



March 2023

# FINANCIAL MANAGEMENT

## DOD Needs to Improve System Oversight

Accessible Version

# GAO Highlights

Highlights of [GAO-23-104539](#), a report to congressional requesters

## Why GAO Did This Study

DOD spends billions of dollars each year on its business and financial systems. However, DOD’s business systems modernization and financial management efforts have been on GAO’s high risk list since 1995. These high risk areas remain obstacles to DOD’s efforts to achieve an unmodified audit opinion.

GAO was asked to review DOD’s financial management systems. This report (1) describes DOD’s efforts to improve its business and financial systems; (2) assesses the extent to which DOD is effectively overseeing its business and financial systems; and (3) assesses the extent to which DOD is taking a strategic approach to managing human capital for its financial management systems.

To describe DOD’s efforts to improve its business and financial systems, GAO reviewed related laws, GAO reports, and DOD and military department documentation associated with DOD’s business and financial systems.

To assess DOD’s oversight of these systems, GAO reviewed reports, guidance, and relevant statutes to identify key elements of business and financial management systems oversight. GAO evaluated DOD policy and DOD, military department, and defense agency guidance and plans against statutory requirements for oversight. It also evaluated DOD’s data on its systems’ compliance with statutory requirements associated with improving the department’s ability to obtain an unmodified audit opinion.

View [GAO-23-104539](#). For more information, contact Kevin Walsh at (202) 512-6151 or [walshk@gao.gov](mailto:walshk@gao.gov) or Vijay A. D’Souza at (202) 512-7650 or [dsouzav@gao.gov](mailto:dsouzav@gao.gov).

March 2023

## FINANCIAL MANAGEMENT

### DOD Needs to Improve System Oversight

#### What GAO Found

For over 30 years, the Department of Defense (DOD) has initiated a variety of efforts and undergone several changes in organizational responsibility to help modernize its business and financial systems. However, these efforts and changes have not been fully successful to date. DOD is the only major federal agency to not achieve an unmodified (clean) audit opinion—its business and financial systems are a key impediment to this effort.

Effective oversight of systems is essential to moving DOD in the right direction. Key elements of such oversight include establishing oversight processes, using and communicating quality information, sustaining leadership commitment, and managing risk.

- Oversight processes.** DOD has established a process for overseeing its business and financial management systems. First, systems are not to proceed into development unless the approving official determines that statutory requirements have been met. These requirements are that the system (1) has been reengineered and streamlined, and unique software requirements and interfaces minimized, (2) complies with the defense business enterprise architecture, (3) has valid, achievable requirements, (4) has an acquisition strategy designed to eliminate or reduce the need to modify commercial off-the-shelf systems, and (5) complies with the Department’s auditability requirements. Second, once approved, systems proceed through an annual certification process in which DOD checks to make sure that systems are continuing to meet the requirements. However, the key guidance documents that govern DOD, military department, and defense agency decisions about initial approvals and annual certifications are limited. Specifically, the guidance does not fully address how systems are to document compliance or how decision-makers are to substantiate that systems are complying with requirements. For example, DOD-level guidance does not describe how approval authorities are to determine compliance with the auditability requirement. This places DOD at risk of making decisions based on a “check the box” exercise.

**Extent to Which DOD, Military Department, and Defense Agency Guidance Addresses Initial Approval and Annual Certification Requirements for Covered Business Systems**

Initial approval and Annual certification requirement	DOD	Army	Department of the Navy	Air Force	Defense Agencies
Business process reengineering	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed
Business enterprise architecture	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed
Requirement plan	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed
Acquisition strategy	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed
Auditability requirement	partially addressed	partially addressed	partially addressed	partially addressed	partially addressed

Legend:

● = Fully addressed: Guidance explains how systems are to address and decision-makers are to substantiate the initial approval and annual certification requirements.

● = Partially addressed: Guidance discusses at least one of the initial approval and annual certification requirements, but does not fully describe how systems are to address and decision-makers are to substantiate the requirements.

○ = Not addressed: Guidance does not discuss the requirements.

Source: GAO Analysis of Department of Defense (DOD) documentation. | GAO-23-104539

GAO also evaluated DOD and military department guidance and plans against key practices for workforce management. In addition, it interviewed relevant officials from DOD and the military departments.

## What GAO Recommends

GAO is making nine recommendations, including that DOD and the military departments update guidance for initial approvals and annual certifications of business and financial systems to substantiate and document compliance with requirements.

GAO is also recommending that DOD ensure that the data collected on the extent of business and financial system compliance with statutory requirements is reliable.

Further, GAO recommends that DOD develop guidance for systems in sustainment to comply with relevant statutory requirements.

In addition, GAO is recommending that DOD implement a strategic approach to workforce planning that, among other things, analyzes gaps in capabilities between existing staff and future needs, and formulates strategies to fill expected gaps.

DOD concurred with seven of the recommendations and partially concurred with the remaining two. Regarding the recommendation to develop guidance for systems in sustainment, DOD stated that its Chief Information Officer would conduct an analysis on the potential need to develop additional guidance. However, by not fully committing to developing needed guidance, DOD is likely missing opportunities for improving its systems in sustainment. Accordingly, GAO maintains that its recommendation is appropriate.

