

441 G St. NW
Washington, DC 20548

Accessible Version

January 28, 2026

Dr. Kelly Fletcher
Chief Information Officer
U.S. Department of State
2201 C St. NW
Washington, DC 20520

Chief Information Officer Open Recommendations: Department of State

Dear Dr. Fletcher:

I am writing to you with respect to your role as the Chief Information Officer (CIO) for the Department of State. 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 GAO recommendations to State 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 To your credit, the department has addressed hundreds of recommendations over the last year. Your continued attention to the remaining recommendations will help ensure the secure and effective use of IT at the department.

Currently, State has 95 open recommendations that call for the attention of the CIO, including 71 that are sensitive. 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 two of the 95 as priority recommendations.³ Fully implementing

¹See 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).

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

³Priority 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.

these open recommendations could significantly improve State's ability to deter threats and manage its critical systems, operations, and information. I have summarized selected recommendations here. See the enclosure for a full list, and additional details on the GAO recommendations, including the sensitive recommendations.

Ensuring the Cybersecurity of the Nation. State has taken significant action to address most of the recommendations related to technical security control deficiencies in the department's IT infrastructure made in our November 2024 report.⁴ However, the department needs to take additional steps to fully implement key risk management practices to secure the information systems it uses to carry out its mission. For example, we recommended that State develop and maintain a department-wide risk portfolio to prioritize significant cybersecurity risks per federal guidance. Until State implements this recommendation, the department will continue to have gaps in its understanding of cybersecurity risks, which may hinder its ability to protect its information systems.

We also recommended that the department fully implement all event logging requirements as directed by the Office of Management and Budget. Until State implements this recommendation, there is increased risk that the department will not have complete information from logs on its systems to detect, investigate, and remediate cyber threats.

Improving IT Acquisitions and Management. State needs to improve its management of the department's IT portfolio. For example, we recommended that State complete annual reviews of its IT portfolio consistent with federal requirements. Until State 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. We also recommended that the department develop and implement procedures for tracking software license usage. Implementing this recommendation will help ensure that State is able to fully leverage opportunities to reduce costs of duplicative or unnecessary licenses.

In addition, State needs to take additional steps to address its IT workforce challenges. For example, we recommended that State develop a plan that includes performance indicators, baselines, milestones, and targets, to monitor the progress of its IT recruitment programs and processes. Establishing and implementing this plan would help management to be fully informed about the effectiveness of, or make improvements to, the actions the department is taking to address the IT workforce challenges it faces.

In addition to GAO's recommendations, the State 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 department's requirements under the Federal Information Security Modernization Act of 2014.⁵ It will be important to address both GAO and Inspector General 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 department-wide priority recommendations, which also conveys the importance of addressing weaknesses in cybersecurity, to the Secretary

⁴GAO, Cybersecurity: State Needs to Implement Technical Controls and Incident Response Practices, GAO-25-106310SU (Washington, D.C.: Nov. 19, 2024).

⁵The 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).

of State.⁶

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 95 open recommendations that call for the attention of the CIO. I appreciate State'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

⁶GAO, Priority Open Recommendation: Department of State, GAO-25-108069 (Washington, D.C.: April 11, 2025).

Enclosure

Chief Information Officer Open Recommendations to the Department of State

This enclosure includes the open GAO recommendations to the Department of State that call for the attention of its Chief Information Officer (CIO), including the sensitive recommendations.⁷ 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 recommendations relevant to the State CIO.

Table 1: Open Chief Information Officer (CIO)-related Cybersecurity Recommendations for the Department of State

GAO report number	GAO report title	Recommendation
GAO-23-107012	Cybersecurity: State Needs to Expediently Implement Risk Management and Other Key Practices	<p>The Secretary of State should direct the CIO to develop and maintain a department-wide risk profile that prioritizes the department's most significant risks, including the areas of exposure and threats that State identified, consistent with federal requirements. (Recommendation 1)*</p> <p>The Secretary of State should direct the CIO to develop plans to mitigate vulnerabilities in the areas of exposure and threats that State previously identified. (Recommendation 2)</p> <p>The Secretary of State should direct the CIO to conduct bureau-level risk assessments for the 28 bureaus that owned information systems that we reviewed. (Recommendation 3)</p> <p>The Secretary of State should direct the CIO to ensure that State's information systems have valid authorizations to operate in accordance with department policies and federal guidance. (Recommendation 5)*</p> <p>The Secretary of State should direct the Assistant Secretary of State for Diplomatic Security to ensure that contingency plans for all high value asset systems are tested annually as required by department policies. (Recommendation 13)</p> <p>The Secretary of State should direct the CIO to update the October 2020 matrix to better ensure compliance with applicable department policies and federal guidance. The update could involve operationalizing the matrix describing the roles and responsibilities of the various bureaus so that the department as a whole can better address cybersecurity requirements. (Recommendation 14)</p>
GAO-24-105658	Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements	<p>The Secretary of State should ensure that the agency fully implements all event logging requirements as directed by Office of Management and Budget guidance. (Recommendation 11)</p>

⁷Due to the sensitive nature of GAO reports with report numbers ending in SU (controlled unclassified information), the recommendation language has been omitted.

