U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. NW
Washington, DC 20548

July 28, 2025

Mr. Antoine McCord
Chief Information Officer
Department of Homeland Security
Washington, DC 20528

Chief Information Officer Open Recommendations: Department of Homeland Security

Dear Mr. McCord:

I am writing to you with respect to your role as the Chief Information Officer (CIO) for the Department of Homeland Security (DHS). 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, evaluating programs and activities of the U.S. Government at the request of congressional committees and subcommittees or 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 DHS 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, DHS has 43 open recommendations that call for the attention of the CIO, including 15 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, (2) Improving IT Acquisitions and Management, or (3) Strengthening DHS IT and Financial Management Functions.[2] In addition, GAO has designated seven of the 43 as priority recommendations.[3] Fully implementing these open recommendations could significantly improve DHS's ability to deter threats and manage its critical systems, operations, and information. I have summarized selected recommendations here. See

[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.

the enclosure for a full list and additional details on the recommendations.

Ensuring the Cybersecurity of the Nation. DHS needs to take additional steps to secure the information systems it uses to carry out its mission. For example, we recommended that the department fully implement Federal Risk and Authorization Management Program requirements, to include issuing an authorization for the cloud service used by the department for one of its systems. Implementing this recommendation will help ensure that DHS fully identifies the security risk of the system.

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

Improving IT Acquisitions and Management. DHS needs to address challenges related to effectively acquiring and managing IT. This includes addressing significant program management shortcomings for its Homeland Advanced Recognition Technology program.[4] For example, we made recommendations that the department revise the program's cost and schedule estimates by incorporating best practices we have identified in prior work. Implementing these recommendations will help DHS develop reliable estimates that enable senior leadership to make informed decisions regarding the program's future.

In addition, DHS needs to fully address statutory requirements for IT portfolio management. For example, we recommended DHS complete annual reviews of its IT portfolio consistent with federal requirements. Until DHS implements this recommendation, investments with substantial cost, schedule, and performance problems may continue unabated without necessary corrective action.

Strengthening DHS IT and Financial Management Functions. DHS needs to continue its efforts to modernize its financial management systems. Our recommendations in this area are directed to the Joint Program Management Office implementing the new financial systems, within the Office of the Chief Financial Officer.[5] This type of systems project needs both the Chief Financial Officer and CIO working together. This collaboration will help reduce project risks and increase the likelihood of successful financial system implementations. For example, we recommended that the Joint Program Management Office work with Coast Guard to remediate known issues identified from testing, prior to declaring full operational capability for the Coast Guard's ongoing financial systems modernization efforts. Implementing this recommendation will increase the likelihood that the new system will meet its mission needs and will produce reliable data for management decision-making and financial reporting.

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 enhancing information technology and cybersecurity, to the Secretary of Homeland Security.[6]

---

[4]The Homeland Advanced Recognition Technology program was initiated in 2016 to replace DHS's Automated Biometric Identification System with a centralized DHS-wide biometric database that stores and manages over 290 million individuals' personally identifiable information, including biographic and biometric information.

[5]GAO, *DHS Financial Management: Actions Needed to Improve Systems Modernization and Address Coast Guard Audit Issues*, GAO-23-105194 (Washington, D.C.: Feb. 28, 2023).

[6]GAO, *Priority Open Recommendations: Department of Homeland Security,* GAO-25-108010 (Washington, D.C.: May 14, 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 43 open recommendations that call for the attention of the CIO. I appreciate DHS'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. Charles R. Armstrong, CIO, Federal Emergency Management Agency

Rear Admiral Russell E. Dash, Assistant Commandant and CIO, Command, Control, Communications, Computers, and Information Technology Directorate, United States Coast Guard

Mr. Robert Kuykendall, Acting CIO, United States Secret Service

Ms. Holly Mehringer, Acting Chief Financial Officer, Office of the Chief Financial Officer, Department of Homeland Security

Mr. Rob Thorne, Acting CIO, United States Immigration and Customs Enforcement

Mr. Greg Barbaccia, Federal CIO, Office of Management and Budget

Enclosure

Chief Information Officer Open Recommendations to the Department of Homeland Security

This enclosure includes the open, publicly available GAO recommendations to the Department of Homeland Security (DHS) that call for the attention of its Chief Information Officer (CIO). We have divided these recommendations into three categories: (1) ensuring the cybersecurity of the nation, (2) improving IT acquisitions and management, and (3) strengthening DHS IT and financial management functions.