For the recommendation on strategic workforce planning, DOD reiterated steps the department takes to address skills and training for individual functional communities (e.g., acquisition management and financial management). However, those steps do not address the collective staff requirements and expertise needed to address financial management systems issues. GAO maintains that its recommendation is appropriate.

In addition, DOD does not apply key requirements to systems in sustainment, even though the statute does not provide for such an exclusion. By excluding application of these requirements, DOD may be missing important opportunities for improving these systems.

- Quality information.** As part of its oversight, DOD collects data about business and financial system compliance with statutory requirements. For example, of the 136 systems that indicated the auditability requirement was applicable or required, 84 indicated they were compliant with the requirement, 44 indicated they planned to comply, three indicated they were not compliant, and five indicated they had not completed an assessment.

**Summary of DOD's Data on Business System Compliance with Statutory Requirements**

Compliance response	Business process reengineering	Business enterprise architecture	Requirement plan	Acquisition Strategy	Auditability
Compliance required or applicable <sup>a</sup>	189	192	66	67	136
No answer	1	1	1	1	1
Not required (Legacy system) <sup>b</sup>	18	15	21	20	no responses
Not required (System in sustainment) <sup>c</sup>	no responses	no responses	120	120	no responses
Not applicable	no responses	no responses	no responses	no responses	71
<b>Total</b>	<b>208</b>	<b>208</b>	<b>208</b>	<b>208</b>	<b>208</b>

Legend:

- = no responses under the specified category.

Source: GAO Analysis of Department of Defense (DOD) documentation. | GAO-23-104539

<sup>a</sup>Systems indicated that compliance with the requirement was required or applicable.

<sup>b</sup>DOD defines legacy systems as systems that it plans to phase out over the next 36 months. It does not require legacy systems to comply with certain requirements.

<sup>c</sup>DOD does not require systems that have proceeded past the development phase (i.e., systems in sustainment) to comply with selected requirements.

However, the reliability of these data is limited. For example, of the 208 systems that DOD identified as relevant to the financial audit, information on 71 systems indicated that the auditability requirement was not applicable to them. However, a separate database indicated that at least 58 of these 71 were relevant to the audit. In addition, as of January 2022, DOD reported that its Independent Public Auditors had identified 1,411 unresolved IT-related notices of findings and recommendations associated with 3,478 underlying IT-related issues. These results raises further questions about data reliability, which may also impact the extent of compliance with statutory requirements.

- Leadership.** DOD has experienced frequent changes to the organizations and entities responsible for overseeing its business and financial systems. For example, in February 2018 a new Chief Management Officer position was established with broad responsibilities for business operations; three years later the position was abolished. GAO has previously reported that demonstrating sustained, consistent leadership is imperative for successful business transformations.
- Managing risk.** Officials from across DOD provided their perspectives on risks and challenges facing the department as it seeks to modernize its financial system environment. These include legacy systems, system interfaces, and human capital. DOD has taken a number of steps to address risks and challenges identified by DOD officials. GAO will continue monitoring DOD's efforts in this area.

In addition, DOD is not taking a strategic approach to managing the human capital needed for its financial management systems. It does not, among other things, analyze the gaps in capabilities between existing staff and future

workforce needs, or formulate strategies for filling expected gaps. As a result, as discussed in the report, challenges have emerged.

---

# Contents

---

GAO Highlights	2
<b>Why GAO Did This Study</b>	2
<b>What GAO Found</b>	2
<b>What GAO Recommends</b>	4
Letter	1
Background	6
DOD Has Undertaken Multiple Initiatives To Modernize Its Business And Financial Systems	19
DOD Established a Process for Overseeing Its Business and Financial Systems but Lacks Fully Developed Guidance and Reliable Data	21
DOD Has Taken Steps to Improve Its Financial Management Systems Workforce but Lacks a Strategic Approach for Gaps	43
Conclusions	47
Recommendations for Executive Action	48
Agency Comments and Our Evaluation	49
Appendix I: Objectives, Scope and Methodology	54
Appendix II: Evaluation of DOD Guidance for Business and Financial System Initial Approvals and Annual Certifications	63
Appendix III: Comments from the Department of Defense	80
Accessible Text for Appendix III: Comments from the Department of Defense	85
Appendix IV: GAO Contacts and Staff Acknowledgments	89
Tables	
Table 1: Selected Responsibilities Previously Assigned to the Department of Defense (DOD) Chief Management Officer (CMO) and New Responsible Entities as Assigned by the Deputy Secretary of Defense in September 2021	12
Table 2: Examples of Organizational Changes Associated with Improving DOD’s Business and Financial Systems Environment	19
Table 3: Examples of Efforts DOD Has Undertaken Associated with Improving its Business and Financial Systems Environment	20

