U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

Accessible Version

May 29, 2025

Ms. Katherine Arrington
Performing the Duties of Chief Information Officer
U.S. Department of Defense
1000 Defense Pentagon
Washington, D.C. 20301-1000

Chief Information Officer Open Recommendations: Department of Defense

Dear Ms. Arrington:

I am writing to you with respect to your role performing the duties of the Chief Information Officer (CIO) of the Department of Defense (DOD). 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 DOD 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, DOD has 54 open recommendations that call for the attention of the CIO, including seven that are directed 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, (3) DOD Business Systems Modernization, and (4) DOD Financial Management.[2] In addition, GAO has designated four of the 54 as priority recommendations.[3]

---

[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

Fully implementing these open recommendations could significantly improve DOD'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.

Ensuring the Cybersecurity of the Nation. DOD needs to better secure the information systems the department uses to carry out its mission. For example, we recommended that the DOD CIO align policy and system requirements to enable the department to have better cyber incident reporting awareness. Implementing this recommendation will help ensure DOD's leadership has accurate information on the department's cybersecurity posture.

DOD also needs to develop and implement plans and processes related to supply chain risk management activities. For example, we recommended DOD commit to a time frame to fully implement supply chain risk management reviews for potential suppliers. Implementing this recommendation will help ensure the department has enough information to manage its supply chain risks.

Further, DOD needs to take steps to improve its cyber hygiene.[4] For example, we recommended that DOD assess whether senior leadership has sufficient information to make risk-based decisions, including on the implementation progress of cybersecurity initiatives. Implementing this recommendation will better position leaders to be aware of the cyber risks DOD faces and make effective decisions to manage such risks.

Improving IT Acquisitions and Management. DOD needs to address challenges related to effectively acquiring and managing IT, including improving the efficient delivery and development of cloud services. For example, we recommended that the department establish a consistent and repeatable cost savings tracking mechanism for the deployment and migration of cloud services. Implementing this recommendation will help ensure that DOD effectively oversees and manages these services.

In addition, DOD needs to take action to improve IT and software management and modernization efforts. This includes incorporating key change management practices and building a workforce—with critical skills and competencies—that can implement these reforms. For example, we recommended that DOD take steps to implement planned software modernization and acquisition reforms. Implementing this recommendation will help DOD achieve its goal of rapidly delivering software to its users.

DOD Business Systems Modernization. DOD needs to better operate, maintain, and modernize its business systems to support key areas such as personnel, financial management, health care, and logistics. This includes improving business and financial system oversight.

For example, we recommended that the department ensure that its business and financial system certification data are complete and accurate. Implementing this recommendation will provide DOD with better assurance that its systems are fully complying with statutory

---

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, including DOD, to highlight the importance of implementing such recommendations.

[4]Cyber hygiene is a set of practices for managing the most common and pervasive cybersecurity risks.

requirements.

In addition, we recommended that DOD clarify the roles, responsibilities, and relationships among the various entities involved in developing the DOD business enterprise architecture. Until DOD implements this recommendation, it risks not ensuring that the department will effectively use the business enterprise architecture as a mechanism to streamline and modernize its business systems environment.

DOD Financial Management. DOD needs to take steps to improve the accuracy of financial reporting of its assets and spending to ensure accountability over department resources and physical assets. For example, we recommended that the department establish a road map to document current and future states of financial management systems as well as gaps, resource requirements, and planned solutions. Implementing this recommendation will assist DOD with analyzing performance gaps related to its financial management systems.

In addition, we recommended that the department establish mechanisms to incorporate strategic planning for the government and contract workforce that support the development and maintenance of financial management systems. Implementing this recommendation will help ensure the DOD maintains systems that can help achieve a clean audit opinion.