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 DHS CIO.

Table 1: Open Chief Information Officer-related Cybersecurity Recommendations for the Department of Homeland Security (DHS)

GAO report number	GAO report title	Recommendation
GAO-23-105466	Cybersecurity: Secret Service Has Made Progress Toward Zero Trust Architecture, but Work Remains	The Director of the Secret Service should instruct the agency's Chief Information Officer to implement outstanding Office of Management and Budget requirements for transitioning to internet protocol version 6, particularly in regard to upgrading its public-facing systems. (Recommendation 1)
GAO-23-105482	Cloud Security: Selected Agencies Need to Fully Implement Key Practices	The Secretary of Homeland Security 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 12) The Secretary of Homeland Security should ensure that the agency fully implements the Federal Risk and Authorization Management Program requirements for its selected software as a service system 2, to include issuing an authorization for the cloud service. (Recommendation 15)
GAO-23-106701	DHS Annual Assessment: Major Acquisition Programs Are Generally Meeting Goals, but Cybersecurity Policy Needs Clarification	The Secretary of Homeland Security should ensure that, as the department updates its Instruction 102-01-012, it clarifies (1) which major acquisition programs are required to have completed cybersecurity risk recommendation memorandums prior to acquisition decision events, and (2) when exemptions apply.
GAO-24-105658	Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements	The Secretary of Homeland Security should ensure that the agency fully implements all event logging requirements as directed by Office of Management and Budget guidance. (Recommendation 6)
GAO-25-106795	Cybersecurity Workforce: Departments Need to Fully Implement Key Practices	The Secretary of Homeland Security should ensure that DHS fully addresses the practices described in our report associated with evaluating and revising a workforce action plan. (Recommendation 6) The Secretary of Homeland Security should ensure that DHS identify and analyze the effectiveness of its mitigation actions on the workforce challenges. (Recommendation 7)

Source: GAO summary based on previously issued reports. | GAO-25-108460

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 DHS CIO.

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

GAO report number	GAO report title	Recommendation
GAO-19-60	U.S. Secret Service: Action Needed to Address Gaps in IT Workforce Planning and Management Practices	The Director [of the Secret Service] should ensure that the Office of Human Resources and the Office of the Chief Information Officer (OCIO) adjust their recruitment and hiring plans and activities, as necessary, after establishing and tracking metrics for assessing the effectiveness of these activities for the IT workforce. (Recommendation 9)
		The Director [of the Secret Service] should ensure that the CIO (1) defines the required training for each IT workforce group, (2) determines the activities that OCIO will include in its IT workforce training and development program based on its available training budget, and (3) implements those activities. (Recommendation 10)
		The Director [of the Secret Service] should ensure that the CIO ensures that the IT workforce completes training specific to their positions (after defining the training required for each workforce group). (Recommendation 11)
		The Director [of the Secret Service] should ensure that the CIO collects and assesses performance data (including qualitative or quantitative measures, as appropriate) to determine how the IT training program contributes to improved performance and results (once the training program is implemented). (Recommendation 12)
GAO-20-213	Agile Software Development: DHS Has Made Significant Progress in Implementing Leading Practices, but Needs to Take Additional Actions	The Secretary [of Homeland Security] should ensure that the CIO, in collaboration with the Chief Procurement Officer, through the Homeland Security Acquisition Institute, establish Agile training requirements for senior stakeholders. (Recommendation 5)
		The Secretary [of Homeland Security] should ensure that the CIO, in collaboration with the Chief Procurement Officer, through the Homeland Security Acquisition Institute, establish Agile training requirements for staff outside of the acquisition workforce but assigned to Agile programs. (Recommendation 7)
GAO-22-105092	Coast Guard: Actions Needed to Enhance IT Program Implementation	The Commandant of the United States Coast Guard should direct the Deputy Commandant for Mission Support to develop network capacity planning policies and procedures that address the leading practices we identified, including (1) compiling a complete and accurate inventory of hardware, software, and configurations; (2) identifying traffic growth predictions; (3) prioritizing network traffic; (4) performing simulations and what-if-analyses; and (5) continually monitoring the health of the infrastructure to ensure it is meeting demand and mission needs. (Recommendation 1)
		The Commandant of the United States Coast Guard should