---

Table 4: Extent to Which the Department of Defense (DOD) Guidance Addresses Requirements for Initial Approval and Annual Certification for Priority Business Systems	25
Table 5: Extent to Which Military Department and Defense Agency Guidance Addresses Initial Approval Requirements for Non-Priority Covered Business Systems	27
Table 6: Extent to Which Military Department and Defense Agency Guidance Addresses Annual Certification Requirements for Non-Priority Covered Business Systems	29
Table 7: Partial Summary of DOD’s Data on Business System Compliance with Statutory Requirements	33
Table 8: Complete Summary of DOD’s Data on Business System Compliance with Statutory Requirements	34
Table 9: The Department of Defense (DOD) Business System Officials Reported Challenges with Software Development Staffing	46
Table 10: Eight Selected Financial Management Systems Managed by Military Department and Defense Agencies	59
Table 11: Assessment of DOD Guidance for Initial Approval Requirements for Systems That Plan to Spend More Than \$250 Million over the Future-Years Defense Program (FYDP)	63
Table 12: Assessment of DOD Guidance for Annual Certification Requirements for Systems That Plan to Spend More Than \$250 Million over the Future-Years Defense Program (FYDP)	65
Table 13: Assessment of DOD Guidance for Initial Approval Requirements for Defense Agency Systems that Plan to Spend Between \$25 Million and \$250 Million over the Future-Years Defense Program (FYDP)	66
Table 14: Assessment of DOD Guidance for Annual Certification Requirements for Defense Agency Systems That Plan to Spend between \$25 Million and \$250 Million over the Future-Years Defense Program (FYDP)	67
Table 15: Assessment of Air Force Guidance for Initial Approval Requirements for Systems That Plan to Spend between \$1 Million and \$250 Million over the Future-Years Defense Program (FYDP)	69
Table 16: Assessment of Air Force Guidance for Annual Certification Requirements for Systems That Plan to Spend between \$1 Million and \$250 Million over the Future-Years Defense Program (FYDP)	71

---

---

Table 17: Assessment of Army Guidance for Initial Approval Requirements for Systems That Plan to Spend up to \$250 Million over the Future-Years Defense Program (FYDP)	73
Table 18: Assessment of Army Guidance for Annual Certification Requirements for Systems That Plan to Spend up to \$250 Million over the Future-Years Defense Program (FYDP)	75
Table 19: Assessment of Department of the Navy (DON) Guidance for Initial Approval Requirements for Systems That Plan to Spend Between \$10 Million and \$250 Million over the Future-Years Defense Program (FYDP)	77
Table 20: Assessment of Department of the Navy (DON) Guidance for Annual Certification Requirements for Systems That Plan to Spend between \$10 Million and \$250 Million over the Future-Years Defense Program (FYDP)	78



---

---

### Abbreviations

CFO	Chief Financial Officer
CIO	Chief Information Officer
CMO	Chief Management Officer
DITIP	Defense IT Investment Portal
DITPR	Defense IT Portfolio Repository
DOD	Department of Defense
DON	Department of the Navy
FIAR	Financial Improvement and Audit Readiness
FY	Fiscal Year
FYDP	Future-Years Defense Program
IBF-DAP	Integrated Business Framework - Data Alignment Portal
IG	Inspector General
IPA	Independent Public Accountant
NDAA	National Defense Authorization Act
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
USD(C)/CFO	Undersecretary of Defense (Comptroller)/Chief Financial Officer

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



March 7, 2023

Congressional Requesters

Sound financial management practices and reliable, useful, and timely financial information are critical to the Department of Defense's (DOD) ability to ensure accountability for its extensive resources. These practices and information also support DOD's ability to efficiently and effectively manage its assets and budgets.

DOD financial management has been on GAO's High Risk List since 1995 because of long-standing deficiencies with its financial management systems,<sup>1</sup> reporting practices, and management of its finances.<sup>2</sup> DOD business systems, which include financial systems as well as systems that support other business functions (e.g., logistics and health care), have also been on GAO's High Risk list since 1995. This high risk area addresses, among other things, the department's critical challenges in

---

<sup>1</sup>According to the Federal Financial Management Improvement Act of 1996, financial management systems are the financial systems and the financial portions of mixed systems necessary to support financial management. These systems include automated and manual processes, procedures, controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions. A financial system is an information system, comprised of one or more applications used for collecting, processing, maintaining, transmitting, or reporting data about financial events; supporting financial planning or budgeting activities; accumulating and reporting costs information; or supporting the preparation of financial statements. A mixed system is an information system that supports both financial and nonfinancial functions. The DOD Financial Management Regulation refers to some mixed systems as feeder systems. The regulation defines feeder systems as the manual or automated programs, procedures, and processes which develop data required to initiate an accounting or financial transaction but do not perform an accounting operation, such as personnel, property, or logistics systems.

<sup>2</sup>GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, [GAO-21-119SP](#) (Washington, D.C.: Mar. 2, 2021).

improving its business system investment management and in leveraging its federated business enterprise architecture.<sup>3</sup>

We have also reported that DOD's financial systems are a significant contributor to its inability to improve how it accounts for and reports its spending and assets. For example, in September 2020, we reported<sup>4</sup> that DOD's Independent Public Accountants (IPAs) issued 2,100 new and reissued Notices of Findings and Recommendations to the military departments for fiscal year (FY) 2019.<sup>5</sup> Of the 2,100 FY 2019 notices, 1,008 were related to IT and cybersecurity issues.

