informed decisions.
Well documented	minimally met	The cost estimate documentation describes how the estimate was developed so that a cost analyst unfamiliar with the program could understand what was done and replicate it.	The estimate does not discuss how the contractor's performance work statements were used to create the estimate or whether risk and uncertainty were considered. Unless thoroughly documented, the cost estimate may not be defensible. That is, the documentation may not present a convincing argument of an estimate's validity or help answer decision-makers' and oversight groups' probing questions.

Characteristic	Assessment	Leading practice	Description of assessment
Well documented	minimally met	The cost estimate documentation discusses the technical baseline description and the data in the technical baseline are consistent with the cost estimate.	The estimate cannot be reconstructed from the information provided because SBA did not document a technical baseline description. Because the technical baseline is intended to serve as the basis for developing a cost estimate, it should be discussed in the cost estimate documentation. Without a technical baseline, the cost estimate will not be based on a comprehensive program description and will lack specific information regarding technical and program risks.
Well documented	minimally met	The cost estimate documentation provides evidence that the cost estimate was reviewed and accepted by management.	Although SBA's Office of the Chief Information Officer and the contracting officer signed off on the cost estimate, it lacked information such as an analysis of risks, benefits, and the methodology used to estimate costs. When management is not presented with sufficient information about how the estimate was constructed—including the specific details about the program's technical characteristics, assumptions, data, cost estimating methodologies, sensitivity, and risk and uncertainty—management will not know that the estimate is complete and high in quality.
Accurate	partially met	The cost estimate is based on a model developed by estimating each work breakdown structure (WBS) element using the best methodology from the data collected.	The estimate was developed using expert judgment and does not include supporting data or methodologies. Expert opinion should be used sparingly, and the estimate should account for the possibility that bias influenced the results.
Accurate	partially met	The cost estimate is adjusted properly for inflation.	The estimate was developed using approved inflation-adjusted rates but does not include an estimate in base-year dollars. Therefore, we were not able to validate inflation rates. When adjusting for inflation, if the index used is not correct, the resulting estimate could overstate or understate the cost of the program.
Accurate	partially met	The cost estimate contains few, if any, minor mathematical mistakes.	The cost estimate appears mathematically correct.
Accurate	partially met	The cost estimate is based on a historical record of cost estimating and actual experiences from other comparable programs.	According to program officials, documentation does not exist to support the estimate, but it is based on the project manager's past experience of over 10 years estimating similar programs. A lack of historical data will leave the cost estimator without insight into actual costs of similar programs, including any cost growth since the original estimate.
Credible	not met	The cost estimate includes a sensitivity analysis that identifies a range of possible costs based on varying major assumptions, parameters, and data inputs.	SBA did not perform a sensitivity analysis for the UCP cost estimate. An agency that fails to conduct a sensitivity analysis to identify the effect of uncertainties associated with different assumptions increases the chances that decisions will be made without a clear understanding of these impacts on costs.

Characteristic	Assessment	Leading practice	Description of assessment
Credible	not met	The cost estimate includes a risk and uncertainty analysis that quantifies the imperfectly understood risks and identifies the effects of changing key cost driver assumptions and factors.	SBA did not perform a risk and uncertainty analysis. When lacking a risk and uncertainty analysis, management cannot determine a defensible level of contingency that is necessary to cover increased costs resulting from unexpected design complexity, incomplete requirements, technology uncertainty, and other uncertainties.
Credible	not met	The cost estimate employs cross-checks—or alternate methodologies—on major cost elements to validate results.	The estimate does not indicate that major cost elements were cross-checked to see whether similar results arise from the use of different methodologies. Unless an estimate employs cross-checks, the estimate will have less credibility because stakeholders will have no assurance that alternative estimating methodologies produce similar results.

- = Fully met: SBA provided complete evidence that satisfies the entire criterion.
- = Substantially met: SBA provided evidence that satisfies a large portion of the criterion.
- ◐ = Partially met: SBA provided evidence that satisfies about half the criterion.
- ◑ = Minimally met: SBA provided evidence that satisfies a small portion of the criterion.
- = Not met: SBA provided no evidence that satisfied any of the criterion.

Source: GAO analysis of UCP project cost estimate and supporting documentation. | GAO-25-106963

Note: Some criteria for the accurate and credible characteristics were not applicable to the UCP project. In particular, the criteria that the cost estimate is regularly updated to ensure it reflects program changes and actual costs; the cost estimate documents, explains, and reviews variances between planned and actual costs; and the cost estimate is compared to an independent cost estimate that is conducted by a group outside the acquiring organization to determine whether other estimating methods produce similar results. These criteria did not apply to the UCP project and were excluded from the assessment.

The weaknesses in SBA’s use of cost estimating practices on the UCP project are due, in part, to shortcomings in SBA’s policies and procedures. Although SBA policies require a cost estimate for new acquisitions, it does not provide procedures and guidance on how to develop reliable cost estimates. SBA policies also encourage but do not require projects to implement leading practices identified in GAO’s cost guide. Further, SBA has not provided additional procedures or guidance regarding applying the cost estimating leading practices.

According to the SBA IT program manager, the UCP cost estimate was developed based on her own past experience producing similar estimates and over a decade of experience in IT contract management. Additionally, SBA officials noted that technology acquisitions are overseen by SBA’s Office of the Chief Information Officer, which reviews and cross-checks cost estimates and serves as a safeguard to the process.

However, as discussed earlier, subject matter expertise by itself should be used sparingly. Given SBA’s multiple attempts at modernizing its certification systems, there should be actual data from those efforts that could be used to inform the UCP cost estimate. Furthermore, since SBA chose to solely rely on expert opinion, the estimate should have explicitly accounted for the possibility of bias since expert opinion is subjective and requires objective analyses to supplement it. The agency, however, did not perform such analyses (as discussed under the credibility practice).

Until SBA establishes and implements policies and procedures that require the implementation of leading practices identified in the GAO cost guide, the agency is less likely to develop reliable cost estimates for its IT modernization efforts that can serve as the basis for informed investment decision making. In addition, the agency risks being unable to effectively estimate funding needs for its IT modernization efforts and using unreliable data to make budgetary decisions.

Conclusions

SBA's contracting assistance programs rely on IT systems to deliver vital support services to entrepreneurs. To improve its ability to provide these services, SBA planned to deploy UCP to replace existing systems in September 2024, but was forced to extend planned deployment into October 2024 due to ongoing system development, testing, and issue resolution. SBA subsequently deployed the system, but work remains to develop additional, more complex functionality, secure the system, and migrate data from legacy systems.

SBA has critical gaps in its risk management implementation for the UCP project—notably, the lack of a project-level risk management plan and mitigation plan. Due to these gaps, SBA deployed the UCP system without a full understanding of the associated risks. Until SBA develops a mitigation plan for ongoing risks, the agency will not be able to quickly or effectively deal with issues that arise as they simultaneously operate the system and develop the more complex functionality that will be added to it. Further, it will be important for SBA to fully consider the probability and impact of any accepted risks related to issuing a final authorization to operate to better ensure that such risks do not affect certification services.

Shortcomings in SBA's implementation of leading cybersecurity practices also increase the likelihood of a deployed system that includes security vulnerabilities. Until it addresses critical cybersecurity weaknesses—notably, the lack of a plan for managing project cybersecurity risks and documenting traceability between the security requirements and system design—it will likely not be prepared for and able to address the impacts of a cybersecurity incident.

Going forward, it will also be important for SBA to establish policies and procedures to address the gaps we identified in risk management, cybersecurity, and schedule and cost estimation. Until it does so, the agency will be hindered in its ability to effectively manage future IT modernization project risks, ensure that its systems meet the security needs of the agency, and effectively manage the schedules and costs for its projects.