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 are sending two separate letters, one relating to agency-wide priority recommendations and the other on open recommendations and key issues related to financial management. These letters will be sent to the Secretary of Defense and DOD's Chief Financial Officer, respectively.[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 54 open recommendations that call for the attention of the CIO. I appreciate DOD's continued commitment and thank you for your personal attention to these important recommendations.
Sincerely,

//SIGNED//

Nicholas Marinos
Managing Director
Information Technology and Cybersecurity

Enclosure

cc: Mr. Leonel Garciga, CIO, Army
Ms. Jane Rathbun, CIO, Navy

[5]We discuss the importance of addressing cybersecurity risks in the letter sent to the Secretary.

Ms. Jennifer Orozco, Acting CIO, Air Force
Mr. Robert G. Salesses, Performance Improvement Officer and Director of Administration and Management
Ms. Jeanette M. Duncan, CIO, Defense Counterintelligence and Security Agency
Mr. Greg Barbaccia, Federal CIO, Office of Management and Budget

Enclosure

Chief Information Officer Open Recommendations to the Department of Defense

This enclosure includes the open, publicly available GAO recommendations to the Department of Defense (DOD) that call for the attention of its Chief Information Officer (CIO). We have divided these recommendations into four categories: (1) ensuring the cybersecurity of the nation, (2) improving IT acquisitions and management, (3) DOD business systems modernization, and (4) DOD financial 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 DOD CIO.

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

GAO report number	GAO report title	Recommendation
GAO-20-241	Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene	The Secretary of Defense should ensure that the DOD CIO takes appropriate steps to ensure implementation of the DOD Cybersecurity Culture and Compliance Initiative tasks. (Recommendation 1)*
		The Secretary of Defense should ensure that DOD components develop plans with scheduled completion dates to implement the four remaining Cybersecurity Discipline Implementation Plan tasks overseen by DOD CIO. (Recommendation 2)*
		The Secretary of Defense should ensure that DOD components accurately monitor and report information on the extent that users have completed the Cyber Awareness Challenge training as well as the number of users whose access to the network was revoked because they have not completed the training. (Recommendation 4)
		The Secretary of Defense should ensure that the DOD CIO assesses the extent to which senior leaders have more complete information to make risk-based decisions—and revise the recurring reports (or develop a new report) accordingly. Such information could include DOD's progress on implementing (a) cybersecurity practices identified in cyber hygiene initiatives and (b) cyber hygiene practices to protect DOD networks from key cyberattack techniques. (Recommendation 7)*

GAO report number	GAO report title	Recommendation
GAO-23-105084	DOD Cybersecurity: Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Reported and Shared	The Secretary of Defense should ensure that the DOD CIO, Commander of U.S. Cyber Command, and Commander of the Joint Force Headquarters-Department of Defense Information Network align policy and system requirements to enable DOD to have enterprise-wide visibility of cyber incident reporting to support tactical, strategic, and military strategies for response. (Recommendation 2) The Secretary of Defense should ensure that the DOD CIO, Commander of U.S. Cyber Command, and Commander of Joint Force Headquarters-Department of Defense Information Network include in new guidance on incident reporting detailed procedures for identifying, reporting, and notifying leadership of critical cyber incidents. (Recommendation 3)
GAO-23-105612	Information and Communications Technology: DOD Needs to Fully Implement Foundational Practices to Manage Supply Chain Risks	The Secretary of Defense should direct the Undersecretary of Defense for Acquisition and Sustainment and the DOD CIO to commit to a time frame to fully implement a process to conduct supply chain risk management reviews of potential suppliers. (Recommendation 2) The Secretary of Defense should direct the Undersecretary of Defense for Acquisition and Sustainment and the DOD CIO to commit to a time frame to fully implement organizational counterfeit detection procedures for products prior to deployment. In doing so, the department should take into consideration the results of its pilot efforts of applicable tools. (Recommendation 3)
GAO-24-106179	Personnel Vetting: DOD Needs to Enhance Cybersecurity of Background Investigation Systems	The Secretary of Defense should direct the Defense Counterintelligence and Security Agency's CIO to ensure the agency's policies and procedures include key information and are reviewed and updated as required. (Recommendation 9)

Source: GAO summary based on previously issued reports. | GAO-25-108211

*Indicates a priority recommendation.

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 DOD CIO.