In addition to our reports, the DOD Inspector General (IG) has also discussed the role of DOD financial systems in the department's annual audit. For example, in May 2022, the IG noted that, for FY 2021, DOD reported that it used 299 separate IT systems to support its financial statements.<sup>6</sup> The DOD IG added that IT remains a material weakness preventing DOD from efficient and effective financial management and

---

<sup>3</sup>A federated business enterprise architecture refers to an architecture in which member architectures (e.g., of the Air Force, Army, and Navy) conform to an overarching corporate or parent architecture and use a common vocabulary. This approach is to provide governance across all business systems, functions, and activities within the department and improve visibility across the respective efforts. DOD's federated business enterprise architecture is intended to serve as a blueprint to guide and constrain the implementation of interoperable defense business systems. The architecture does so by, among other things, documenting the department's business functions and activities. See, for example, GAO, *Business Systems Modernization: DOD Has Made Progress in Addressing Recommendations to Improve IT Management, but More Action Is Needed*, [GAO-20-253](#) (Washington, D.C., Mar. 5, 2020). Also see GAO, *Defense Business Systems: DOD Needs to Continue Improving Guidance and Plans for Effectively Managing Investments*, [GAO-18-130](#) (Washington, D.C.: Apr. 16, 2018); *DOD Business Systems Modernization: Additional Action Needed to Achieve Intended Outcomes*, [GAO-15-627](#) (Washington, D.C.: July 16, 2015); *Business Systems Modernization: Summary of GAO's Assessment of the Department of Defense's Initial Business Enterprise Architecture*, [GAO-03-877R](#) (Washington, D.C.: July 7, 2003); *Information Technology: Architecture Needed to Guide Modernization of DOD's Financial Operations*, [GAO-01-525](#) (Washington, D.C.: May 17, 2001); and *High-Risk Series: An Overview*, [GAO/HR-95-1](#) (Washington, D.C.: February 1995).

<sup>4</sup>GAO, *Financial Management: DOD Needs to Implement Comprehensive Plans to Improve Its Systems Environment*, [GAO-20-252](#) (Washington, D.C.: Sept. 30, 2020).

<sup>5</sup>A notice of finding and recommendation includes one or more findings and discusses deficiencies that IPAs identified during the audit along with a corresponding recommendation(s) for addressing the deficiencies. The IPAs issue both financial and IT notices of finding and recommendation.

<sup>6</sup>Department of Defense Office of Inspector General, *Understanding the Results of the Audit of the FY 2021 DOD Financial Statements* (Alexandria, VA: May 18, 2022).

preventing progress toward receiving an unmodified (clean) audit opinion.<sup>7</sup>

You asked us to review DOD's financial management systems. Our specific objectives for this review were to (1) describe DOD's efforts to improve its business and financial systems, (2) assess the extent to which DOD is effectively overseeing its business and financial systems, and (3) assess the extent to which DOD is taking a strategic approach to managing human capital needed for developing and maintaining its financial management systems.<sup>8</sup>

To address the first objective, we reviewed related statutes, GAO reports, and DOD and military department documentation associated with DOD's business and financial systems.<sup>9</sup> For example, we reviewed DOD reports and guidance to identify key efforts initiated by DOD associated with improving its financial systems.

To address the second objective, we reviewed prior GAO reports and guidance and relevant statutes to identify key elements of business and financial management systems oversight.<sup>10</sup> In doing so, we identified the

---

<sup>7</sup>According to the DOD IG, a material weakness represents weaknesses in internal control that result in a reasonable possibility that management will not prevent, or detect and correct, a material misstatement in the financial statement in a timely manner. An unmodified opinion, sometimes referred to as a clean opinion, is expressed when the auditor concludes that management has presented the financial statements fairly and in accordance with generally accepted accounting principles.

<sup>8</sup>This report examined DOD's business and financial system programs (referred to as "systems" in this report). Systems that support audit activities (i.e., financial management systems) include systems identified as financial systems, as well as business systems that provide information to those financial systems (e.g., logistics systems).

<sup>9</sup>This report refers to the Department of the Army, the Department of the Air Force, and the Department of the Navy (DON) as the military departments. References in this report to DON reflect that DON encompasses both the Navy and the Marine Corps.

<sup>10</sup>GAO, *Defense Management: Opportunities Exist to Improve DOD's Reform Efforts*, [GAO-21-532T](#) (Washington, D.C., Apr. 27, 2021); *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014); *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0)*, [GAO-10-846G](#) (Washington, D.C., Aug. 5, 2010); *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, [GAO-04-394G](#) (Washington, D.C., Mar. 1, 2004); *Business Process Reengineering Assessment Guide--Version 3*, [AIMD-10.1.15](#) (Washington, D.C., April 1, 1997); and Pub. L. No. 108-375, division A, title III, subtitle D, § 332, 118 Stat. 1181, at 1851 (2004), as amended in pertinent part by Pub. L. No. 114-92, division A, title VIII, subtitle G, § 883(a), 129 Stat. 726, 942 (2015).

following key elements: establishing oversight processes,<sup>11</sup> using and communicating quality information, sustaining leadership commitment, and managing risk.