Recommendations for Executive Action

We are making fourteen recommendations to SBA:

The Administrator of SBA should direct the Associate Administrator of SBA's Office of Government Contracting and Business Development to expeditiously address critical UCP project risk management issues, including developing a project risk management strategy and risk mitigation plan. (Recommendation 1)

The Administrator of SBA should direct the Associate Administrator of SBA's Office of Government Contracting and Business Development to expeditiously address critical UCP project cybersecurity issues, including developing a plan for managing project cybersecurity risks and documenting a traceability analysis for project security requirements. (Recommendation 2)

The Administrator of SBA should direct the Chief Information Officer to consider the probability and impact of accepted UCP deployment risks if deciding to issue a final authorization to operate for the system. (Recommendation 3)

The Administrator of SBA should direct the Chief Information Officer to establish and implement policies and procedures to ensure that risk registers or equivalent risk documentation explicitly state risk sources for IT modernization projects. (Recommendation 4)

The Administrator of SBA should direct the Chief Information Officer to establish and implement policies and procedures to ensure that parameters to categorize or analyze risks are clearly defined at the project level for IT modernization projects. (Recommendation 5)

The Administrator of SBA should direct the Chief Information Officer to establish and implement policies and procedures to ensure that project risk management strategies are established and maintained for IT modernization projects. (Recommendation 6)

The Administrator of SBA should direct the Chief Information Officer to establish and implement policies and procedures to ensure that risks are identified and documented for IT modernization projects for all phases of the development lifecycle, including deployment. (Recommendation 7)

The Administrator of SBA should direct the Chief Information Officer to establish and implement policies and procedures to ensure that risks are evaluated, categorized and prioritized using defined parameters, and also to ensure that project risk mitigation plans are developed for IT modernization projects. (Recommendation 8)

The Administrator of SBA should direct the Chief Information Officer to establish and implement policies and procedures to ensure that identified risk mitigations are connected to a project risk mitigation plan for IT modernization projects. (Recommendation 9)

The Administrator of SBA should direct the Chief Information Officer to establish and implement policies and procedures to ensure that IT system acquisition plans and strategic plans for IT modernization projects contain all the information needed to manage cybersecurity risks, including how such risks will be managed, security milestones, how assets will be protected at a program or project level, and security-relevant criteria for selecting suppliers. (Recommendation 10)

The Administrator of SBA should direct the Chief Information Officer to establish and implement policies and procedures to ensure that a traceability analysis is performed and documented for IT modernization projects to show the traceability of the security requirements to the design of the proposed IT system solution. (Recommendation 11)

The Administrator of SBA should direct the Chief Information Officer to establish and implement policies and procedures to ensure that security-related subject matter experts are involved in the contractor selection process for IT modernization projects. (Recommendation 12)

The Administrator of SBA should direct the Chief Information Officer to establish and implement policies and procedures to ensure that integrated master schedules are developed for IT modernization projects using leading practices described in GAO's Schedule Assessment Guide. (Recommendation 13)

The Administrator of SBA should direct the Chief Information Officer to establish and implement policies and procedures to ensure that cost estimates for IT modernization projects are developed using leading practices described in GAO's Cost Estimating and Assessment Guide. (Recommendation 14)

Agency Comments and Our Evaluation

We provided a draft of this report to SBA for review and comment. In written comments provided by SBA (reproduced in appendix III), the agency concurred with three recommendations, partially concurred with three recommendations, and did not concur with eight recommendations.

The draft report included an additional recommendation that SBA identify UCP deployment delay as a risk and identify mitigation strategies (draft report Recommendation 3). SBA deployed the UCP system on October 18, 2024. Therefore, we removed the recommendation and modified our report accordingly.

SBA concurred with recommendations 11, 12, and 13 to establish and implement policies and procedures to ensure traceability analyses are documented, security-related subject matter experts are involved in the contractor selection process, and integrated master schedules are developed for IT modernization projects in accordance with the GAO Schedule Guide. SBA stated it intends to initiate activities in line with the recommendations.

In addition, SBA partially concurred with our first, second, and third recommendations. Specifically:

- For our first recommendation, SBA noted that it intends to document a UCP project level risk management strategy and risk management plan, expand the risk register to ensure risks are appropriately categorized, prioritized, and evaluated, and determine appropriate mitigation strategies for the risks. These actions are in line with our recommendation; however, as noted in our report, we reiterate the need for a risk mitigation plan that includes relevant information such as responsible parties, required tasks, resources, and timelines. As a result, we believe that our recommendation is warranted.
- For our second recommendation, SBA outlined its planned process for assessing the security of the UCP through testing and addressing critical findings during the beta period. SBA also plans to document traceability between security requirements in line with our recommendation. However, as stated in our report, the agency did not document a plan for managing UCP project cybersecurity risks. As such, we believe that our recommendation is warranted.
- For our third recommendation, SBA outlined its procedures for approving an authorization to operate for IT systems and agreed that additional security measures would enhance the deployment risk assessment and validation for the UCP system. As noted in our report, it will be important for SBA to fully consider the impact of deployment risks when fully authorizing the system, and SBA has yet to provide documentation to that effect. As a result, we believe that our recommendation is warranted.

SBA did not concur with eight recommendations. Specifically:

- For recommendations four through nine, SBA outlined its current processes and guidance for reviewing and approving major IT investments. SBA also reiterated that it has an enterprise risk management strategy and cybersecurity and privacy policies that reference federally mandated requirements. However, as noted in our report, SBA did not provide a UCP project-level risk management plan. Additionally, SBA did not provide documentation of the various meetings where risks are discussed, and risk management decisions made. Further, SBA's policies and procedures did not require the explicit statement of risk sources for IT modernization projects (recommendation 4), parameters that define how to categorize or analyze risks (recommendation 5), and ensure that project level risk management strategies are established (recommendation 6). SBA's policies and procedures also did not require that risks are identified and documented at all phases of the development lifecycle (recommendation 7), ensure that risks

are evaluated, categorized, and prioritized using defined parameters and that risk mitigation plans are developed (recommendation 8), and that identified risk mitigations are connected to project risk mitigation plans (recommendation 9). As a result, we maintain that our recommendations on these leading practices are warranted.

- For recommendation 10, SBA stated that its cybersecurity and privacy policy and procedures are in-line with federal requirements. SBA also noted that its IT-related acquisitions, instructions to potential vendors are required to include an appendix that details general cybersecurity requirements. However, as noted in our report, the acquisition documentation we received for the UCP did not include key project level details for how SBA planned to manage risks, protect assets, or define security-relevant criteria for selecting the suppliers. As a result, we believe our recommendation is warranted.
- For recommendation 14, SBA noted that its current policy references the leading practices in GAO's *Cost Estimating and Assessment Guide*, and that all IT modernization projects are required to follow SBA policies. However, as noted in our report, SBA guidance only suggests, and does not require, that investments implement leading practices identified in GAO's cost guide. Additionally, we identified gaps in the implementation of the leading practices for the UCP. As a result, we believe that our recommendation is warranted.

In SBA's preamble to the recommendation responses, the agency stated that it believes we mischaracterized its risk management practices in the report. Specifically, the agency stated that we implied that SBA had no project risk management in place. However, our report does not state that SBA had no project risk management. Our report gives credit to SBA for areas where its efforts aligned with leading practices, such as monitoring risks through the various meetings attended by the IT program manager and documenting them in a project level risk register.

However, our report also describes specific instances where SBA's risk management documentation and practices do not fully align with leading practices. For example, we note that SBA does not have a project level risk management strategy or a project level risk mitigation plan. Further, in its agencywide risk management guidance and project risk management tools, SBA does not include explicit risk sources or use defined parameters when evaluating, categorizing, and prioritizing risks, among other weaknesses.

SBA also stated that we mischaracterized the agency's cybersecurity practices, and that we implied that the UCP project was managed without any cybersecurity plan or oversight. However, our report does not state that SBA has no cybersecurity plan or oversight. Our report gives SBA credit for the areas where its practices and documentation align with leading cybersecurity practices. For example, we noted that SBA included security-related aspects in the UCP contract solicitation documentation, UCP performance work statement, cybersecurity appendix attached to the UCP contract, and UCP systems requirements document. We also detailed SBA's effective methods for maintaining and managing a skilled pool of cybersecurity and systems engineering personnel.

However, our report also provides instances where SBA's cybersecurity documentation and practices do not fully align with leading cybersecurity practices. For example, as noted in the report, SBA did not include key details in the UCP acquisition plan for how SBA plans to manage security risks, security milestones, and asset protection at the project level. It also did not document traceability between security requirements and how the UCP system is expected to satisfy the requirements; specify how suppliers would be rated against security criteria; or document how to involve agency subject matter experts in the contractor selection process. Additionally, while we note the Office of the Chief Information Security Officer managed security risks at the agency level, SBA did not provide documentation of how security risks are managed at the project level.

At the time that we sent our draft report to SBA for comment, the agency planned to deploy the UCP in September 2024. SBA announced in June 2024 a pause, effective August 1, 2024, in accepting new applications for certification. According to SBA, it planned to lift the pause when the new system was deployed. Based on our findings when the report was sent to SBA for comment, we raised concerns about SBA's ability to deploy the system on time and without significant deficiencies. We posed questions to SBA about 1) how long the agency planned to wait to lift the new application pause in case of a deployment delay, and 2) in the case of a delayed deployment or performance issues, whether SBA could temporarily return to its processes that were previously in place. In its response, SBA noted that that pause was intended to clear a backlog of certification applications and did not anticipate significant delays.