Table 2: Open Chief Information Officer (CIO)-related IT Acquisitions Recommendations for the Department of Defense (DOD)

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 Defense should ensure an inventory of mobile devices and services is established department-wide (i.e., all components' devices and associated services are accounted for).

GAO report number	GAO report title	Recommendation
GAO-19-58	Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked	The Secretary of Defense should ensure that the CIO of Defense establishes a consistent and repeatable mechanism to track savings and cost avoidances from the migration and deployment of cloud services. (Recommendation 6)

GAO report number	GAO report title	Recommendation
GAO-22-104070	Cloud Computing: DOD Needs to Improve Workforce Planning and Software Application Modernization	The Secretary of Defense should direct the CIO to ensure that the department's components and Office of the Undersecretary of Defense for Acquisition & Sustainment conduct regular evaluations of customer experience and user needs to ensure that the solutions for the enterprise-wide cloud environment foster efficiency, accessibility, and privacy. (Recommendation 2) The Secretary of Defense should direct the CIO and department components to develop and execute a communication plan that will help employees understand the planned changes that will occur for the implementation of the department's enterprise-wide cloud environment. (Recommendation 3) The Secretary of Defense should direct the CIO to establish an enterprise-wide rationalization governance structure, identify and document all rationalization requirements in department policy, and determine the relevant information required on each application for rationalization and the means to collect it. (Recommendation 4) The Secretary of Defense should direct the CIO to establish measurable objectives, milestones, and time frames for the development and implementation of the department's enterprise-wide application rationalization process. (Recommendation 5) The Secretary of Defense should direct the CIO to ensure that all department components are held accountable for meeting the objectives, milestones, and time frames included in the department's enterprise-wide application rationalization process. (Recommendation 6) The Secretary of Defense should direct the CIO to update department-wide guidance to components regarding Technology Business Management (TBM) implementation to include more specific information: how components should allocate spending for cloud services to specific cost pools and towers; identify what control process should be in place to ensure the TBM data is reliable; and provide clarification on the use of minimum reported spending of at least $1,000 for IT investments. (Recommendation 7) The Secretary of the Air Force should direct the Air Force CIO to designate a unit within the component with responsibility for TBM implementation, provide additional guidance on TBM allocation of spending for cloud services to specific cost pools and towers, and to develop a process for assessing and improving the quality of TBM data. (Recommendation 8) The Secretary of the Army should direct the Army CIO to provide additional guidance on TBM allocation of spending for cloud services to specific cost pools and towers, and to develop a process for assessing and improving the quality of TBM data. (Recommendation 9)

GAO report number	GAO report title	Recommendation
GAO-23-105611	Software Acquisition: Additional Actions Needed to Help DOD Implement Future Modernization Efforts	The Secretary of Defense should ensure that, as the Software Modernization Senior Steering Group and other relevant entities develop performance measures for future software modernization efforts, these measures incorporate GAO's key attributes of successful performance measures, to the extent appropriate, to track progress towards achieving agency goals. (Recommendation 1) The Secretary of Defense should direct the Undersecretary of Defense (USD) Acquisition & Sustainment (A&S), USD Research & Engineering (R&E), and DOD CIO to identify the resources needed, such as staffing and funding, to lead DOD's software acquisition and development reform efforts, and to address any related deficiencies these officials identify. (Recommendation 2) The Secretary of Defense should fully identify roles and responsibilities for leaders throughout the department for carrying out reforms included in key software strategies. (Recommendation 3) The Secretary of Defense should direct the USD (A&S), USD (R&E), and DOD CIO to establish processes to collect the data necessary to effectively measure progress against outcome-oriented goals related to software modernization efforts. (Recommendation 6) The Secretary of Defense should ensure that, once the software workforce is identified, the USD (A&S), the Under Secretary of Defense for Personnel and Readiness, and other relevant entities, use that information to develop a department-wide strategic workforce plan that identifies strategies tailored to address gaps in the critical skills and competencies needed to achieve software modernization goals. (Recommendation 7)
GAO-23-106290	DOD Software Licenses: Better Guidance and Plans Needed to Ensure Restrictive Practices Are Mitigated	The Secretary of Defense should direct the DOD CIO, in coordination with Enterprise Software Initiative, to update and implement guidance and plans to fully address identifying, analyzing, and mitigating the impacts of restrictive software licensing practices on cloud computing efforts. (Recommendation 1)
GAO-24-105811	Navy Readiness: Actions Needed to Improve the Reliability and Management of Ship Crewing Data	The Secretary of the Navy should ensure that the Department of the Navy CIO develops and implements a timeframe to finalize the governance structure for the Business Mission Area for Navy's information technology. (Recommendation 10)
GAO-25-107034	DOD Satellite Communications: Reporting on Progress Needed to Provide Insight on New Approach	The Secretary of Defense should ensure that the DOD CIO, supported by the U.S. Space Force, reports annually to Congress on the department's progress implementing Enterprise SATCOM Management and Control and hybrid SATCOM architectures. This report should identify outcomes, opportunities, and risks associated with these efforts, and be submitted coinciding with the President's budget submission through fiscal year 2030. (Recommendation 1)