For effective oversight processes and quality information, we focused on DOD's initial approval and annual certification process for its business and financial systems. This was initially required by the Ronald W. Reagan National Defense Authorization Act (NDAA) for Fiscal Year 2005.<sup>12</sup> We focused on this process because it is one of DOD's key efforts to help ensure its financial systems support auditable financial statements. In doing so, we evaluated DOD's data on its business and financial systems and system compliance with statutory requirements associated with improving the department's ability to obtain an unmodified audit opinion.<sup>13</sup> We used the data to determine the extent to which relevant systems reported complying with applicable statutory requirements.

We assessed the reliability of DOD's data on system compliance with statutory requirements by identifying internal inconsistencies and blank fields. We also compared selected fields from this dataset to the list of systems in a different dataset that documents DOD systems that are relevant to the annual financial audit. As discussed in this report, we found the data were not fully reliable for our purposes. In addition, we reviewed relevant DOD, military department, and defense agency guidance<sup>14</sup> pertaining to the oversight of DOD's business and financial systems. We assessed this guidance against statutory requirements for DOD officials to assert that business and financial systems comply with

---

<sup>11</sup>Oversight processes contribute to improved acquisition management and include processes for managing portfolios of investments and enterprise architecture compliance.

<sup>12</sup>*Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005*, Pub. L. No. 108-375, § 332, 118 Stat. at 1851 (2004) (codified in part at 10 U.S.C. § 2222).

<sup>13</sup>We requested compliance data from DOD for the business and financial systems that were relevant to the annual financial audit. An unmodified audit opinion is commonly referred to as a clean audit opinion.

<sup>14</sup>Defense agency guidance referred to in this report applies to systems that exist within a defense agency, field activity, or support more than one portion of DOD. DOD's defense agencies and field activities are intended to provide department-wide consolidated support functions. Defense agencies include the Defense Logistics Agency and the Defense Finance and Accounting Service. Field Activities include the DOD Education Activity and the DOD Human Resources Activity.

---

requirements associated with improving the department's ability to achieve a positive audit opinion.

For managing sustained leadership commitment and managing risks, we reviewed information from recent GAO reports.<sup>15</sup> We also developed a non-generalizable random sample of eight systems to obtain additional perspectives on challenges associated with DOD's financial management systems. These systems included four that DOD identified as major systems and four that DOD identified as non-major systems.<sup>16</sup> We met with DOD, military department, and system-level officials from our sample of eight systems to discuss associated challenges.

To address the third objective, we reviewed human capital strategies and plans supporting the department's financial management systems and interviewed relevant acquisition, IT, and military department staff. We assessed DOD's approach for determining the government and contractor human capital skills needed to develop and maintain its financial management systems against GAO's guidance on strategic human capital management.<sup>17</sup> This included identifying existing government and contractor human capital skills, assessing gaps between needed and existing skills, and developing plans to address the gaps.

We also met with relevant officials from across DOD, the military departments, and system staff for the eight systems we identified to

---

<sup>15</sup>See GAO, *Business Systems: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning*, [GAO-22-105330](#). (Washington, D.C., June 14, 2022) and [GAO-21-119SP](#).

<sup>16</sup>The systems that DOD identified as major systems were Defense Logistics Agency's Enterprise Business System; Air Force's Defense Enterprise Accounting and Management System; Army's General Fund Enterprise Business System; and the Navy Standard Integrated Personnel System. The systems that DOD identified as non-major systems were the Defense Finance and Accounting Service's Defense Military Pay Office System; the Air Force's Financial Inventory Accounting and Billing System; the Army's Rock Island Arsenal Joint Manufacturing Technology Center Automated Storage and Retrieval System; and Navy's Decision Knowledge Programming for Logistics Analysis and Technical Evaluation.

<sup>17</sup>See GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, [GAO-04-39](#) (Washington, D.C.: Dec. 11, 2003). Also see GAO, *Joint Information Environment: DOD Needs to Strengthen Governance and Management*, [GAO-16-593](#) (Washington, D.C.: Oct. 25, 2016); and *DOD Business Systems Modernization: Further Actions Needed to Address Challenges and Improve Accountability*, [GAO-13-557](#) (Washington, D.C.: May 17, 2013).

discuss related human capital challenges. See Appendix I for a more detailed discussion of our objectives, scope, and methodology.

We conducted this performance audit from October 2020 to February 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

## Background

DOD is the largest U.S. government department and one of the most complex organizations in the world. DOD employs 2.1 million military service members and approximately 780,000 civilian employees at approximately 4,600 DOD sites located in all 50 states, 7 U.S. territories, and more than 40 foreign countries. The President's budget submission for fiscal year 2023 requested \$773 billion for DOD.<sup>18</sup> In addition, DOD's FY 2023 budget request called for \$57.9 billion in expenditures for IT and cyberspace activities. This included \$9.1 billion for business system investments.