As discussed in the report, SBA did experience a delay before deploying the system. In addition, work still remains to develop additional, more complex functionality, secure the system, and migrate data. In follow-ups with SBA, officials reported making recent changes in management of the UCP. These include the appointment of a Chief Technology Officer and a new project manager. SBA also noted that they have conducted security testing with the assistance of the Cybersecurity and Infrastructure Security Agency. These actions are positive steps toward addressing the issues we identified in our report and our recommendations.

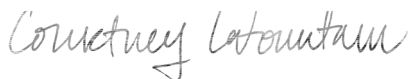
As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 7 days from the report date. At that time we will send copies of this report to the appropriate congressional committee, the Administrator of SBA, and other interested parties. In addition, the report will be available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact Carol C. Harris at (202) 512-4456 or HarrisCC@gao.gov, or Courtney LaFountain at (202) 512-5463 or LaFountainC@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Sincerely,



Carol C. Harris, Director
Information Technology and Cybersecurity



Courtney LaFountain, Acting Director
Financial Markets & Community Investment

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the Small Business Administration’s (SBA) plans for the Unified Certification Platform (UCP) project and the status of its efforts; (2) determine to what extent the UCP project has adopted leading IT management practices for risk management, cybersecurity, and schedule and cost estimation.

To address our first objective, we reviewed and summarized relevant UCP project information such as acquisition plans, solicitation documents, monthly meeting minutes, and schedule and cost documentation. Specifically, we determined which key UCP project activities had been completed as of July 2024 and the expected completion dates for the remaining activities. We also reviewed SBA documentation regarding its planned pause in accepting certification applications prior to deployment. Lastly, we interviewed agency officials to verify SBA’s plans for its modernization effort and its current status.

To address our second objective, we assessed the UCP project and SBA’s policies and procedures for managing risks, cybersecurity, and schedule and cost estimation.

- To determine the extent to which SBA implemented leading practices for risk management, we identified seven risk management leading practices based on prior GAO work and ISACA’s Capability Maturity Model Integration (CMMI).¹ These leading practices map to the managed practices of risk management, where projects are planned, performed, measured, and controlled. These selected practices were (1) determining risk sources and categories; (2) defining parameters to analyze and categorize risks; (3) establishing and maintaining a risk management strategy; (4) identifying and documenting risks; (5) evaluating, categorizing, and prioritizing each identified risk; (6) developing a risk mitigation plan in accordance with the risk management strategy; and (7) monitoring the status of each risk periodically and implementing the risk mitigation plan as appropriate.

We then evaluated the UCP project documentation, such as the risk registers and SBA policies on risk management, against the seven selected leading practices to determine whether the project fully met, partially met, or did not meet the practices.² We also reviewed SBA documentation regarding its planned pause in accepting certification application and its UCP system deployment plans. We then reviewed SBA’s risk register, provided to us in February 2024, for system deployment risks and mitigation strategies related to its planned UCP system deployment.³

- To determine the extent that SBA had adopted leading practices for cybersecurity, we identified and selected five leading practices that represented key elements for addressing cybersecurity requirements and needs in an acquisition based on prior GAO work and the National Institute of Standards and

¹ISACA, *CMMI Model V3.0* (Pittsburgh, PA: Apr. 6, 2023). CMMI Model and ISACA© [2021] All rights reserved. Used with permission.

²“Fully met” means that the agency provided evidence that satisfies the entire practice, “partially met” means the agency provided evidence that addressed one or more of the practice activities, but not all of the activities, and “not met” means the agency provided no evidence that addressed the practice.

³We provided SBA with the opportunity to produce a more recent risk register and other documentation of the meetings where risks are discussed and documented; however, the agency has not yet provided us with any such documents.

Technology's (NIST) guidance on *Engineering Trustworthy Secure Systems*.⁴ The selected leading practices are (1) defining security aspects for how the acquisition would be conducted; (2) including security requirements as part of system requirements; (3) selecting one or more suppliers that meet the security criteria; (4) developing an agreement with supplier that includes the security requirements that will be supplied; and (5) identifying, acquiring, and maintaining skilled systems and cybersecurity personnel to staff ongoing projects.

We then evaluated documentation related to the UCP project, including the UCP project acquisition plan, request for quotes, and performance work statements against the selected leading practices to determine whether the project fully met, partially met, or did not meet the practices.⁵

- To determine the extent to which SBA implemented schedule estimation leading practices for the UCP project, we reviewed documentation supporting the project's road map from January 2024. We assessed this documentation against leading practices for developing a comprehensive, well-constructed, credible, and controlled schedule, as identified in GAO's *Schedule Assessment Guide*.⁶ We also interviewed program officials responsible for developing and managing the road map, including the UCP program manager, to understand the practices for creating and maintaining the road map.

To assess the reliability of SBA's schedule data, we evaluated relevant UCP documentation such as the project road map, to substantiate evidence obtained from interviews with knowledgeable agency officials. We determined that the schedule data provided by SBA was not complete and reliable. We discuss the limitations of this data in the report and we have made appropriate attribution indicating the sources of this data.

- Finally, to determine the extent to which SBA had adopted cost estimation leading practices, we reviewed documentation supporting SBA's UCP project cost estimates from May 2023. We assessed this documentation against the leading practices in GAO's *Cost Estimating and Assessment Guide*.⁷ These leading practices map to four characteristics of a high-quality, reliable cost estimate. Those characteristics are: comprehensive, well-documented, accurate, and credible. To understand UCP's methodology, data, and approach we interviewed relevant agency officials, including the UCP program manager. In performing our analysis for the UCP project, we determined the extent to which each characteristic was either not met, minimally met, partially met, substantially met, or fully met.⁸

We shared our preliminary cost findings with project officials to verify that the information on which we based our findings was complete, accurate, and up-to-date. We then discussed our preliminary assessment results with the project management officials.

⁴National Institute of Standards and Technology, *Engineering Trustworthy Secure Systems*, Special Publication 800-160, Volume 1, Revision 1 (Gaithersburg, Md.: Nov. 16, 2022).

⁵"Fully met" means that the agency provided evidence that satisfies the entire practice, "partially met" means the agency provided evidence that addressed one or more of the practice activities, but not all of the activities, and "not met" means the agency provided no evidence that addressed the practice.

⁶GAO, *Schedule Assessment Guide: Best Practices for Project Schedules*, [GAO-16-89G](#) (Washington, D.C.: Dec. 22, 2015).

⁷GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, [GAO-20-195G](#) (Washington, D.C.: Mar. 12, 2020).

⁸"Not met" means SBA provided no evidence that satisfies any of the leading practices criterion. "Minimally met" means SBA provided evidence that satisfies a small portion of the criterion. "Partially met" means SBA provided evidence that satisfies about half of the criterion. "Substantially met" means SBA provided evidence that satisfies a large portion of the criterion. "Fully met" means SBA provided evidence that completely satisfies the leading practices criterion.

To assess the reliability of SBA's cost data, we evaluated relevant UCP documentation, such as the cost estimate and contracts, to substantiate evidence obtained from interviews with knowledgeable agency officials. We determined that the cost data provided by SBA was not complete and reliable. We discuss the limitations of this data in the report and we have made appropriate attribution indicating the sources of this data.

For both objectives, we interviewed cognizant agency officials in SBA's Office of Government Contracting and Business Development, as well as SBA's Office of the Chief Information Officer to obtain their views and verify the information provided.

We conducted this performance audit from July 2023 to November 2024 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.

Appendix II: SBA UCP Project Cost Estimate Compared to Leading Practices

According to the GAO *Cost Estimating and Assessment Guide*,¹ the four characteristics of a high-quality, reliable cost estimate are comprehensive, well-documented, accurate, and credible. Table 7 provides our assessment of the Unified Certification Platform (UCP) project’s cost estimate compared to these characteristics and the associated leading practices, as of October 2024.