GAO report number	GAO report title	Recommendation
GAO-25-107041	IT Portfolio Management: Office of Management and Budget (OMB) and Agencies Are Not Fully Addressing Selected Statutory Requirements	The Secretary of Defense should direct the department CIO to work with OMB to ensure that annual reviews of DOD's 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. (Recommendation 13)

Source: GAO summary based on previously issued reports. | GAO-25-108211

DOD Business Systems Modernization

The DOD spends billions of dollars each year to operate, maintain, and modernize business systems and functions to support its military operations. However, challenges such as a lack of updated guidance and documentation and inefficient IT processes limit its ability to effectively manage its business system modernization efforts. Table 3 provides information on the open business systems modernization-related recommendations relevant to the DOD CIO.

Table 3: Open Chief Information Officer (CIO)-related Business Systems Modernization Recommendations for the Department of Defense (DOD)

GAO report number	GAO report title	Recommendation
GAO-12-685	DOD Business Systems Modernization: Governance Mechanisms for Implementing Management Controls Need to Be Improved.	To ensure that DOD continues to implement the full range of institutional management controls needed to address its business systems modernization high-risk area, the Secretary of Defense should ensure that the Deputy Secretary of Defense, as the department's Chief Management Officer,[a] establish a policy that clarifies the roles, responsibilities, and relationships among the Chief Management Officer, Deputy Chief Management Officer, DOD and military department CIOs, Principal Staff Assistants, military department Chief Management Officers, and the heads of the military departments and defense agencies, associated with the development of a federated business enterprise architecture (BEA). Among other things, the policy should address the development and implementation of an overarching taxonomy and associated ontologies to help ensure that each of the respective portions of the architecture will be properly linked and aligned. In addition, the policy should address alignment and coordination of business process areas, military department and defense agency activities associated with developing and implementing each of the various components of the BEA, and relationships among these entities. (Recommendation 1)

GAO report number	GAO report title	Recommendation
GAO-13-557	DOD Business Systems Modernization: Further Actions Needed to Address Challenges and Improve Accountability	To effectively implement key components of DOD's business systems modernization program, the Secretary of Defense should direct the Deputy Chief Management Officer to define by when and how the department plans to develop an architecture that would extend to all defense components and include, among other things, (a) information about the specific business systems that support BEA business activities and related system functions; (b) business capabilities for the Hire-to-Retire and Procure-to-Pay business processes; and (c) sufficient information about business activities to allow for more effective identification of potential overlap and duplication. (Recommendation 1) To effectively implement key components of DOD's business systems modernization program, the Secretary of Defense should direct the Deputy Chief Management Officer to ensure that the functional strategies include all of the critical elements identified in DOD investment management guidance, including performance measures to determine progress toward achieving the goals that incorporate all of the attributes called for in the department's guidance. (Recommendation 3) To effectively implement key components of DOD's business systems modernization program, the Secretary of Defense should direct the Deputy Chief Management Officer to select and control its mix of investments in a manner that best supports mission needs by (a) documenting a process for evaluating portfolio performance that includes the use of actual versus expected performance data and predetermined thresholds; (b) ensuring that portfolio assessments are conducted in key areas identified in our IT investment management framework: benefits attained; current schedule; accuracy of project reporting; and risks that have been mitigated, eliminated, or accepted to date; and (c) ensuring that the documents provided to the Defense Business Council as part of the investment management process include critical information for conducting all assessments. (Recommendation 4)
GAO-15-627	DOD Business Systems Modernization: Additional Action Needed to Achieve Intended Outcomes	To help ensure that the department can better achieve business process reengineering and enterprise architecture outcomes and benefits, the Secretary of Defense should utilize the results of our portfolio manager survey to determine additional actions that can improve the department's management of its business process reengineering and enterprise architecture activities. (Recommendation 1)