DOD's business systems include financial management systems, human resource management systems, logistics and supply chain management systems, property management systems, and acquisition management systems. Many of the systems that DOD has not specifically designated as financial systems also contribute information that supports the department's efforts to prepare financial statements.

In addition, as we have previously reported, the DOD systems environment that supports its business functions, including financial management, has been overly complex and error prone.<sup>19</sup> For example,

---

<sup>18</sup>Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *Defense Budget Overview: United States Department of Defense Fiscal Year 2023 Budget Request*, April 2022.

<sup>19</sup>See, for example, GAO, *DOD Financial Management: Air Force Needs to Improve Its System Migration Efforts*, [GAO-22-103636](#) (Washington, D.C.: Feb. 28, 2022) and *DOD Financial Management: Implementation Weaknesses in Army and Air Force Business Systems Could Jeopardize DOD's Auditability Goals*, [GAO-12-134](#) (Washington, D.C.: Feb. 28, 2012).

---

there is little standardization for DOD systems across the department, and multiple systems perform the same tasks.

---

## DOD Financial Management and Business Systems Are High Risk Areas

DOD's financial management continues to face long-standing issues—including its ineffective processes, systems, and controls; incomplete corrective action plans; and the need for more effective monitoring and reporting. DOD financial management has been on our High Risk List since 1995.<sup>20</sup> Although DOD's spending makes up about half of the federal government's discretionary spending, and its physical assets represent more than 70 percent of the federal government's physical assets, it remains the only major agency that has never been able to accurately account for and report on its spending or physical assets.

DOD's financial management issues extend beyond financial reporting as long-standing control deficiencies adversely affect the economy, efficiency, and effectiveness of its operations. Sound financial management practices and reliable, useful, and timely financial and performance information would help ensure DOD's accountability over its extensive resources and more efficient management of its assets and budgets.

Regarding the business systems modernization high risk area, DOD spends billions of dollars each year to acquire modernized systems, including ones that address key areas such as personnel, financial management, health care, and logistics. While DOD's capacity for modernizing its business systems has improved over time, significant challenges remain. We first added this area to our High Risk List in 1995.<sup>21</sup>

This high risk area includes three elements critical to the success of DOD's efforts: (1) improving business systems acquisition management, (2) improving business systems investment management, and (3) leveraging DOD's federated business enterprise architecture. Addressing

---

<sup>20</sup>[GAO-21-119SP](#).

<sup>21</sup>[GAO-21-119SP](#).



the challenges in these three areas is critical to the success of DOD's efforts.

Regarding acquisition management, over the last few years DOD has had mixed success in acquiring business systems that meet cost, schedule, and performance commitments.<sup>22</sup> For example, we reported in June 2020 that the Integrated Personnel and Pay System—Army Increment 2, which is intended to deliver fully integrated personnel and pay services for all Army components, met all five of its technical performance targets.<sup>23</sup> However, it also experienced a 72 percent increase in its life-cycle cost estimate (\$1.38 billion). We also reported that the DOD Healthcare Management System Modernization, which is intended to provide modernized electronic health records, failed to meet any of its three technical performance targets and experienced a 15.7 percent increase in its life-cycle cost estimate (\$1.27 billion).

Investment management includes evaluating and assessing how well an agency is selecting and managing its IT resources.<sup>24</sup> DOD has taken steps to improve its business system investment management process by addressing some associated recommendations. For example, DOD developed a policy to require full consideration of sustainability and technological refreshment requirements for its defense business systems investments.

DOD should implement our prior recommendations on improving its business system investment management efforts. For example, DOD needs to ensure that functional strategies include the critical elements identified in DOD investment management guidance.<sup>25</sup> DOD also needs to follow-through on previously planned actions related to this area, including updating its investment management policy and guidance.

---

<sup>22</sup>[GAO-21-119SP](#).

<sup>23</sup>GAO, *Information Technology: DOD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule*, [GAO-21-182](#) (Washington, D.C., Dec. 23, 2020). This is the public version of the June 2020 report *Information Technology: DOD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule*, GAO-20-456SU (Washington, D.C.: June 9, 2020).

<sup>24</sup>[GAO-04-394G](#).

<sup>25</sup>[GAO-13-557](#).

DOD's business enterprise architecture is to serve as a blueprint for the department's business transformation efforts. In particular, the architecture is to guide and constrain implementation of interoperable defense business and financial systems by, among other things, documenting the department's business functions and activities and the business rules, laws, regulations, and policies associated with them. For example, the architecture is to include information related to DOD's Standard Financial Information Structure, which is an enterprise-wide data standard for categorizing financial information to support financial management and reporting functions.<sup>26</sup>

Consistent with DOD's tiered approach to business and financial systems management, the department's approach to developing its business enterprise architecture has focused on the development of a federated enterprise architecture. In a federated enterprise architecture, member architectures (e.g., Air Force, Army, and Navy) conform to an overarching corporate or parent architecture and use a common vocabulary. This approach is to provide governance across all business systems, functions, and activities within the department and improve visibility across the respective efforts.

