![GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE]

441 G St. NW
Washington, DC 20548

September 30, 2025

Mr. Rick Kryger
Deputy Chief Information Officer
U.S. Department of Labor
200 Constitution Avenue, NW
Washington, DC 20210

Chief Information Officer Open Recommendations: Department of Labor

Dear Mr. Kryger:

I am writing to you with respect to your role as the Deputy Chief Information Officer (CIO) for the Department of Labor (DOL). 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 DOL 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 department.

Currently, DOL has nine 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] Fully implementing these open recommendations could significantly improve DOL'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 recommendations.

---

[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).

GAO-25-108657 DOL CIO Recommendations

Ensuring the Cybersecurity of the Nation. DOL needs to take additional steps to improve its cybersecurity practices, including its risk management program. For example, we recommended that the department update its policies to require the use of risk assessments to inform its security control tailoring process for the department's information systems, and to prioritize its plan of action and milestones. Until DOL implements this recommendation, it may not be able to effectively identify and prioritize activities to mitigate cybersecurity risks that could result in the loss of sensitive data or compromise of department systems.

In addition, we recommended that DOL fully implement event logging requirements per federal guidance. Implementing this recommendation will help ensure that DOL has complete information to effectively detect, investigate, and remediate cyber threats.

Improving IT Acquisitions and Management. DOL needs to take additional steps to improve its IT operations, including meeting federal requirements for its IT portfolio reviews. For example, we recommended that DOL conduct a review 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. Until DOL implements this recommendation, investments with substantial cost, schedule, and performance problems may continue unabated without necessary corrective action.

We also recommended that the department establish a plan and time frame for completing an Internet of Things inventory as directed by the Office of Management and Budget. Until DOL does so, the department may lack visibility into the Internet of Things devices in its enterprise environment and have an inability to mitigate the associated cybersecurity risks.

In addition to GAO's recommendations, the DOL Inspector General also has multiple open recommendations in the area of cybersecurity. These include recommendations that relate to the department's requirements under the Federal Information Security Modernization Act of 2014.[3]

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[4] to the Secretary of Labor.[5]

---

[3]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).

[4]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.

[5]GAO, *Priority Open Recommendation: Department of Labor,* GAO-25-108003 (Washington, D.C.: May 7, 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 nine open recommendations that call for the attention of the CIO. I appreciate DOL'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 Department of Labor

This enclosure includes the open, publicly available GAO recommendations to the Department of Labor (DOL) 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 recommendations relevant to the DOL CIO.

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

GAO report number	GAO report title	Recommendation
GAO-19-384	Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges	The Secretary of Labor should update the department's policies to require (1) the use of risk assessments to inform control tailoring and (2) the use of risk assessments to inform plan of action and milestones prioritization. (Recommendation 23)
GAO-23-105482	Cloud Security: Selected Agencies Need to Fully Implement Key Practices	The Secretary of Labor should ensure that the agency's service level agreements with cloud service providers define performance metrics, including how they are measured and the enforcement mechanisms. (Recommendation 19)
GAO-24-105658	Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements	The Secretary of Labor should ensure that the agency fully implements all event logging requirements as directed by Office of Management and Budget guidance. (Recommendation 10)

Source: GAO summary based on previously issued reports. | GAO-25-108657

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 DOL CIO.

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

GAO report number	GAO report title	Recommendation
GAO-20-129	Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities	The Secretary of Labor should ensure that the agency fully implements each of the eight key IT workforce planning activities it did not fully implement. (Recommendation 8)

GAO-25-108657 DOL CIO Recommendations

GAO report number	GAO report title	Recommendation
GAO-23-105478	Unemployment Insurance: DOL Needs to Further Help States Overcome IT Modernization Challenges	The Secretary of the Department of Labor should direct the Office of Unemployment Insurance Modernization and the Office of the CIO to update their processes for unemployment insurance pilots to reflect leading practices for pilot design, and implement the leading pilot design practices that address the weaknesses that we identified on its future pilots. (Recommendation 1)
GAO-24-105980	Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements	The Secretary of Labor 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 22)
GAO-25-107041	IT Portfolio Management: OMB and Agencies Are Not Fully Addressing Selected Statutory Requirements	The Secretary of Labor should direct the department CIO to work with the Office of Management and Budget (OMB) to ensure that annual reviews of its 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 24)
		The Secretary of Labor should direct the department CIO to work with OMB 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 FITARA, 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 25)
GAO-25-107179	Internet of Things: Federal Actions Needed to Address Legislative Requirements	The Secretary of Labor should direct the CIO to establish a plan and time frame for completing the covered Internet of Things inventory, as directed by OMB. (Recommendation 4)

Source: GAO summary based on previously issued reports. | GAO-25-108657