Table 7: Assessment of the Unified Certification Platform (UCP) Cost Estimate Compared to Leading Practices, as of October 2024

Characteristic	Overall assessment	Leading practice	Individual assessment
Comprehensive	Partially met	The cost estimate includes all life cycle costs.	Partially met
Comprehensive	Partially met	The cost estimate is based on a technical baseline description that completely defines the program, reflects the current schedule, and is technically reasonable.	Partially met
Comprehensive	Partially met	The cost estimate is based on a work breakdown structure (WBS) that is product-oriented, traceable to the statement of work, and at an appropriate level of detail to ensure that cost elements are neither omitted nor double-counted.	Substantially met
Comprehensive	Partially met	The cost estimate documents all cost-influencing ground rules and assumptions.	Partially met
Well documented	Minimally met	The cost estimate documentation shows the source data used, the reliability of the data, and the estimating methodology used to derive each element’s cost.	Minimally met
Well documented	Minimally met	The cost estimate documentation describes how the estimate was developed so that a cost analyst unfamiliar with the program could understand what was done and replicate it.	Minimally met
Well documented	Minimally met	The cost estimate documentation discusses the technical baseline description and the data in the technical baseline are consistent with the cost estimate	Not met
Well documented	Minimally met	The cost estimate documentation provides evidence that the cost estimate was reviewed and accepted by management.	Partially met
Accurate	Partially met	The cost estimate is based on a model developed by estimating each WBS element using the best methodology from the data collected.	Minimally met
Accurate	Partially met	The cost estimate is adjusted properly for inflation.	Minimally met
Accurate	Partially met	The cost estimate contains few, if any, minor mistakes.	Substantially met
Accurate	Partially met	The cost estimate is regularly updated to ensure it reflects program changes and actual costs.	Not applicable
Accurate	Partially met	The cost estimate documents, explains, and reviews variances between planned and actual costs.	Not applicable

¹GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, [GAO-20-195G](#) (Washington, D.C.: Mar 12, 2020).

Appendix II: SBA UCP Project Cost Estimate Compared to Leading Practices

Characteristic	Overall assessment	Leading practice	Individual assessment
Accurate	Partially met	The cost estimate is based on a historical record of cost estimating and actual experiences from other comparable programs	Minimally met
Credible	Not met	The cost estimate includes a sensitivity analysis that identifies a range of possible costs based on varying major assumptions, parameters, and data inputs.	Not met
Credible	Not met	The cost estimate includes a risk and uncertainty analysis that quantifies the imperfectly understood risks and identifies the effects of changing key cost driver assumptions and factors.	Not met
Credible	Not met	The cost estimate employs cross-checks—or alternate methodologies—on major cost elements to validate results.	Not met
Credible	Not met	The cost estimate is compared to an independent cost estimate that is conducted by a group outside the acquiring organization to determine whether other estimating methods produce similar results.	Not applicable

Fully met: SBA provided complete evidence that satisfies the entire criterion.

Substantially met: SBA provided evidence that satisfies a large portion of the criterion.

Partially met: provided evidence that satisfies about half the criterion.

Minimally met: SBA provided evidence that satisfies a small portion of the criterion.

Not met: SBA provided no evidence that satisfied any of the criterion.

Source: GAO analysis of UCP project cost estimate and supporting documentation. | GAO-25-106963

Appendix III: Comments from the Small Business Administration



U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, DC 20416

October 4, 2024

Carol Harris
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
Washington, D.C. 20548

Dear Director Harris:

Thank you for providing the U.S. Small Business Administration (SBA) with a copy of the Government Accountability Office (GAO) draft report titled, *IT Modernization: SBA Urgently Needs to Address Risks*, GAO-25-106963. The draft report (1) describes SBA's Unified Certification Platform (UCP) project plans and status, and (2) evaluates the extent SBA has adopted leading practices for risk management, cybersecurity, and schedule and cost estimation for the project. SBA appreciates the role GAO plays in working with management in ensuring that SBA's programs are administered effectively and understands the importance of the work GAO does to support risk mitigation for the agency.

In GAO's draft report, the "Background" section includes information about SBA's Office of Government Contracting and Business Development (GCBD) (GAO draft report pages 6-9). SBA would like to provide additional clarity on the functions of GCBD and the Office of the Chief Information Officer (OCIO) and how OCIO and GCBD partnered for the UCP project.

The Chief Information Officer (CIO) is responsible for strategic execution and management of Agency-wide functions and reports to the SBA Administrator and Deputy Administrator. The CIO also chairs the Business Technology Investment Council (BTIC), composed of senior Agency executives and district office directors. The BTIC is charged with overseeing the selection, control and evaluation of SBA's major IT investment initiatives. OCIO staff and managers cover a broad information technology landscape, including day-to-day operations and oversight of SBA's systems, the development, management of information management and data, the investment, planning and oversight of SBA's systems, as well as systems performance and employee competency assessments.

The Office of Government Contracting and Business Development's (GCBD) is responsible for all aspects of the federal government's small business contracting program to include setting small business goals for all 24 CFO Act federal agencies and certifying small firms to be eligible to bid on and win certain small business set-aside contracts. GCBD's portfolio of certifications programs includes 8(a) Business Development certifications (8(a) Program), Women Owned Small Business certifications (WOSB), Veterans Owned Small Business certifications (VetCert), and certifications for Historically Underutilized Business Zones (HUBZone) small business concerns. GCBD's mission is to work to create an environment for maximum participation by small, disadvantaged, and woman-owned businesses in federal government contract awards and

large prime subcontract awards. The goal is to prepare small, disadvantaged firms for procurement and other business opportunities.

GCBD's certification programs support statutory small business set-aside mandates that apply to the 24 CFO Act agencies. GCBD does not facilitate contract awards, rather assists small businesses in becoming contract ready, partners with federal agencies to identify contract opportunities for small businesses and certifies that small business firms competing for government set aside contracting, meet eligibility requirements for certain types of small business set-aside contracts.

These certification programs enabled the government to achieve awards of over \$176B in prime contracts and \$86B in subcontracts to eligible small businesses in fiscal year (FY) 23. However, these programs are not equally funded, resulting in a disparity of staffing for review, information technology systems, technical support, outreach and training, and application processing timelines. While a small business applicant waits an extended period for certification processing timelines, the applicant is excluded from opportunities to bid on certain small business set-aside contracts for which they would otherwise be eligible. Currently, SBA's four certification programs are managed by different leadership teams with different IT platforms. Small business applicants must upload the same or similar documents multiple times, maintain multiple SBA login credentials, and self-assess eligibility across the various program rules and requirements. While an estimated 40% of certified small businesses are eligible for multiple certifications, many forego additional certifications because the different application processes are administratively burdensome and complicated.

SBA's goal is to launch a customer-centric certification and recertification process platform that will enable small businesses to apply to and maintain all SBA government contracting certifications in one system. Further, applicants will be able to submit one application to obtain all four certifications at the same time, where eligible. This multi-year initiative is designed to unite the customer experience and streamline processes while retaining critical functions unique to each program area. OCIO and GCBD partnered extensively, within each's respective functions and authority, to develop and deploy the UCP system, and fulfill the requirements of the major IT investment. From the start, the OCIO played a critical role in oversight and management of the project to include IT governance.

SBA would like to provide additional context and perspective for the "Risk Management" and "Cyber Security" sections of the draft report (Sections beginning on draft report pages 20 and 26, respectively). SBA believes GAO mischaracterizes SBA's risk management as presented in the report, which implies SBA had no project risk management in place and that the UCP project was managed without any cybersecurity plan or oversight. Furthermore, SBA's FOLIO system was used to capture risks identified in a risk assessment, which was established and sustained for the project, and those identified risks were addressed with the appropriate risk response. The SBA ensured that the contractor followed the requirements for cybersecurity as outlined in the contract. SBA would like to highlight that throughout the UCP project, SBA managed project risk and cybersecurity risk through the established partnership between GCBD and OCIO and CISO, continuous communication with stakeholders, and contract and project execution.

Further, SBA would like to provide responses to two questions GAO posed within the draft report.

- 1) **QUESTION:** If deployment of the certification system is delayed or there are performance issues after deployment, how long does SBA wait until lifting the pause on accepting certification applications?

ANSWER: SBA paused applications on August 1, 2024, to clear the backlog of certification applications, some pending for several months as a result of short staffing in the WOSB program and the delays resulting from the *Ultima* case. SBA established an internal goal of clearing the backlog, and decisioned all 8(a), HubZone, and VetCert applications in preparation for launch of the new system. SBA approved over 4,900 small firms in GCBD certification program since pausing new applications on August 1. There are 0 applications remaining for all programs, except WOSB. SBA cleared 90% of the WOSB applications with only 800 remaining, and these applications should be decisioned within the next 10 business days. To date, SBA has completed extensive cyber and user testing on the new system, and do not anticipate significant delays. The UCP beta testing period started August 28, with an internal goal to complete the beta period no later than October 15th. In order to launch the VetCert platform in 2023, SBA paused applications for 10 weeks. The pause for UCP is similar. For risk mitigation, SBA retained legacy systems and could accept applications after October 15th. However, we would assess the issues and timeframes for corrective action in order to make an informed decision in the interest of small businesses on reopening legacy systems or extending the pause for a week(s) to provide a significantly better customer experience with the ability to apply for multiple certifications using a single application.