GAO report number	GAO report title	Recommendation
GAO-25-106310SU	Cybersecurity: State Needs to Implement Technical Controls and Incident Response Practices	Recommendations 3, 4, 18, 19, 23, 33, 37, 40, 43-45, 88-90, 153, 158-162, 175, 176, 184, 187-189, 205-207, 215, 217, 230-236, 240, 241, 244, 245, 250, 254, 260-278, 372, 384, 393-395, 431, 437, and 438

*Indicates a priority recommendation.

Source: GAO summary based on previously issued reports. | GAO-26-108658

Notes: Due to the sensitive nature of GAO reports with report numbers ending in SU (controlled unclassified information), the recommendation language has been omitted.

State officials provided information that is intended to close recommendations 5 and 13 from [GAO-23-107012](#), and the remaining 71 open recommendations from GAO-25-106310SU. GAO is currently evaluating the information for completeness and verifying whether it addresses the open recommendations.

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 State CIO.

Table 2: Open Chief Information Officer (CIO)-related IT Acquisitions and Management Recommendations for the Department of State

GAO report number	GAO report title	Recommendation
GAO-22-105932	State Department: Additional Actions Needed to Address IT Workforce Challenges	<p>The Secretary of State should direct the Under Secretary for Management to develop a plan, including performance indicators, baselines, milestones, and targets, to monitor the progress of the department's IT recruitment programs and processes. (Recommendation 5)</p> <p>The Secretary of State should direct the Under Secretary for Management to ensure that relevant data related to IT recruitment activities are accurate and available to facilitate decision-making and enable the department to monitor and evaluate its performance in meeting its IT human capital goals. (Recommendation 6)</p> <p>The Secretary of State should direct the Under Secretary for Management to consider expanding the number of Civil Service IT positions that are available to external applicants year-round. (Recommendation 8)</p> <p>The Secretary of State should direct the Under Secretary for Management to create and document a strategy for using hiring flexibilities and recruitment incentives for IT recruiting. (Recommendation 9)</p> <p>The Secretary of State should direct the Under Secretary for Management to develop a plan, including performance indicators, baselines, milestones, and targets, to monitor the progress of the department's IT retention programs and processes. (Recommendation 10)</p> <p>The Secretary of State should direct the Under Secretary for Management to ensure that relevant data related to IT retention activities are accurate and available to facilitate decision-making and enable the department to monitor and evaluate its performance in meeting its IT human capital goals. (Recommendation 11)</p> <p>The Secretary of State should direct the Under Secretary for Management to obtain and track data related to employee morale issues for IT professionals in order to evaluate State's progress toward meeting its human capital goals. (Recommendation 12)</p> <p>The Secretary of State should direct the Under Secretary for Management to create and document a strategy on implementing meaningful rewards programs and on providing incentives to motivate and reinforce expected levels of performance and desired conduct in the IT workforce. (Recommendation 13)</p> <p>The Secretary of State should direct the Under Secretary for Management to create and document a strategy to develop a tailored approach to the use of available flexibilities, benefits, and incentives and tailoring benefits to current IT employees' needs for retention. (Recommendation 14)</p> <p>The Secretary of State should direct the Under Secretary for Management to obtain and track data on aligning Foreign Service IT employee performance expectations with agency goals to facilitate decision-making and enable the department to monitor and evaluate its performance in meeting its IT human capital goals. (Recommendation 15)</p> <p>The Secretary of State should direct the Under Secretary for Management to obtain and track data on aligning Civil Service IT employee performance expectations with agency goals to facilitate decision-making and enable the department to monitor and evaluate its performance in meeting its IT human capital goals. (Recommendation 16)</p>

GAO report number	GAO report title	Recommendation
GAO-24-105717	Federal Software Licenses: Agencies Need to Take Action to Achieve Additional Savings	<p>The Secretary of State should ensure that the agency consistently tracks software licenses that are currently in use for its widely used licenses by, at a minimum, developing and implementing procedures for tracking license usage. (Recommendation 9)</p> <p>The Secretary of State should ensure that the agency consistently compares the inventories of software licenses that are currently in use with information on purchased licenses to identify opportunities to reduce costs and better inform investment decision-making for its widely used licenses on a regular basis. At a minimum, it should develop and implement procedures for comparing the inventories of licenses in use to purchase records. (Recommendation 10)</p>
GAO-24-105980	Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements	<p>The Secretary of State should ensure that the department updates its artificial intelligence use case inventory to include all the required information, at minimum, and takes steps to ensure that the data in the inventory aligns with provided instructions. (Recommendation 23)</p>
GAO-25-107041	IT Portfolio Management: OMB and Agencies Are Not Fully Addressing Selected Statutory Requirements	<p>The Secretary of State should direct the department CIO to work with the Office of Management and Budget (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 (FITARA). (Recommendation 26)</p> <p>The Secretary of State should direct the department CIO to work with OMB to ensure that the Federal CIO is consulted in performing high-risk IT investment reviews, as prescribed by FITARA. (Recommendation 27)</p> <p>The Secretary of State should direct the department CIO to work with OMB to ensure that its high-risk IT investment reviews include a root cause analysis of the high level of risk and the probability of future successes (e.g., outcomes), as prescribed by FITARA. (Recommendation 28)</p>

Source: GAO summary based on previously issued reports. | GAO-26-108658