We reported in March 2021 that DOD has established the capacity to identify potentially duplicative investments and provided examples of benefits attributed, at least in part, to its business enterprise architecture.<sup>27</sup> Nevertheless, the department is revamping its approach to its business enterprise architecture and has not yet demonstrated that it is actively and consistently assessing potential duplication and overlap to eliminate unnecessary systems. As we reported, it needs to take action to

---

<sup>26</sup>According to an official from the office of the Undersecretary of Defense (Comptroller)/Chief Financial Officer (USD(C)/CFO), Business Enterprise Architecture version 11.2, published in 2019, includes the acquisition business area's procurement data standards and purchase request data standards and the human resources business area's common human resources information standards. The official also noted that it includes the information and environment business area's information management standards as well as the logistics business area's defense logistics management standards, and the financial management business area's delinquent debt and Standard Financial Information Structure standards. This official added that all these standards are required for compliance as components develop new capabilities and assert compliance to the business enterprise architecture with their systems annual investment review process. Moreover, this official noted that these standards are one of several mechanisms that are used to standardize how business information that informs the financial statement from across the DOD.

<sup>27</sup>[GAO-21-119SP](#).

---

do so. In addition, it needs to demonstrate that it has developed a plan for improving its business enterprise architecture.

---

## Statute Calls for DOD to Establish an Initial Approval and Annual Certification Process for Business and Financial Systems

The Ronald W. Reagan NDAA for FY 2005 enacted the initial approval and annual certification requirements, which were later amended, as codified in 10 U.S.C. § 2222.<sup>28</sup> Title 10 U.S.C. § 2222 currently states the Secretary of Defense should ensure that covered defense business systems<sup>29</sup> (including financial systems) cannot proceed into development unless the appropriate approval official determines that the following five criteria have been addressed.

1. **Business process reengineering.** The system has been, or is being, reengineered to be as streamlined and efficient as practicable, and the implementation of the system will maximize the elimination of unique software requirements and unique interfaces;
2. **Business enterprise architecture.** The system and business system portfolio are or will be in compliance with the defense business enterprise architecture or will be in compliance as a result of modifications planned;
3. **Requirements plan.** The system has valid, achievable requirements and a viable plan for implementing those requirements;
4. **Acquisition strategy.** The system has an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable; and
5. **Auditability.** The system is in compliance with the Department's auditability requirements.

The statute further calls for the appropriate approval official to review covered systems on an annual basis and certify, certify with conditions, or

---

<sup>28</sup>Pub. L. No. 108-375, § 332, 118 Stat. at 1851 (2004), as amended in pertinent part by Pub. L. No. 114-92, § 883(a), 129 Stat. at 942 (2015).

<sup>29</sup>A covered defense business system is one expected to have a total amount of budget authority of more than \$50 million over the current fiscal year and at least the succeeding four fiscal years.

decline to certify, that it continues to satisfy these requirements. If the approval official determines that certification cannot be granted, the approval official shall notify the milestone decision authority for the system and provide a recommendation for corrective action.

The statute specifies a tiered approach for these initial approvals and annual certifications. Priority defense business systems, which are systems that expect to spend more than \$250 million over the course of the current future-years defense program,<sup>30</sup> were to be approved by the DOD Chief Management Officer (CMO).<sup>31</sup> Systems that expect to spend between \$50 and \$250 million over the same time period are to be approved by either the CMO of their respective military department or by the DOD CMO.<sup>32</sup>

DOD's current guidance for implementing this statute is documented in DOD Instruction 5000.75 and its June 2018 guidance for DOD business systems investment management.<sup>33</sup> This guidance, discussed subsequently in this report, applies to business systems in development and in sustainment.<sup>34</sup> Specifically, all systems are required to respond to the five requirements: business process reengineering, business enterprise architecture, requirement plan, acquisition strategy, and auditability.

---

<sup>30</sup>The future-years defense program is to be submitted to Congress by the Secretary of Defense each year, at or about the time that the President's budget is submitted to Congress. It is to reflect the estimated expenditures and proposed appropriations included in the DOD budget, and cover the budget-submission fiscal year and at least the four succeeding fiscal years.

<sup>31</sup>As discussed subsequently in this report, the DOD CMO position was eliminated in January 2021. Approval responsibilities formerly assigned to the DOD CMO are now shared by the USD(C)/CFO and the DOD CIO.

<sup>32</sup>The DOD CMO was to approve systems that are owned by a DOD agency or field activity, or support the business process of more than one military department or Defense Agency or DOD Field Activity.

<sup>33</sup>Department of Defense, *DOD Instruction 5000.75: Business Systems Requirements and Acquisition* (Jan. 24, 2020) and DOD, *Office of the Chief Management Officer, Defense Business Systems Investment Management Guidance, Version 4.1* (June 26, 2018).

<sup>34</sup>Systems in sustainment are operational and not currently in the development phase. As a general matter, the statute requires the Secretary of Defense to ensure that defense business processes are appropriately revised through reengineering to best match commercial practices so as to minimize customization. We have previously reported on the importance of limiting the customization of DOD's commercial off-the-shelf systems. See, for example, [GAO-22-105330](#) and [GAO-22-103636](#).