GAO report number	GAO report title	Recommendation
GAO-18-130	Defense Business Systems: DOD Needs to Continue Improving Guidance and Plans for Effectively Managing Investments	The Secretary of Defense should ensure that the DOD CIO develops an IT enterprise architecture which includes a transition plan that provides a road map for improving the department's IT and computing infrastructure, including for each of its business processes. (Recommendation 5) The Secretary of Defense should ensure that the DOD CIO and Chief Management Officer work together to define a specific time frame for when the department plans to integrate its business and IT architectures and ensure that the architectures are integrated. (Recommendation 6)
GAO-18-326	DOD Major Automated Information Systems: Adherence to Best Practices Is Needed to Better Manage and Oversee Business Programs	The Secretary of Defense should direct the Under Secretary of Defense for Acquisition and Sustainment to update the policy or guidance for Major Automated Information Systems business programs. Specifically, the update should include the following elements: (1) establishment of initial and current baseline cost and schedule estimates, (2) predetermined threshold cost and schedule estimates to identify the point when programs may be at high risk, and (3) quarterly and annual reports on the performance of programs to stakeholders. (Recommendation 1)
GAO-18-93	Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities	The Secretary of Defense should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the five areas we identified. (Recommendation 6)
GAO-22-105330	Business Systems: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning	The Secretary of Defense should direct the CIO to ensure that major IT business programs report operational performance measures, as appropriate, as part of the department's submission to the federal IT Dashboard. (Recommendation 1) The Secretary of Defense should direct the CIO to ensure that major IT business programs develop approved cybersecurity strategies, as appropriate. (Recommendation 2) The Secretary of Defense should direct the CIO to ensure that major IT business programs develop plans that address information and communication technology supply chain risk management, as appropriate. (Recommendation 3)

GAO report number	GAO report title	Recommendation
GAO-23-104539	Financial Management: DOD Needs to Improve System Oversight	The Secretary of Defense should direct the DOD CIO and Undersecretary of Defense (Comptroller) (USD[C])/Chief Financial Officer (CFO) to update guidance for initial approval and annual certification of business and financial systems to ensure guidance for priority business and financial systems fully addresses the statutory requirements discussed in this report. (Recommendation 1)
		The Secretary of Defense should direct the DOD CIO and USD(C)/CFO to update guidance for initial approval and annual certification of business and financial systems. The update should ensure guidance for non-priority covered business and financial systems that exist within a defense agency, field activity, or support more than one portion of DOD fully addresses the statutory requirements discussed in this report. (Recommendation 2)
		The Secretary of the Army should direct the Chief Management Officer of the Department of the Army to update guidance for initial approval and annual certification of covered business and financial systems. The update should ensure guidance for non-priority Department of the Army business and financial systems fully addresses the statutory requirements discussed in this report. (Recommendation 3)
		The Secretary of the Navy should direct the Chief Management Officer of the Department of the Navy to update guidance for initial approval and annual certification of covered business and financial systems. The update should ensure guidance for non-priority Department of the Navy business and financial systems fully addresses the statutory requirements discussed in this report. (Recommendation 4)
		The Secretary of the Air Force should direct the Chief Management Officer of the Department of the Air Force to update guidance for initial approval and annual certification of covered business and financial systems. The update should ensure guidance for non-priority Department of the Air Force business and financial systems fully addresses the statutory requirements discussed in this report. (Recommendation 5)
		The Secretary of Defense should direct the DOD CIO and USD(C)/CFO to develop guidance that calls for business and financial systems in sustainment to comply with statutory requirements for having valid, achievable requirements and eliminating or reducing the need to tailor commercial off-the-shelf systems. (Recommendation 6)
		The Secretary of Defense should direct the DOD CIO and USD(C)/CFO to ensure that data maintained about business and financial system certifications are complete and accurate. (Recommendation 7)
		The Secretary of Defense should direct the DOD CIO to develop and implement plans for documenting detailed system compliance with the business enterprise architecture. (Recommendation 8)

