U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. NW
Washington, DC 20548

September 30, 2025

Mr. Hartley Caldwell
Chief Information Officer
U.S. Small Business Administration
409 3rd Street, SW
Washington, DC 20416

Chief Information Officer Open Recommendations: Small Business Administration

Dear Mr. Caldwell:

I am writing to you with respect to your role as the Chief Information Officer (CIO) for the Small Business Administration (SBA). As an independent, non-partisan agency that works for Congress, GAO's mission is to support Congress in meeting its constitutional responsibilities and help improve the performance and ensure the accountability of the federal government. Our work includes investigating matters related to the use of public funds and evaluating programs and activities of the U.S. Government at the request of congressional committees and subcommittees, on the initiative of the Comptroller General, and as required by public laws or committee reports. Our duties include reporting our findings and recommending ways to increase economy and efficiency in government spending. The purpose of this letter is to provide an overview of the open, publicly available GAO recommendations to SBA that call for the attention of the CIO.

We identified recommendations that relate to the CIO's roles and responsibilities in effectively managing IT. They include strategic planning, investment management, and information security. We have previously reported on the significance of the CIO's role in improving the government's performance in IT and related information management functions.[1] Your attention to these recommendations will help ensure the secure and effective use of IT at the agency.

Currently, SBA has 20 open recommendations that call for the attention of the CIO. Each of these recommendations relates to a GAO High-Risk area: (1) Ensuring the Cybersecurity of the Nation or (2) Improving IT Acquisitions and Management.[2] In addition, GAO has designated four of the 20 as priority recommendations.[3] Fully implementing these open recommendations could significantly improve SBA's ability to deter threats and manage its critical systems, operations,

[1]See for example, GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, GAO-18-93 (Washington, D.C.: Aug. 2, 2018).

[2]GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, GAO-25-107743 (Washington, D.C.: Feb. 25, 2025).

[3]Priority recommendations are those that GAO believes warrant priority attention from heads of key departments or agencies. They are highlighted because, upon implementation, they may significantly improve government operations, for example, by realizing large dollar savings; eliminating mismanagement, fraud, and abuse; or making progress toward addressing a high-risk or duplication issue. Since 2015, GAO has sent letters to selected agencies to highlight the importance of implementing such recommendations.

and information. I have summarized selected recommendations here. See the enclosure for a full list and additional details on the GAO recommendations.

Ensuring the Cybersecurity of the Nation. SBA needs to fully establish a process for privacy workforce management. Specifically, we recommended that the agency fully define and document a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. Without involvement from designated privacy officials, SBA will be limited in its ability to identify staffing needs and ensure a well-qualified privacy workforce.

Improving IT Acquisitions and Management. SBA needs to better manage and track its IT resources. For example, we recommended that SBA develop a project risk management strategy and risk mitigation plan for the newly deployed Unified Certification Platform.[4] Until SBA establishes and implements policies and procedures that require specific plans to manage IT modernization risks, it will be limited in its ability to identify potential problems before they occur and mitigate adverse impacts.

SBA also needs to fully address statutory requirements for IT portfolio management. Specifically, we recommended that SBA complete annual reviews of its IT portfolio consistent with federal requirements. Until SBA implements this recommendation, it may miss opportunities to identify areas of duplication within its IT portfolio and to develop strategies to streamline operations and optimize resource allocation.

In addition to GAO's recommendations, the SBA Inspector General also has multiple open recommendations in the areas of cybersecurity and IT acquisitions and management. These include cybersecurity recommendations that relate to the agency's requirements under the Federal Information Security Modernization Act of 2014.[5] Similarly, SBA's independent Financial Statement Auditor has open recommendations related to deficiencies in IT controls at the agency. It will be important to address GAO, Inspector General, and Financial Statement Auditor recommendations.

Copies of this letter are being sent to the appropriate congressional committees and the Federal CIO. The letter will also be available at no charge on the GAO website at https://www.gao.gov. In addition, we sent a separate letter related to agencywide priority recommendations, which also conveys the importance of enhancing information technology and cybersecurity, to the Administrator of SBA.[6] We also sent a letter on key issues related to financial management in the federal government to the SBA Chief Financial Officer.[7]

---

[4]In 2023, the Small Business Administration initiated the Unified Certification Platform modernization project. The project deployed a new system intended to allow small businesses to more efficiently apply for and maintain certifications to the Small Business Administration's contracting assistance programs.

[5]The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002, enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

[6]GAO, *Priority Open Recommendations: Small Business Administration*, GAO-25-108048 (Washington, D.C.: May 01, 2025).

[7]GAO, *U.S. Consolidated Financial Statements: Key Issues for the Small Business Administration*, GAO-25-108147 (Washington, D.C.: July 23, 2025).