- 2) **QUESTION:** If the pause is lifted due to a delayed deployment or there are performance issues after deployment, can SBA temporarily return to its processes that were in place before August 1, 2024?

ANSWER: Yes. In the event of a significant launch delay, SBA retained the ability to accept applications under processes in place before August 1. All four legacy systems will remain intact through the UCP deployment. Additionally, SBA worked with firms facing a critical contract opportunity deadline to mitigate the risks of small firms being negatively impacted during the pause. The engagement of our team in support of firms with contract offers significantly reduce the risks associated with the pause and potential delays in deployment.

GAO made the following 15 recommendations directed to the Administrator of SBA and SBA's responses to the recommendations in the draft report are noted as follows:

GAO Recommendation 1: The Administrator of SBA should direct the Associate Administrator of SBA's Office of Government Contracting and Business Development to expeditiously address critical UCP project risk management issues, including developing a project risk management strategy and risk mitigation plan

SBA's Response to Recommendation 1: SBA partially agrees with this recommendation.

SBA appreciates the value of such program documents as a strategy and a plan outlined in GAO's recommendation. SBA will continue to strengthen its risk management strategies in addition to our current risk determination process and risk register. SBA will document the UCP project level risk management strategy and risk management plan. SBA will implement that strategy and plan and expand the existing risk register, ensuring more detailed identification of risks and risk sources, that are appropriately categorized, prioritized and evaluated. Based on the evaluation of risks included in the risk register, SBA will determine any appropriate mitigation strategies needed.

GAO Recommendation 2: The Administrator of SBA should direct the Associate Administrator of SBA's Office of Government Contracting and Business Development to expeditiously address critical UCP project cybersecurity issues, including developing a plan for managing project cybersecurity risks and documenting a traceability analysis for project security requirements.

SBA's Response to Recommendation 2: SBA partially agrees with this recommendation.

The SBA acknowledges the importance of the recommendation and continues to focus on any potential UCP security issues in partnership with our Chief Information Security Officer (CISO). Our CISO's process is comprehensive and includes response to malicious cybersecurity incidents, availability of service, data retention, encryption of data at rest. After significant testing, the CISO clears the system for operation and GCBD does not operate without this clearance. SBA has already begun implementing internal and external assessments including malicious penetration testing to find and mitigate cyber security risks. This testing is ongoing. The external testing includes SBA's agency partner CISA (FAST) Team. The external team is conducting a web application security assessment, which does include looking deep into the source code of this application. In addition, SBA has opened the system to a small beta group of external beta testers. The CISO and GCBD are continuing to work collaboratively to address security issues through a successful launch. The Tech Team has successfully deployed updated code and remediated all Critical/High findings during our beta period. SBA and its partners are evaluating and prioritizing risks, and our CISO team is ensuring critical cybersecurity safeguards are fully implemented. SBA will provide update requested by GAO about this process, with a final update, when the process is complete.

SBA has provided GAO with the UCP project's business requirements document and system security requirements document. However, in agreement with GAO's recommendation SBA will document traceability between security requirements and how the developed system satisfies those requirements, specific to cybersecurity requirements.

GAO Recommendation 3: The Administrator of SBA should direct the Associate Administrator of SBA's Office of Government Contracting and Business Development to identify a delay in UCP system deployment as a risk and to identify mitigation strategies for addressing UCP system deployment delays.

SBA's Response to Recommendation 3: SBA agrees with this recommendation. SBA will include UCP system deployment delay as a risk in the risk register. Based on the evaluation of risks included in the risk register, SBA will determine any appropriate mitigation strategies needed.

GAO Recommendation 4: The Administrator of SBA should direct the Office of the Chief Information Officer to consider the probability and impact of accepted UCP deployment risks if deciding to authorize to operate the system.

SBA's Response to Recommendation 4: SBA partially agrees with this recommendation to consider the probability and impact of accepted UCP deployment risks when approving Authority to Operates (ATOs) for systems. SBA agrees that additional security measures would enhance the deployment risk assessment and validation of the UCP IT system. For the UCP project, SBA is following its standard operating procedure to grant an interim ATO with Plans of Action and Milestones (POAM) until all IT security controls are met before for a full ATO can be issued.

OCIO manages cybersecurity and privacy risk through its SBA SOP 90 47, *Cybersecurity and Privacy Policy* and related procedures which provide requirements for all systems being onboarded into the environment. This policy is in-line with Federal Information Security Modernization Act (FISMA) of 2014 requirements. All systems' risks are managed as part of SBA's Information Security Continuous Monitoring (ISCM) program. Security Control Assessments are performed annually with additional vulnerability scans performed on a weekly basis. Plan of Actions and Milestones (POA&Ms) are created as needed to manage identified issues/risks for remediation.

Per SOP 90 47, *Cybersecurity and Privacy Policy*, "the Authorizing Official (AO) is the management official with the responsibility to ensure that the level of residual risk for an IT system or application is acceptable to the agency. Final Authority to Operate (ATO) a system approval lies with the AO. The SBA identifies the CIO as the agency AO". All programmatic risks, including high-value security specific risks are being tracked in Folio and reported to the IT Dashboard on a monthly basis.

SBA will continue to evaluate and update any necessary security policies and procedures to address high-value IT systems, as we continue to implement IT modernization projects.

GAO Recommendation 5: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that risk registers or equivalent risk documentation explicitly state risk sources for IT modernization projects.

SBA's Response to Recommendation 5

SBA disagrees with this recommendation. SBA engages all Major IT investments at various levels and stages within the IT enterprise governance lifecycle as part of the IT Investment risk management identification and assessment. Our current Standard Operating Procedures (SOPs), reference the Information Technology Management Reform Act of 1996 (Clinger-Cohen), the

Federal Information Technology Acquisition Reform Act (FITARA), OMB Circular A-11 section 55 Capital Planning Investment Control (CPIC), OMB Memorandum M-15-14, *Management and Oversight of Federal Information Technology*, and OMB Circular A-130, *Managing Information as a Strategic Resource*. All IT modernization investments/projects are required to follow SBA policies, processes, and/or procedures for risk management and mitigation, to include:

- The Business Investment Technology Council (BTIC), the governing body for SBA's IT Portfolio, conducts bi-monthly BTIC meetings to review and assess project health and identify potential risks and budgetary constraints within the IT investment portfolio. The BTIC process is in accordance with SOP 90 82, *IT Governance Investment Board*.
- In accordance with SOP 90 44, *SBA Information Technology and Capital Planning and Investment Control Standard Operating Procedures*, monthly CIO rating meetings are conducted by the CIO to evaluate, monitor, and control baselines applying any necessary corrective measures for IT investments that are reported as part of the OMB monthly submission published to the IT Dashboard.
- As stated in SOP 90 45, *CIO Responsibilities*, the CIO will "review high-risk investments" and "evaluate IT investments to ensure projects are effectively managed (IT Dashboard CIO Ratings)". This ensures that the CIO remains engaged with high-risk investments throughout the lifecycle.
- Stated in SOP 90 44, "OMB has defined required documents which demonstrate how SBA manages IT investment and how its governance processes are used when planning and implementing IT investment within the agency". These artifacts include a Risk Management Plan (RMP) with defined and categorized risks, mitigation strategies, probability and impact scores, and contingency plans. All programmatic risks are documented in the RMP, as well as the Folio tool for tracking.
- OCIO manages cybersecurity and privacy risk through its SBA SOP 90 47, *Cybersecurity and Privacy Policy* and related procedures which provide requirements for all systems being onboarded into the environment. This policy is in-line with Federal Information Security Modernization Act (FISMA) of 2014 requirements. All systems' risks are managed as part of SBA's Information Security Continuous Monitoring (ISCM) program. Security Control Assessments are performed annually with additional vulnerability scans performed on a weekly basis. Plan of Actions and Milestones (POA&Ms) are created as needed to manage identified issues/risks for remediation.

OCIO will continue to engage IT Investments thru the Capital Planning Investment Control (CPIC) process (OMB Circular A-11 section 55) to improve the reporting and accuracy of IT investment cost, schedule, and performance of IT modernization projects. As an ongoing and iterative process, IT modernization projects are identified, approved, funded, and continually monitored throughout the lifecycle to ensure proper management, mitigation, and documentation of project risks. Additionally, as a result of the audit SBA will perform an internal review of its policies and procedures to ensure they are current. We will update them in accordance with federal guidance and mandates, as well as institute and communicate any changes to SBA's existing policies, and procedures to IT investments.