GAO report number	GAO report title	Recommendation
GAO-24-106912	IT Systems Annual Assessment: DOD Needs to Strengthen Software Metrics and Address Continued Cybersecurity and Reporting Gaps	The Secretary of Defense should direct the CIO and Under Secretary of Defense for Acquisition and Sustainment to ensure that IT business programs developing software use the metrics and management tools required by DOD and consistent with those identified in GAO's Agile Assessment Guide.

Source: GAO summary based on previously issued reports. | GAO-25-108211

[a]In January 2021, the Chief Management Officer position was disestablished. In September 2021, the Deputy Secretary of Defense directed a broad realignment of the responsibilities previously assigned to the Chief Management Officer.

DOD Financial Management

The DOD's spending makes up almost half of the federal government's discretionary spending, and about 82 percent of federal government physical assets belong to DOD. However, the department's financial management is hampered by ineffective processes, aging systems, and inadequate controls; incomplete corrective action plans; and insufficient monitoring and reporting. Table 4 provides information on the open financial management-related recommendations relevant to the DOD CIO.

Table 4: Open Chief Information Officer (CIO)-related Financial Management Recommendations for the Department of Defense (DOD)

GAO report number	GAO report title	Recommendation
GAO-20-252	Financial Management: DOD Needs to Implement Comprehensive Plans to Improve Its Systems Environment	The Secretary of Defense should direct the Chief Management Officer and other entities, as appropriate, to establish measures to determine if the department is succeeding in achieving its goal to improve its financial management systems. Specifically, it should document targets and time frames to define the level of performance to be achieved. It should also document how DOD plans to measure expected outcomes by identifying data sources, how it plans to measure values, and how DOD plans to verify and validate measured values. (Recommendation 1)
		The Secretary of Defense should direct the Chief Management Officer and other entities, as appropriate, to establish a specific time frame for developing an enterprise road map to implement its financial management systems strategy, and ensure that it is developed. The road map should document the current and future states at a high level, from an architecture perspective, and present a transition plan for moving from the current to the future in an efficient, effective manner. The road map should discuss performance gaps, resource requirements, and planned solutions, and it should map DOD's financial management systems strategy to projects and budget. The plan should also document the tasks, time frames, and milestones for implementing new solutions, and include an inventory of systems. (Recommendation 2)
		The Secretary of Defense should direct the Chief Management Officer and other entities, as appropriate, to implement a mechanism for identifying financial management systems that support the preparation of the department's financial statements in the department's systems inventory and budget data, and identify a complete list of financial management systems. (Recommendation 5)
		The Secretary of Defense should direct the Chief Management Officer and other entities, as appropriate, to ensure that the department limits investments in financial management systems to only what is essential to maintain functioning systems and help ensure system security until it implements the other recommendations in this report. (Recommendation 6)*
GAO-23-104539	Financial Management: DOD Needs to Improve System Oversight	The Secretary of Defense should direct the DOD CIO and the Undersecretary of Defense (Comptroller) / Chief Financial Officer to establish a mechanism for ensuring that DOD financial management systems take a strategic approach to workforce planning for the government and contractor staff that develop and maintain its systems. (Recommendation 9)

Source: GAO summary based on previously issued reports. | GAO-25-108211

*Indicates a priority recommendation.