GAO Highlights

IT SYSTEMS ANNUAL ASSESSMENT

DOD Should Improve IT Fraud Risk Management Practices

GAO-26-108596 September 2026

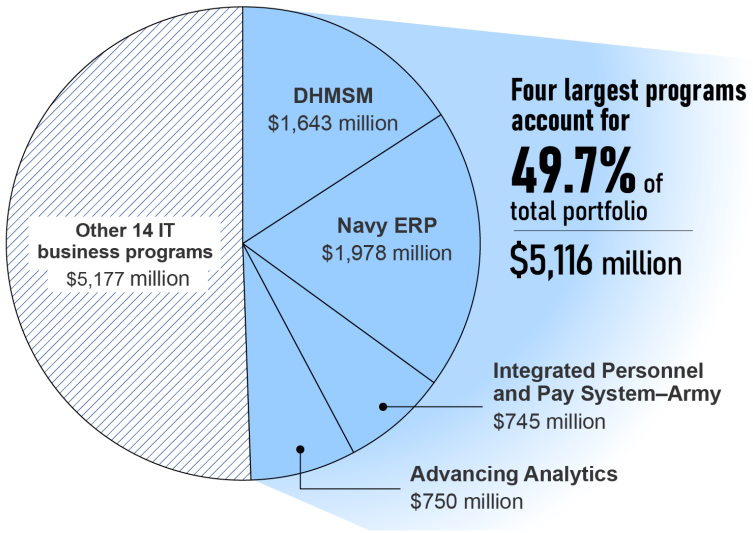
A report to congressional committees.

For more information, contact: Vijay D'Souza at dsouzav@gao.gov.

What GAO Found

To meet its mission to protect the security of our nation and provide warfighters the assets they need, the Department of Defense (DOD) relies heavily on the use of information technology (IT). According to DOD's Office of the Chief Information Officer (OCIO), the department planned to spend $10.3 billion on the 18 major IT business programs from fiscal years (FY) 2024 through 2026. The four largest programs account for 50 percent of the planned spending (see figure).

The Department of Defense's (DOD) Planned Costs for the Four Largest Information Technology (IT) Business Programs Compared to the Remaining 14 Selected Programs from Fiscal Year (FY) 2024 through FY 2026



DHMSM = Department of Defense (DOD) Healthcare Management System Modernization, Navy ERP = Navy Enterprise Resource Planning, IT = information technology

Source: GAO analysis of Department of Defense Office of the Chief Information Officer data, as of February 2026. | GAO-26-108596

To help determine whether operational programs are meeting their business or mission purpose, programs are required by the General Services Administration to identify and track a minimum of five performance metrics across the categories of customer satisfaction, strategic and business results, financial performance, and innovation. Of the 18 programs, 17 were operational. Of these, 15 identified the minimum required number of performance metrics in each category. However, the remaining two did not. Accordingly, the extent to which these two programs were improving customer satisfaction, increasing financial performance, and delivering innovative approaches is unknown. GAO has previously reported on DOD IT business programs not fully reporting

Why GAO Did This Study

IT is critical to the success of DOD's major business functions. These functions include such areas as health care, human capital, financial management, logistics, and contracting.

The National Defense Authorization Act for FY 2019, as amended, includes a provision for GAO to conduct assessments of selected DOD IT programs annually through March 2029. GAO's objectives for this seventh review were to (1) examine what progress selected DOD IT business programs have made on cost, schedule, and performance; (2) assess the extent to which DOD has implemented key fraud risk management, software development, and cybersecurity practices for selected programs; and (3) describe actions DOD has taken to implement legislative and policy changes that could affect its IT acquisitions.

To address the first objective, GAO selected the 18 IT business programs listed as DOD's major IT investments in its FY 2026 submission to the Federal IT Dashboard. GAO analyzed data from DOD's OCIO to examine DOD's planned expenditures for these programs from FY 2024 through FY 2026. GAO also administered a questionnaire to the 18 program offices to obtain and analyze information about cost and schedule changes that the programs reported experiencing since January 2024. Further, GAO compared programs' performance metrics data provided by DOD's OCIO to guidance from the Office of Management and Budget.