If you have any questions or would like to discuss any of the recommendations outlined in this letter, please do not hesitate to contact me at marinosn@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this letter. Our teams will continue to coordinate with your staff on addressing these 20 open recommendations that call for the attention of the CIO. I appreciate SBA's continued commitment and thank you for your personal attention to these important recommendations.

Sincerely,

//SIGNED//

Nick Marinos
Managing Director
Information Technology and Cybersecurity

Enclosure

cc: Mr. Gregory Barbaccia, Federal CIO, Office of Management and Budget

Enclosure

Chief Information Officer Open Recommendations to the Small Business Administration

This enclosure includes the open, publicly available GAO recommendations to the Small Business Administration (SBA) that call for the attention of its Chief Information Officer (CIO). We have divided these recommendations into two categories: (1) ensuring the cybersecurity of the nation and (2) improving IT acquisitions and management.

Ensuring the Cybersecurity of the Nation

Federal agencies depend on IT systems to carry out operations and process, maintain, and report essential information. The security of these systems and data is vital to protecting individual privacy and ensuring national security. Table 1 provides information on the open cybersecurity-related recommendation relevant to the SBA CIO.

Table 1: Open Chief Information Officer-related Cybersecurity Recommendation for the Small Business Administration

GAO report number	GAO report title	Recommendation
GAO-22-105065	Privacy: Dedicated Leadership Can Improve Programs and Address Challenges	The Administrator of the Small Business Administration should fully define and document a process for ensuring that the senior agency official for privacy or other designated privacy official is involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy. (Recommendation 58)*

*Indicates a priority recommendation.
Source: GAO summary based on previously issued reports. | GAO-25-108660

Improving IT Acquisitions and Management

Federal IT investments too frequently fail to deliver capabilities in a timely, cost-effective manner. Key management challenges—such as a lack of disciplined project planning and program oversight—continue to hamper effective acquisition and management of the government's IT assets. Table 2 provides information on the open IT acquisition and management-related recommendations relevant to the SBA CIO.

Table 2: Open Chief Information Officer (CIO)-related IT Acquisition and Management Recommendations for the Small Business Administration (SBA)

GAO report number	GAO report title	Recommendation
GAO-24-106137	Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements	The Administrator of SBA should ensure that the CIO of SBA develops guidance that requires a periodic review of the agency's policies related to cloud services, including any technical guidance and business requirements, to determine if improvements should be made. (Recommendation 42) The Administrator of SBA should ensure that the CIO of SBA develops guidance to put a cloud service level agreement in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses the Office of Management and Budget's (OMB) four required elements for service level agreements, including: continuous awareness of the confidentiality, integrity, and availability of its assets; a

GAO report number	GAO report title	Recommendation
		detailed description of roles and responsibilities; clear performance metrics; and remediation plans for non-compliance. (Recommendation 43) The Administrator of SBA should ensure that the CIO of SBA develops guidance regarding standardizing cloud service level agreements. (Recommendation 44)
GAO-25-106963	IT Modernization: SBA Urgently Needs to Address Risks on Newly Deployed System	The Administrator of SBA should direct the Associate Administrator of SBA's Office of Government Contracting and Business Development to expeditiously address critical Unified Certification Platform (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 CIO 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 CIO 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 CIO 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 CIO 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 CIO 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 CIO 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 CIO 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)

GAO report number	GAO report title	Recommendation
		The Administrator of SBA should direct the CIO 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 CIO 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 CIO 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 CIO 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 CIO 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)
GAO-25-107041	IT Portfolio Management: OMB and Agencies Are Not Fully Addressing Selected Statutory Requirements	The Administrator of SBA should direct its agency CIO to work with OMB to ensure that annual reviews of their IT portfolio are conducted in conjunction with the Federal CIO and the Chief Operating Officer or Deputy Secretary (or equivalent), as prescribed by the Federal Information Technology Acquisition Reform Act. (Recommendation 42)
		The Administrator of SBA should direct its agency CIO to ensure they conduct a review in conjunction with the investment's program manager and in consultation with the Federal CIO, for major IT investments that have been designated as high risk for four consecutive quarters, as prescribed by the Federal Information Technology Acquisition Reform Act, including identifying (1) the root causes of the high level of risk of the investment; (2) the extent to which these causes can be addressed (e.g., action items and due dates); and (3) the probability of future success (e.g., outcomes). (Recommendation 43)

*Indicates a priority recommendation.
Source: GAO summary based on previously issued reports. | GAO-25-108660

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.

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 X, LinkedIn, Instagram, and YouTube.
Subscribe to our 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

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us

Please Print on Recycled Paper.