GAO Recommendation 6: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that parameters

to categorize or analyze risks are clearly defined at the project level for IT modernization projects.

SBA's Response to Recommendation 6: See response to recommendation 5

GAO Recommendation 7: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that project risk management strategies are established and maintained for IT modernization projects.

SBA's Response to Recommendation 7: See response to recommendation 5

GAO Recommendation 8: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that risks are identified and documented for IT modernization projects for all phases of the development lifecycle, including deployment.

SBA's Response to Recommendation 8: See response to recommendation 5

GAO Recommendation 9: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that risks are evaluated, categorized and prioritized using defined parameters for IT modernization projects, and also to ensure that project risk mitigation plans are developed for IT modernization projects.

SBA's Response to Recommendation 9: See response to recommendation 5

GAO Recommendation 10: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that identified risk mitigations are connected to a project risk mitigation plan for IT modernization projects.

SBA's Response to Recommendation 10: See response to recommendation 5

GAO Recommendation 11: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that IT system acquisition plans and strategic plans for IT modernization projects contain all the information needed to manage cybersecurity risks, including how such risks will be managed, security milestones, how assets will be protected at a program or project level, and security-relevant criteria for selecting suppliers.

SBA's Response to Recommendation 11:

SBA disagrees with this recommendation as policies and procedures have been established and implemented to ensure that project risk management strategies are established and maintained for IT modernization projects.

SBA manages cybersecurity and privacy risk through its SBA SOP 90 47 *Cybersecurity and Privacy Policy* and related procedures which provide requirements for all systems being onboarded into the environment. This policy is in-line with Federal Information Security

Modernization Act (FISMA) of 2014 requirements. All systems' risks are managed as part of SBA's Information Security Continuous Monitoring (ISCM) program. Security Control Assessments are performed annually with additional vulnerability scans performed on a weekly basis. Plan of Actions and Milestones (POA&Ms) are created as needed to manage identified issues/risks for remediation. Additionally, SBA has created its Cybersecurity Acquisition Language for insertion into all contracts with Information Technology (IT) related aspects.

For all IT and IT-related acquisitions, the instructions to offerors section must include the following sentences:

- 1) The offeror shall, as part of their technical proposal, provide a detailed description of how the proposed solution will adhere to the requirements included in the "Appendix – Cybersecurity Language for IT Acquisitions" section of this solicitation.
- 2) The offeror shall, as part of their technical proposal, provide a detailed description of how the proposed solution will manage and minimize supply chain risk, addressing the requirements included in the "Appendix – Cybersecurity Language for IT Acquisitions" section of this solicitation.

SBA will perform a review of said policies and procedures to ensure they are effective and communicated to all stakeholders.

GAO Recommendation 12: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that a traceability analysis is performed and documented for IT modernization projects to show the traceability of the security requirements to the design of the proposed IT system solution.

SBA's Response to Recommendation 12: SBA agrees with this recommendation. Additionally, SBA is currently updating its System Development Methodology (SDM), which includes related requirements as part of its capital planning process for approving new technology. SBA will ensure that traceability analysis requirements are included in this methodology. As part of the SDM development, SBA will update its Cybersecurity and Privacy policy and communicate these updates to all stakeholders.

GAO Recommendation 13: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that security-related subject matter experts are involved in the contractor selection process for IT modernization projects.

SBA's Response to Recommendation 13: SBA agrees with this recommendation. SBA will engage IT acquisitions to make the inclusion of IT security experts a requirement during vendor/contractor selections. SBA IT acquisitions will incorporate language in their existing policies and procedures for all IT modernization projects.

GAO Recommendation 14: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that integrated

master schedules are developed for IT modernization projects using leading practices described in GAO's Schedule Assessment Guide.

SBA's Response to Recommendation 14: SBA agrees with this recommendation and will establish and implement policies and procedures to ensure that integrated master schedules are developed for IT modernization projects using leading practices described in GAO's Schedule Assessment Guide.

GAO Recommendation 15: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that cost estimates for IT modernization projects are developed using leading practices described in GAO's Cost Estimating and Assessment Guide.

SBA's Response to Recommendation 15:
SBA disagrees with this recommendation. SBA's current SOP 90 52 *IT Investment Performance Baseline Management (PBM)* references the leading practices in GAO-20-195G, Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs. All IT modernization investments/projects are required to follow SBA policies, processes, and/or procedures for cost estimation outlined in SOP 90 52.

OCIO will update policies and procedures in accordance with federal guidance and mandates, as well as institute and communicate any changes to SBA's existing policies, and procedures to IT investments.

Thank you for allowing SBA the opportunity to comment on GAO's draft report.

Sincerely,

**LARRY
STUBBLEFIELD**

Digitally signed by LARRY
STUBBLEFIELD
Date: 2024.10.04 15:19:31 -04'00'

Jaqueline L. Robinson-Burnette
Associate Administrator
Office of Government Contracting and Business Development

STEPHEN KUCHARSKI Digitally signed by STEPHEN KUCHARSKI
Date: 2024.10.04 15:28:18 -04'00'

Steven Kucharski
Chief Information Officer
Office of the Chief Information Officer

Cc:
Jonathan Ticehurst, Assistant Director, Information Technology & Cybersecurity
Dr. Courtney LaFountain, Director, Financial Markets and Community Investment

Accessible Text for Appendix III: Comments from the Small Business Administration

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, DC 20416

October 4, 2024

Carol Harris
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
Washington, D.C. 20548

Dear Director Harris:

Thank you for providing the U.S. Small Business Administration (SBA) with a copy of the Government Accountability Office (GAO) draft report titled, "IT Modernization: SBA Urgently Needs to Address Risks," GAO-25-106963. The draft report (1) describes SBA's Unified Certification Platform (UCP) project plans and status, and (2) evaluates the extent SBA has adopted leading practices for risk management, cybersecurity, and schedule and cost estimation for the project. SBA appreciates the role GAO plays in working with management in ensuring that SBA's programs are administered effectively and understands the importance of the work GAO does to support risk mitigation for the agency.

In GAO's draft report, the "Background" section includes information about SBA's Office of Government Contracting and Business Development (GCBD) (GAO draft report pages 6-9). SBA would like to provide additional clarity on the functions of GCBD and the Office of the Chief Information Officer (OCIO) and how OCIO and GCBD partnered for the UCP project.

The Chief Information Officer (CIO) is responsible for strategic execution and management of Agency-wide functions and reports to the SBA Administrator and Deputy Administrator. The CIO also chairs the Business Technology Investment Council (BTIC), composed of senior Agency executives and district office directors. The BTIC is charged with overseeing the selection, control and evaluation of SBA's major IT investment initiatives. OCIO staff and managers cover a broad information technology landscape, including day-to-day operations and oversight of SBA's systems, the development, management of information management and data, the investment, planning and oversight of SBA's systems, as well as systems performance and employee competency assessments.

The Office of Government Contracting and Business Development's (GCBD) is responsible for all aspects of the federal government's small business contracting program to include setting small business goals for all 24 CFO Act federal agencies and certifying small firms to be eligible to bid on and win certain small business set-aside contracts. GCBD's portfolio of certifications programs includes 8(a) Business Development certifications (8(a) Program), Women Owned Small Business certifications (WOSB), Veterans Owned Small Business certifications (VetCert), and certifications for Historically Underutilized Business Zones (HUBZone) small

business concerns. GCBD's mission is to work to create an environment for maximum participation by small, disadvantaged, and woman-owned businesses in federal government contract awards and large prime subcontract awards. The goal is to prepare small, disadvantaged firms for procurement and other business opportunities.

GCBD's certification programs support statutory small business set-aside mandates that apply to the 24 CFO Act agencies. GCBD does not facilitate contract awards, rather assists small businesses in becoming contract ready, partners with federal agencies to identify contract opportunities for small businesses and certifies that small business firms competing for government set aside contracting, meet eligibility requirements for certain types of small business set-aside contracts.

These certification programs enabled the government to achieve awards of over \$176B in prime contracts and \$86B in subcontracts to eligible small businesses in fiscal year (FY) 23. However, these programs are not equally funded, resulting in a disparity of staffing for review, information technology systems, technical support, outreach and training, and application processing timelines. While a small business applicant waits an extended period for certification processing timelines, the applicant is excluded from opportunities to bid on certain small business set-aside contracts for which they would otherwise be eligible. Currently, SBA's four certification programs are managed by different leadership teams with different IT platforms. Small business applicants must upload the same or similar documents multiple times, maintain multiple SBA login credentials, and self-assess eligibility across the various program rules and requirements. While an estimated 40% of certified small businesses are eligible for multiple certifications, many forego additional certifications because the different application processes are administratively burdensome and complicated.

