![GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE]

441 G St. NW
Washington, DC 20548

Accessible Version

January 15, 2026

Mr. Perryn Ashmore
Acting Chief Information Officer
Office of Personnel Management
1900 E Street, NW
Washington, DC 20415-1000

Chief Information Officer Open Recommendations: Office of Personnel Management

Dear Mr. Ashmore:

I am writing to you with respect to your role as the Acting Chief Information Officer (CIO) for the Office of Personnel Management (OPM). 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 OPM 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, OPM has 16 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 two of the 16 as priority recommendations.[3] Fully implementing these open recommendations could

---

[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.

significantly improve OPM'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.

Ensuring the Cybersecurity of the Nation. OPM needs to take additional steps to fully implement incident response requirements. Specifically, we recommended that the agency fully implement all event logging requirements as directed by the Office of Management and Budget. Until OPM does so, there is increased risk that the agency will not have complete information from logs on its systems to detect, investigate, and remediate cyber threats.

Improving IT Acquisitions and Management. OPM needs to address challenges related to effectively acquiring and managing IT, including to improve its oversight of IT investments. For example, we recommended that OPM complete annual reviews of its IT portfolio in conjunction with the Federal CIO. Until OPM 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 OPM compare in-use software license inventories with information on purchased licenses to identify opportunities to reduce costs and better inform decision-making. At a minimum, the agency should consistently implement its procedures for comparing the inventories of licenses in use to purchase records. Until OPM implements this recommendation it is likely to miss opportunities to reduce costs on duplicative or unnecessary software licenses.

In addition to GAO's recommendations, the OPM 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.[4] 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 agency-wide priority recommendations, to the Director of OPM.[5]

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 16 open recommendations that call for the attention of the CIO. I appreciate OPM's continued commitment and thank you for your personal attention to these important recommendations.

Sincerely,

---

[4]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).

[5]GAO, Priority Open Recommendations: Office of Personnel Management, GAO-25-108081 (Washington, D.C.: August 6, 2025).

//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 Office of Personnel Management

This enclosure includes the open, publicly available GAO recommendations to the Office of Personnel Management (OPM) 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 OPM CIO.

Table 1: Open Chief Information Officer-related Cybersecurity Recommendation for the Office of Personnel Management

GAO report number	GAO report title	Recommendation
GAO-24-105658	Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements	The Director of the Office of Personnel Management should ensure that the agency fully implements all event logging requirements as directed by Office of Management and Budget guidance. (Recommendation 19)

Source: GAO summary based on previously issued reports. | GAO-26-108708

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 OPM CIO.

Table 2: Open Chief Information Officer (CIO)-related IT Acquisition and Management Recommendations for the Office of Personnel Management (OPM)

GAO report number	GAO report title	Recommendation
GAO-14-413	Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide	To ensure the effective management of software licenses, the Director of OPM should provide software license management training to appropriate agency personnel addressing contract terms and conditions, negotiations, laws and regulations, acquisition, security planning, and configuration management.
GAO-18-148	Information Technology Reform: Agencies Need to Improve Certification of Incremental Development	The Director of OPM should ensure that the CIO of OPM updates the agency's policy and process for the CIO's certification of major IT investments' adequate use of incremental development, in accordance with the Office of Management and Budget's (OMB) guidance on the implementation of the Federal Information Technology Acquisition Reform Act (FITARA), and confirm that it includes a description of the CIO's role in the certification process and a description of how CIO certification will be documented. (Recommendation 16)

GAO report number	GAO report title	Recommendation
GAO-20-129	Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities	The Director of OPM should ensure that the agency fully implements each of the eight key IT workforce planning activities it did not fully implement. (Recommendation 15)*
GAO-20-59	Information Management: Selected Agencies Need to Fully Address Federal Electronic Recordkeeping Requirements	The Director of OPM should establish a time frame to develop an inventory of electronic information systems used to store agency records that includes all of the required elements. (Recommendation 31)
		The Director of OPM should establish a time frame to update its policies and procedures to include all of the required electronic information system functionalities for recordkeeping systems. (Recommendation 33)
		The Director of OPM should establish a time frame to update the agency's policies and procedures on retention and management for email to include retaining electronic calendars and draft documents. (Recommendation 34)
GAO-23-105562	Information Management: Agencies Need to Streamline Electronic Services	The Director of OPM should establish a reasonable time frame for when the agency will be able to accept remote identity proofing with authentication, digitally accept access and consent forms from individuals who were properly identity proofed and authenticated, and post access and consent forms on the agency's privacy program website. (Recommendation 11)
GAO-24-105717	Federal Software Licenses: Agencies Need to Take Action to Achieve Additional Savings	The Director of OPM should ensure that the agency consistently tracks software licenses that are currently in use for its widely used licenses by, at a minimum, consistently implementing its procedures for tracking license usage. (Recommendation 13)
		The Director of OPM should ensure that the agency 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 consistently implement its procedures for comparing the inventories of licenses in use to purchase records. (Recommendation 14)*
GAO-24-106137	Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements	The Director of OPM should ensure that the CIO of OPM updates 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 OMB required element for service level agreements: remediation plans for non-compliance. (Recommendation 41)

GAO report number	GAO report title	Recommendation
GAO-25-107041	IT Portfolio Management: OMB and Agencies Are Not Fully Addressing Selected Statutory Requirements	The Director of OPM 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, as prescribed by FITARA. (Recommendation 40)
		The Director of OPM 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 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 41)
GAO-25-107114	Cloud Computing: Selected Agencies Need to Implement Updated Guidance for Managing Restrictive Licenses	The Director of OPM should update and implement guidance to fully address identifying, analyzing, and mitigating the impacts of restrictive software licensing practices on cloud computing efforts. (Recommendation 9)
		The Director of OPM should assign and document responsibility for identifying and managing potential impacts of restrictive software licensing practices across the agency. (Recommendation 10)
GAO-25-107179	Internet of Things: Federal Actions Needed to Address Legislative Requirements	The Director of OPM should direct the CIO to establish a plan and time frame for completing the covered Internet of Things inventory, as directed by OMB. (Recommendation 9)

*Indicates a priority recommendation.