To address the second objective, the questionnaire also sought information about the selected programs' practices in fraud risk management, software development, and cybersecurity. GAO compared the responses and documentation against relevant

What GAO Found (continued)

performance metric data and made recommendations to the department to do so (see GAO-22-105330 and GAO-25-107649). Regarding achieving performance goals, of the 17 programs that identified metrics, six programs met all performance targets, 10 programs met more than one target but not all, and one program met no targets.

The IT programs demonstrated mixed progress in implementing key practices for fraud risk awareness, software development, and key cybersecurity initiatives. Developing fraud risk awareness—particularly in staff who manage key IT programs—is an important step toward maturing DOD in fraud risk management. Of the 18 programs, seven programs reported via GAO's questionnaire that program staff were either unaware of or did not receive training to recognize and report signs of fraud or tampering in IT systems (see table). In response, DOD officials indicated that the department does not currently require training to recognize and report signs of fraud in IT systems, rather that personnel receive mandatory, general fraud awareness training. While these broad efforts are important, programs' reported lack of awareness of training to manage or report fraud can increase the risk of software development- and cybersecurity-related fraud within IT programs, making them vulnerable to exploitation.

Department of Defense (DOD) Major Information Technology (IT) Business Programs Reporting Fraud Risk Awareness

Fraud risk awareness practice	Number of programs that reported practice
Receiving training or knowing about available training over the past two years to recognize and report signs of fraud in IT systems	11 of 18
Assessing fraud risks facing the program	10 of 18

Source: GAO analysis of DOD program questionnaire responses as of April 2026. | GAO-26-108596

Further, 10 of the 18 DOD IT business programs reported actively developing software using recommended Agile and iterative software development approaches and practices. However, in areas related to tracking customer satisfaction and progress of software development, eight of the 10 programs did not report or demonstrate using required metrics and management tools. GAO previously recommended that DOD address this issue. Additionally, six of the 18 programs had not developed plans to implement zero trust in their cybersecurity frameworks by DOD's 2027 deadline (see table). In addition, while five programs reported using artificial intelligence (AI) tools to secure their systems, three programs did not have an approved cybersecurity strategy. GAO has previously recommended that all programs develop one (see GAO-22-105330).

Department of Defense (DOD) Major Information Technology (IT) Business Programs That Reported Having an Approved Cybersecurity Strategy or Implementing Zero Trust Architecture

Development approach or practice	Number of programs that reported using each approach or practice
Having a DOD approved cybersecurity strategy	15 of 18
Implementing zero trust architecture as part of the security framework	12 of 18

Source: GAO analysis of DOD program questionnaire responses as of April 2026. | GAO-26-108596

DOD continues to make efforts to improve its management of IT investments as a result of legislative and policy changes. These efforts include revising its business systems investment management guidance, modernizing its business enterprise architecture, adopting a zero trust cybersecurity strategy, developing AI acquisition guidance, updating its agency strategic plan, and implementing cost efficiency initiatives. GAO will continue to monitor DOD's efforts to improve how the department manages its IT investments.

Why GAO Did This Study (continued)

guidance and leading practices to identify gaps and risks. For programs that did not demonstrate having documentation or strategies, GAO followed up with DOD officials for clarification.

For the third objective, GAO reviewed and summarized (1) policy, plans, and guidance associated with the department's efforts to implement changes to its defense business systems investment management guidance and business enterprise architecture and (2) efforts to adopt zero trust cybersecurity principles, develop AI acquisition guidance, update its strategic plan, and implement cost efficiency initiatives. GAO also met with DOD OCIO officials to discuss their efforts in these areas.

What GAO Recommends

GAO reiterates that DOD should address the six recommendations previously made that have not yet been implemented from prior annual assessment reviews. GAO is also making one new recommendation to DOD to ensure that major IT business programs promote and sustain an antifraud tone that permeates programs' organizational culture through training focused on increasing awareness of fraud and fraud risk, recognition of fraud risks in relevant functional settings, and awareness of fraud risk assessment activities.

DOD partially agreed with GAO's recommendation and described actions it was taking to address the recommendation. While the response stated that the DOD Comptroller is the dedicated entity to oversee fraud risk management, GAO maintains that the OCIO must coordinate with that office to ensure that the staff of major IT business systems receive fraud risk training.