SBA's goal is to launch a customer-centric certification and recertification process platform that will enable small businesses to apply to and maintain all SBA government contracting certifications in one system. Further, applicants will be able to submit one application to obtain all four certifications at the same time, where eligible. This multi-year initiative is designed to unite the customer experience and streamline processes while retaining critical functions unique to each program area. OCIO and GCBD partnered extensively, within each's respective functions and authority, to develop and deploy the UCP system, and fulfill the requirements of the major IT investment. From the start, the OCIO played a critical role in oversight and management of the project to include IT governance.

SBA would like to provide additional context and perspective for the "Risk Management" and "Cyber Security" sections of the draft report (Sections beginning on draft report pages 20 and 26, respectively). SBA believes GAO mischaracterizes SBA's risk management as presented in the report, which implies SBA had no project risk management in place and that the UCP project was managed without any cybersecurity plan or oversight. Furthermore, SBA's FOLIO system was used to capture risks identified in a risk assessment, which was established and sustained for the project, and those identified risks were addressed with the appropriate risk response. The SBA ensured that the contractor followed the requirements for cybersecurity as outlined in the contract. SBA would like to highlight that throughout the UCP project, SBA managed project risk and cybersecurity risk through the established partnership between GCBD and OCIO and CISO, continuous communication with stakeholders, and contract and project execution.

Further, SBA would like to provide responses to two questions GAO posed within the draft report.

- 1) QUESTION: If deployment of the certification system is delayed or there are performance issues after deployment, how long does SBA wait until lifting the pause on accepting certification applications?

ANSWER: SBA paused applications on August 1, 2024, to clear the backlog of certification applications, some pending for several months as a result of short staffing in the WOSB program and the delays resulting from the Ultima case. SBA established an internal goal of clearing the backlog, and decisioned all 8(a), HubZone, and VetCert applications in preparation for launch of the new system. SBA approved over 4,900 small firms in GCBD certification program since pausing new applications on August 1. There are 0 applications remaining for all programs, except WOSB. SBA cleared 90% of the WOSB applications with only 800 remaining, and these applications should be decisioned within the next 10 business days. To date, SBA has completed extensive cyber and user testing on the new system, and do not anticipate significant delays. The UCP beta testing period started August 28, with an internal goal to complete the beta period no later than October 15th. In order to launch the VetCert platform in 2023, SBA paused applications for 10 weeks. The pause for UCP is similar. For risk mitigation, SBA retained legacy systems and could accept applications after October 15th. However, we would assess the issues and timeframes for corrective action in order to make an informed decision in the interest of small businesses on reopening legacy systems or extending the pause for a week(s) to provide a significantly better customer experience with the ability to apply for multiple certifications using a single application.

2) QUESTION: If the pause is lifted due to a delayed deployment or there are performance issues after deployment, can SBA temporarily return to its processes that were in place before August 1, 2024?

ANSWER: Yes. In the event of a significant launch delay, SBA retained the ability to accept applications under processes in place before August 1. All four legacy systems will remain intact through the UCP deployment. Additionally, SBA worked with firms facing a critical contract opportunity deadline to mitigate the risks of small firms being negatively impacted during the pause. The engagement of our team in support of firms with contract offers significantly reduce the risks associated with the pause and potential delays in deployment.

GAO made the following 15 recommendations directed to the Administrator of SBA and SBA's responses to the recommendations in the draft report are noted as follows:

GAO Recommendation 1: The Administrator of SBA should direct the Associate Administrator of SBA's Office of Government Contracting and Business Development to expeditiously address critical UCP project risk management issues, including developing a project risk management strategy and risk mitigation plan

SBA's Response to Recommendation 1: SBA partially agrees with this recommendation.

SBA appreciates the value of such program documents as a strategy and a plan outlined in GAO's recommendation. SBA will continue to strengthen its risk management strategies in addition to our current risk determination process and risk register. SBA will document the UCP project level risk management strategy and risk management plan. SBA will implement that strategy and plan and expand the existing risk register, ensuring more detailed identification of risks and risk sources, that are appropriately categorized, prioritized and evaluated. Based on the evaluation of risks included in the risk register, SBA will determine any appropriate mitigation strategies needed.

GAO Recommendation 2: The Administrator of SBA should direct the Associate Administrator of SBA's Office of Government Contracting and Business Development to expeditiously address critical UCP project cybersecurity issues, including developing a plan for managing project cybersecurity risks and documenting a traceability analysis for project security requirements.

SBA's Response to Recommendation 2: SBA partially agrees with this recommendation.

The SBA acknowledges the importance of the recommendation and continues to focus on any potential UCP security issues in partnership with our Chief Information Security Officer (CISO). Our CISO's process is comprehensive and includes response to malicious cybersecurity incidents, availability of service, data retention, encryption of data at rest. After significant testing, the CISO clears the system for operation and GCBD does not operate without this clearance. SBA has already begun implementing internal and external assessments including malicious penetration testing to find and mitigate cyber security risks. This testing is ongoing. The external testing includes SBA's agency partner CISA (FAST) Team. The external team is conducting a web application security assessment, which does include looking deep into the source code of this application. In addition, SBA has opened the system to a small beta group of external beta testers. The CISO and GCBD are continuing to work collaboratively to address security issues through a successful launch. The Tech Team has successfully deployed updated code and remediated all Critical/High findings during our beta period. SBA and its partners are evaluating and prioritizing risks, and our CISO team is ensuring critical cybersecurity safeguards are fully implemented. SBA will provide update requested by GAO about this process, with a final update, when the process is complete.

SBA has provided GAO with the UCP project's business requirements document and system security requirements document. However, in agreement with GAO's recommendation SBA will document traceability between security requirements and how the developed system satisfies those requirements, specific to cybersecurity requirements.

GAO Recommendation 3: The Administrator of SBA should direct the Associate Administrator of SBA's Office of Government Contracting and Business Development to identify a delay in UCP system deployment as a risk and to identify mitigation strategies for addressing UCP system deployment delays.

SBA's Response to Recommendation 3: SBA agrees with this recommendation. SBA will include UCP system deployment delay as a risk in the risk register. Based on the evaluation of risks included in the risk register, SBA will determine any appropriate mitigation strategies needed.

GAO Recommendation 4: The Administrator of SBA should direct the Office of the Chief Information Officer to consider the probability and impact of accepted UCP deployment risks if deciding to authorize to operate the system.

SBA's Response to Recommendation 4: SBA partially agrees with this recommendation to consider the probability and impact of accepted UCP deployment risks when approving Authority to Operates (ATOs) for systems. SBA agrees that additional security measures would enhance the deployment risk assessment and validation of the UCP IT system. For the UCP project, SBA is following its standard operating procedure to grant an interim ATO with Plans of Action and Milestones (POAM) until all IT security controls are met before for a full ATO can be issued.

OCIO manages cybersecurity and privacy risk through its SBA SOP 90 47, Cybersecurity and Privacy Policy and related procedures which provide requirements for all systems being onboarded into the environment. This policy is in-line with Federal Information Security Modernization Act (FISMA) of 2014 requirements. All systems' risks are managed as part of SBA's Information Security Continuous Monitoring (ISCM) program. Security Control Assessments are performed annually with additional vulnerability scans performed on a

weekly basis. Plan of Actions and Milestones (POA&Ms) are created as needed to manage identified issues/risks for remediation.

Per SOP 90 47, Cybersecurity and Privacy Policy, “the Authorizing Official (AO) is the management official with the responsibility to ensure that the level of residual risk for an IT system or application is acceptable to the agency. Final Authority to Operate (ATO) a system approval lies with the AO. The SBA identifies the CIO as the agency AO”. All programmatic risks, including high-value security specific risks are being tracked in Folio and reported to the IT Dashboard on a monthly basis.

SBA will continue to evaluate and update any necessary security policies and procedures to address high-value IT systems, as we continue to implement IT modernization projects.

GAO Recommendation 5: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that risk registers or equivalent risk documentation explicitly state risk sources for IT modernization projects.

