![GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE]

441 G St. NW
Washington, DC 20548

Accessible Version

September 3, 2025

Mr. Paul McInerny
Chief Information Officer
U.S. Department of the Interior
1849 C Street, NW
Washington, DC 20240

Chief Information Officer Open Recommendations: Department of the Interior

Dear Mr. McInerny:

I am writing to you with respect to your role as the Chief Information Officer (CIO) for the Department of the Interior. 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 Interior 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, Interior has 13 open recommendations that call for the attention of the CIO, including two that are relevant to component-level CIOs. 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 one of the 13 as a priority

---

[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).

recommendation.[3] Fully implementing these open recommendations could significantly improve Interior's ability to address 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. Interior needs to make progress in its cybersecurity incident response preparedness by taking steps to improve its investigation and remediation capabilities. Specifically, we recommended that the department fully implement all event logging requirements as directed by the Office of Management and Budget. Until Interior does so, 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. Interior needs to improve its oversight of IT investments. For example, we recommended that the department implement leading practices in executive-level IT governance for major IT investments. Implementing this recommendation will provide Interior with greater assurance that it will expend funds for future IT investments in the most cost-effective way and will support, rather than detract from, mission needs.

We also recommended that the department complete annual reviews of its IT portfolio consistent with federal requirements. Until Interior 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 Interior Inspector General also has multiple open recommendations in the areas of cybersecurity and IT acquisitions and management. These include recommendations that relate to the department'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 department-wide priority recommendations to the Secretary of the Interior.[5]

---

[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.

[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*: *Department of the Interior,* GAO-25-108096 (Washington, D.C.: May 09, 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 13 open recommendations that call for the attention of the CIO. I appreciate Interior'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. James Rolfes, Associate CIO, Bureau of Land Management
        Mr. Kevin Sturlaugson, Associate CIO, Bureau of Indian Affairs
        Mr. Gregory Barbaccia, Federal CIO, Office of Management and Budget

Enclosure

Chief Information Officer Open Recommendations to the Department of the Interior

This enclosure includes the open, publicly available GAO recommendations to the Department of the Interior 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 Interior CIO.

Table 1: Open Chief Information Officer-related Cybersecurity Recommendation for the Department of the Interior

GAO report number	GAO report title	Recommendation
GAO-24-105658	Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements	The Secretary of the Interior should ensure that the agency fully implements all event logging requirements as directed by Office of Management and Budget guidance. (Recommendation 8)

Source: GAO summary based on previously issued reports. | GAO-25-108536

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 Interior CIO.

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

GAO report number	GAO report title	Recommendation
GAO-15-431	Telecommunications: Agencies Need Better Controls to Achieve Significant Savings on Mobile Devices and Services	To help the department effectively manage spending on mobile devices and services, the Secretary of the Interior should ensure an inventory of mobile devices and services is established department-wide (i.e., all components' devices and associated services are accounted for).
		To help the department effectively manage spending on mobile devices and services, the Secretary of the Interior should ensure a reliable department-wide inventory of mobile service contracts is developed and maintained.
GAO-21-209	Oil and Gas: Interior Should Strengthen Management of Key Data Systems Used to Oversee Development on Federal Lands	The Secretary of the Interior should direct the CIO to update Interior's Solution Development Lifecycle Guide or other relevant IT policies and guidance to address how program offices are to implement agile methodologies for the development of software. (Recommendation 6)

GAO report number	GAO report title	Recommendation
GAO-21-492T	Indian Education: Schools Need More Assistance to Provide Distance Learning	The Director of the Bureau of Indian Education should work with the Assistant Secretary-Indian Affairs' Office of Information Management Technology to develop and implement written policies and procedures for collecting timely information on Bureau of Indian Education -operated schools' technology needs. (Recommendation 2)
GAO-24-105980	Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements	The Secretary of the Interior should ensure that the department develops a plan to either achieve consistency with Executive Order 13960 section 5 for each artificial intelligence (AI) application or retires AI applications found to be developed or used in a manner that is not consistent with the order. (Recommendation 19)
		The Secretary of the Interior should ensure that the department (a) reviews the agency's authorities related to applications of AI and (b) develops and submits to the Office of Management and Budget (OMB) plans to achieve consistency with the Regulation of AI Applications memorandum (M-21-06). (Recommendation 20)
		The Secretary of the Interior should ensure that the department updates its AI 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 21)
GAO-24-107223	Oil and Gas: Interior Urgently Needs Leadership and Oversight to Address IT System Development Failure	The Secretary of the Interior should direct Interior's CIO to strengthen IT leadership and oversight by implementing leading practices in executive-level IT governance for major IT investments including the Automated Fluid Minerals Support System 2 replacement. (Recommendation 2)*
		The Director of the Bureau of Land Management should document concurrence from Interior's CIO that Bureau of Land Management is implementing policies and procedures for developing IT systems, including the Automated Fluid Minerals Support System 2 replacement, that are in alignment with the CIO's direction. Such policies and procedures should include that root cause analyses and corrective action plans are completed for projects that exceed established cost, schedule, and performance thresholds. (Recommendation 3)
GAO-25-107041	IT Portfolio Management: OMB and Agencies Are Not Fully Addressing Selected Statutory Requirements	The Secretary of the Interior should direct the department 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 (FITARA). (Recommendation 29)
		The Secretary of the Interior should direct the department CIO to ensure that the Federal CIO is consulted in performing high-risk IT investment reviews, as prescribed by FITARA. (Recommendation 30)
		The Secretary of the Interior should direct the department CIO to ensure that its high-risk IT investment reviews document the extent to which these causes can be addressed (e.g., action items with due dates), as prescribed by FITARA. (Recommendation 31)

*Indicates a priority recommendation.