GAO report number	GAO report title	Recommendation
		direct the Deputy Commandant for Mission Support to implement the leading practices for network capacity planning that we identified, including (1) compiling a complete and accurate inventory of hardware, software, and configurations; (2) identifying traffic growth predictions; (3) prioritizing network traffic; (4) performing simulations and what-if-analyses; and (5) continually monitoring the health of the infrastructure to ensure it is meeting demand and mission needs. (Recommendation 2)*
		The Commandant of the United States Coast Guard should direct the Deputy Commandant for Mission Support to establish a comprehensive and accurate inventory of all operational technology, including industrial control systems and supervisory control and data acquisition systems. (Recommendation 3)
		The Commandant of the United States Coast Guard should direct the Deputy Commandant for Mission Support to develop a plan or strategy for aligning all operational technology to the Department of Defense risk management framework, including time frames for completing the alignment. (Recommendation 4)
		The Commandant of the United States Coast Guard should direct the Deputy Commandant for Mission Support to ensure that the plan or strategy for aligning all operational technology to the Department of Defense risk management framework is effectively implemented. (Recommendation 5)*
		The Commandant of the United States Coast Guard should direct the Deputy Commandant for Mission Support to send its list of cloud services that do not meet Federal Risk and Authorization Management Program requirements to the appropriate agency head for submission to the Federal CIO. (Recommendation 7)
		The Commandant of the United States Coast Guard should direct the Deputy Commandant for Mission Support to update the service's cloud strategy and other relevant documentation to include a cross-walk of new and old skills and occupational categories, and to conduct a skills gap analysis. (Recommendation 8)
GAO-23-105959	Biometric Identity System: DHS Needs to Address Significant Shortcomings in Program Management and Privacy	The Secretary of DHS should direct the Office of Biometric Identity Management (OBIM) Director to update the cost estimate for the Homeland Advanced Recognition Technology (HART) program to account for all costs and incorporate the best practices called for in the GAO *Cost Estimating and Assessment Guide*. (Recommendation 1)
		The Secretary of DHS should direct the OBIM Director to revise the schedule estimate for the HART program that incorporates the best practices called for in the GAO *Schedule Assessment Guide*. (Recommendation 2)*
		The Secretary of DHS should direct the OBIM Director to coordinate with the Privacy Office to establish and implement a timeline for updating the HART privacy impact assessment to fully describe the categories of individuals whose data will be stored in HART and the partners with whom the system shares information. (Recommendation 3)
		The Secretary of DHS should direct the Privacy Office to describe planned methodologies for determining that all