SBA’s Response to Recommendation 5

SBA disagrees with this recommendation. SBA engages all Major IT investments at various levels and stages within the IT enterprise governance lifecycle as part of the IT Investment risk management identification and assessment. Our current Standard Operating Procedures (SOPs), reference the Information Technology Management Reform Act of 1996 (Clinger-Cohen), the

Federal Information Technology Acquisition Reform Act (FITARA), OMB Circular A-11 section 55 Capital Planning Investment Control (CPIC), OMB Memorandum M-15-14, Management and Oversight of Federal Information Technology, and OMB Circular A-130, Managing Information as a Strategic Resource. All IT modernization investments/projects are required to follow SBA policies, processes, and/or procedures for risk management and mitigation, to include:

- The Business Investment Technology Council (BTIC), the governing body for SBA’s IT Portfolio, conducts bi-monthly BTIC meetings to review and assess project health and identify potential risks and budgetary constraints within the IT investment portfolio. The BTIC process is in accordance with SOP 90 82, IT Governance Investment Board.
- In accordance with SOP 90 44, SBA Information Technology and Capital Planning and Investment Control Standard Operating Procedures, monthly CIO rating meetings are conducted by the CIO to evaluate, monitor, and control baselines applying any necessary corrective measures for IT investments that are reported as part of the OMB monthly submission published to the IT Dashboard.
- As stated in SOP 90 45, CIO Responsibilities, the CIO will “review high-risk investments” and “evaluate IT investments to ensure projects are effectively managed (IT Dashboard CIO Ratings)”. This ensures that the CIO remains engaged with high-risk investments throughout the lifecycle.
- Stated in SOP 90 44, “OMB has defined required documents which demonstrate how SBA manages IT investment and how its governance processes are used when planning and implementing IT investment within the agency”. These artifacts include a Risk Management Plan (RMP) with defined and categorized risks, mitigation strategies, probability and impact scores, and contingency plans. All programmatic risks are documented in the RMP, as well as the Folio tool for tracking.

- OCIO manages cybersecurity and privacy risk through its SBA SOP 90 47, Cybersecurity and Privacy Policy and related procedures which provide requirements for all systems being onboarded into the environment. This policy is in-line with Federal Information Security Modernization Act (FISMA) of 2014 requirements. All systems' risks are managed as part of SBA's Information Security Continuous Monitoring (ISCM) program. Security Control Assessments are performed annually with additional vulnerability scans performed on a weekly basis. Plan of Actions and Milestones (POA&Ms) are created as needed to manage identified issues/risks for remediation.

OCIO will continue to engage IT Investments thru the Capital Planning Investment Control (CPIC) process (OMB Circular A-11 section 55) to improve the reporting and accuracy of IT investment cost, schedule, and performance of IT modernization projects. As an ongoing and iterative process, IT modernization projects are identified, approved, funded, and continually monitored throughout the lifecycle to ensure proper management, mitigation, and documentation of project risks. Additionally, as a result of the audit SBA will perform an internal review of its policies and procedures to ensure they are current. We will update them in accordance with federal guidance and mandates, as well as institute and communicate any changes to SBA's existing policies, and procedures to IT investments.

GAO Recommendation 6: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that parameters to categorize or analyze risks are clearly defined at the project level for IT modernization projects.

SBA's Response to Recommendation 6: See response to recommendation 5

GAO Recommendation 7: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that project risk management strategies are established and maintained for IT modernization projects.

SBA's Response to Recommendation 7: See response to recommendation 5

GAO Recommendation 8: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that risks are identified and documented for IT modernization projects for all phases of the development lifecycle, including deployment.

SBA's Response to Recommendation 8: See response to recommendation 5

GAO Recommendation 9: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that risks are evaluated, categorized and prioritized using defined parameters for IT modernization projects, and also to ensure that project risk mitigation plans are developed for IT modernization projects.

SBA's Response to Recommendation 9: See response to recommendation 5

GAO Recommendation 10: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that identified risk mitigations are connected to a project risk mitigation plan for IT modernization projects.

SBA's Response to Recommendation 10: See response to recommendation 5

GAO Recommendation 11: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that IT system acquisition plans and strategic plans for IT modernization projects contain all the information needed to manage cybersecurity risks, including how such risks will be managed, security milestones, how assets will be protected at a program or project level, and security-relevant criteria for selecting suppliers.

SBA's Response to Recommendation 11:

SBA disagrees with this recommendation as policies and procedures have been established and implemented to ensure that project risk management strategies are established and maintained for IT modernization projects.

SBA manages cybersecurity and privacy risk through its SBA SOP 90 47 Cybersecurity and Privacy Policy and related procedures which provide requirements for all systems being onboarded into the environment. This policy is in-line with Federal Information Security Modernization Act (FISMA) of 2014 requirements. All systems' risks are managed as part of SBA's Information Security Continuous Monitoring (ISCM) program. Security Control Assessments are performed annually with additional vulnerability scans performed on a weekly basis. Plan of Actions and Milestones (POA&Ms) are created as needed to manage identified issues/risks for remediation. Additionally, SBA has created its Cybersecurity Acquisition Language for insertion into all contracts with Information Technology (IT) related aspects.

For all IT and IT-related acquisitions, the instructions to offerors section must include the following sentences:

- 1) The offeror shall, as part of their technical proposal, provide a detailed description of how the proposed solution will adhere to the requirements included in the "Appendix – Cybersecurity Language for IT Acquisitions" section of this solicitation.
- 2) The offeror shall, as part of their technical proposal, provide a detailed description of how the proposed solution will manage and minimize supply chain risk, addressing the requirements included in the "Appendix – Cybersecurity Language for IT Acquisitions" section of this solicitation.

SBA will perform a review of said policies and procedures to ensure they are effective and communicated to all stakeholders.

GAO Recommendation 12: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that a traceability analysis is performed and documented for IT modernization projects to show the traceability of the security requirements to the design of the proposed IT system solution.

SBA's Response to Recommendation 12: SBA agrees with this recommendation. Additionally, SBA is currently updating its System Development Methodology (SDM), which includes related requirements as part of its capital planning process for approving new technology. SBA will ensure that traceability analysis requirements are included in this methodology. As part of the SDM development, SBA will update its Cybersecurity and Privacy policy and communicate these updates to all stakeholders.

GAO Recommendation 13: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that security-related subject matter experts are involved in the contractor selection process for IT modernization projects.

SBA's Response to Recommendation 13: SBA agrees with this recommendation. SBA will engage IT acquisitions to make the inclusion of IT security experts a requirement during vendor/contractor selections. SBA IT acquisitions will incorporate language in their existing policies and procedures for all IT modernization projects.

GAO Recommendation 14: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that integrated master schedules are developed for IT modernization projects using leading practices described in GAO's Schedule Assessment Guide.

SBA's Response to Recommendation 14: SBA agrees with this recommendation and will establish and implement policies and procedures to ensure that integrated master schedules are developed for IT modernization projects using leading practices described in GAO's Schedule Assessment Guide.

GAO Recommendation 15: The Administrator of SBA should direct the Office of the Chief Information Officer to establish and implement policies and procedures to ensure that cost estimates for IT modernization projects are developed using leading practices described in GAO's Cost Estimating and Assessment Guide.

SBA's Response to Recommendation 15:

SBA disagrees with this recommendation. SBA's current SOP 90 52 IT Investment Performance Baseline Management (PBM) references the leading practices in GAO-20-195G, Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs. All IT modernization investments/projects are required to follow SBA policies, processes, and/or procedures for cost estimation outlined in SOP 90 52.

OCIO will update policies and procedures in accordance with federal guidance and mandates, as well as institute and communicate any changes to SBA's existing policies, and procedures to IT investments.

Thank you for allowing SBA the opportunity to comment on GAO's draft report.

Sincerely,

LARRY STUBBLEFIELD

Digitally signed by LARRY STUBBLEFIELD

Date: 2024.10.04 15:19:31 -04'00'

Jaqueline L. Robinson-Burnette
Associate Administrator
Office of Government Contracting and Business Development

STEPHEN KUCHARSKI

Digitally signed by STEPHEN KUCHARSKI

Date: 2024.10.04 15:28:18 -04'00'

Steven Kucharski
Chief Information Officer
Office of the Chief Information Officer

Cc:
Jonathan Ticehurst, Assistant Director, Information Technology & Cybersecurity
Dr. Courtney LaFountain, Director, Financial Markets and Community Investment

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Carol C. Harris at (202) 512-4456 or HarrisCC@gao.gov

Courtney LaFountain at (202) 512-5463 or LaFountainC@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following staff made key contributions to this report: Jon Ticehurst (Assistant Director), Marshall Hamlett (Assistant Director), Lee Hinga (Analyst-in-Charge), Donna Epler, Emile Ettegui, Michael Farrell, Jason Lee, Lisa Maine, and Richard Zarrella.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [X](#), and [YouTube](#).

Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).

Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Sarah Kaczmarek, Managing Director, KaczmarekS@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548