GAO report number	GAO report title	Recommendation
		privacy controls are implemented correctly and operating as intended for future control assessments of the HART program. (Recommendation 4) The Secretary of DHS should direct the Privacy Office to develop a timeline for completing the planned HART privacy compliance review. (Recommendation 5) The Secretary of DHS should direct the OBIM Director to coordinate with the Privacy Office to establish and implement plans for correcting seven remaining privacy deficiencies identified in the HART privacy impact assessment. (Recommendation 6) The Secretary of DHS should direct the Privacy Office to ensure the complete HART authorization package is reviewed by the office prior to future system authorizations. (Recommendation 7) The Secretary of DHS should direct the OBIM Director to establish and implement a timeline for maintaining a reliable inventory of information sharing and access agreements with partners that share data with HART. (Recommendation 8) The Secretary of DHS should direct the OBIM Director to establish and maintain a process for ensuring that partners that provide data to HART have used the system's services to help to appropriately dispose of personally identifiable information from the system, in accordance with applicable records retention schedules. (Recommendation 9)
GAO-24-105980	Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements	The Secretary of Homeland Security 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 16) The Secretary of Homeland Security should ensure that the department (a) reviews the department'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 17) The Secretary of Homeland Security 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 18)
GAO-24-106137	Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements	The Secretary of Homeland Security should ensure that the CIO of DHS updates its guidance to put a cloud service level agreement (SLA) in place with every vendor when a cloud solution is deployed. The guidance should include language that addresses OMB's required elements for SLAs, including remediation plans for non-compliance. (Recommendation 12) The Secretary of Homeland Security should ensure that the CIO of DHS develops guidance regarding standardizing cloud SLAs. (Recommendation 13)
GAO-24-106153	DHS Hiring: Additional Actions Needed to Enhance Vetting	The DHS Chief Security Officer should ensure that the IT vetting system that is under development includes

GAO report number	GAO report title	Recommendation
	Processes Across the Department	enhanced capabilities, such as being able to track information for DHS priority positions and distinguish between different types of reciprocity. (Recommendation 2)
GAO-25-107041	IT Portfolio Management: OMB and Agencies Are Not Fully Addressing Selected Statutory Requirements	The Secretary of Homeland Security 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 17) The Secretary of Homeland Security 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 18) The Secretary of Homeland Security should direct the department CIO, in conjunction with the project manager, to conduct high-risk IT investment reviews, as prescribed by FITARA. (Recommendation 19) The Secretary of Homeland Security should direct the department CIO to work with OMB to ensure that its high-risk IT investment reviews include the extent to which these causes can be addressed (e.g., action items and due dates) and the probability of future successes (e.g., outcomes), as prescribed by FITARA. (Recommendation 20)
GAO-25-108085	Federal Protective Service: Actions Needed to Address Critical Guard Oversight and Information System Problems	The DHS CIO should determine whether to terminate and replace the Post Tracking System, or make corrective actions to the existing system, including a schedule for providing tenants with timely communication of guard shortages. (Recommendation 4)*

*Indicates a priority recommendation.
Source: GAO summary based on previously issued reports. | GAO-25-108460

Strengthening DHS IT and Financial Management Functions

DHS has made progress but needs to address remaining challenges in its financial management systems. To address these issues, DHS needs to execute a multiyear plan that includes modernizing its financial management systems at Coast Guard, the Federal Emergency Management Agency, and U.S. Immigration and Customs Enforcement. Table 3 provides information on the open financial management system-related recommendations relevant to the DHS CIO.

Table 3: Open Chief Information Officer-related Financial Management System Recommendations for the Department of Homeland Security (DHS)

GAO report number	GAO report title	Recommendation
GAO-23-105194	DHS Financial Management: Actions Needed to Improve Systems Modernization and Address Coast Guard Audit Issues	DHS's Under Secretary for Management should ensure that the Joint Program Management Office works with Coast Guard to remediate known issues identified from testing, prior to declaring full operational capability for the ongoing financial systems modernization efforts. (Recommendation 1)*
		DHS's Under Secretary for Management should ensure that the Joint Program Management Office works with the Federal Emergency Management Agency to remediate issues as they arise from user testing prior to moving forward with subsequent milestones for the ongoing financial systems modernization efforts. (Recommendation 2)*
		DHS's Under Secretary for Management should ensure that the Joint Program Management Office works with the U.S. Immigration and Customs Enforcement agency to remediate issues as they arise from user testing prior to moving forward with subsequent milestones for the ongoing financial systems modernization efforts. (Recommendation 3)*

*Indicates a priority recommendation.
Source: GAO summary based on previously issued reports. | GAO-25-108460