## Roles and Responsibilities of Key Entities for DOD Financial Management Systems

The Undersecretary of Defense (Comptroller)/CFO (USD(C)/CFO), DOD Chief Information Officer (CIO), and the Director of Administration and Management have various responsibilities for the department’s financial management systems. For example:

- The USD(C)/CFO is responsible for developing and maintaining an integrated agency accounting and financial management system, including financial reporting and internal controls.
- The CIO is responsible for policy, oversight, and guidance for DOD’s IT, networking, information assurance, cybersecurity, and cyber capability architectures.

In addition, as of September 2021, DOD’s Director of Administration and Management, the USD(C)/CFO, and the DOD CIO have additional responsibilities associated with business systems, which include financial systems that inform and support the department’s audit efforts. Table 1 identifies selected responsibilities associated with DOD’s business systems.

**Table 1: Selected Responsibilities Previously Assigned to the Department of Defense (DOD) Chief Management Officer (CMO) and New Responsible Entities as Assigned by the Deputy Secretary of Defense in September 2021**

Responsibility	Director of Administration and Management (new responsible entity)	Undersecretary of Defense (Comptroller)/Chief Financial Officer (USD(C)/CFO) (new responsible entity)	DOD CIO (new responsible entity)
Establish a Defense Business Council, chaired by the CMO and the DOD Chief Information Officer (CIO), to provide advice to the Secretary of Defense on developing the defense business enterprise architecture, reengineering DOD business processes, developing and deploying defense business systems, and developing requirements for defense business systems.	entity assigned	entity assigned	entity assigned
Develop and maintain the DOD business enterprise architecture to guide the development of integrated DOD business processes.	entity not assigned	entity not assigned	entity assigned
Ensure that each covered defense business system developed, deployed, and operated by DOD: (1) supports efficient business processes, (2) is integrated into a comprehensive defense business enterprise architecture, (3) is managed to provide visibility into expenditures, and (4) uses an acquisition and sustainment strategy that prioritizes use of commercial software/business practices.	entity not assigned	entity assigned	entity assigned

Responsibility	Director of Administration and Management (new responsible entity)	Undersecretary of Defense (Comptroller)/Chief Financial Officer (USD(C)/CFO) (new responsible entity)	DOD CIO (new responsible entity)
Serve as initial approving official for a covered defense business system proceeding into development (or as appropriate production or fielding) for a priority defense business system or a system of a defense agency or field activity or more than one military department.	entity not assigned	entity assigned	entity assigned
Serve as approving official for annual certification for continued development or sustainment of a covered defense business system and provide recommendations to the milestone decision authority for corrective actions.	entity not assigned	entity assigned	entity assigned
Designate priority defense business systems based upon complexity, scope and technical risks, and provide notification of designation to Congress.	entity not assigned	entity assigned	entity assigned
Issue supporting guidance, along with USD Acquisition and Sustainment, DOD CIO, and military department CMOs, within respective areas of responsibility for the coordination of, and decision making for, the planning, programming, and control of investments in covered defense business systems.	entity not assigned	entity assigned	entity assigned

Legend:  
 ✓ = the entity was assigned the former CMO responsibility as of September 2021  
 — = the entity is not assigned the former CMO responsibility

Source: GAO analysis of Department of Defense documentation. | GAO-23-104539

## Key Elements of Business and Financial Management Systems Oversight

Effective oversight of business and financial management systems is critical for producing reliable financial information. Key elements of business and financial management systems oversight include the following.

- Establishing oversight processes.** Establishing oversight processes, including processes to address portfolio management, business process reengineering, enterprise architecture compliance, requirements management, and auditability requirements.<sup>35</sup> Oversight

<sup>35</sup>Oversight processes contribute to improved acquisition management and include processes for managing portfolios of investments and enterprise architecture compliance. See, for example, [GAO-10-846G](#); [GAO-04-394G](#); [AIMD-10.1.15](#); and Pub. L. No. 108-375, § 332, 118 Stat. at 1851 (2004), as amended in pertinent part by Pub. L. No. 114-92, § 883(a), 129 Stat. at 942 (2015).

processes also include mechanisms to monitor and enforce stated requirements.

- **Using and communicating quality information.** Effective oversight includes using quality information to make decisions and communicating quality information, as appropriate, to help DOD ensure business and financial systems are meeting appropriate requirements.<sup>36</sup>
- **Sustaining leadership commitment.** Improving DOD's business and financial systems environment is a significant change management initiative. As we have previously reported, demonstrating sustained leadership commitment is imperative for successful business transformation.<sup>37</sup> In our 2003 report on results-oriented cultures at federal agencies, we noted that people are at the center of any serious change management initiative.<sup>38</sup> This includes top leadership, which must drive the transformation. In addition, leadership commitment is a key practice for addressing high risk areas to support removing them from our high risk list.<sup>39</sup>
- **Managing risk.** Effective oversight also includes identifying, analyzing, and responding to risks.<sup>40</sup>

Strategic workforce planning is another key element of effective business and financial management systems oversight. GAO has previously identified key practices for effective strategic workforce planning.<sup>41</sup> These key practices include:

- assessing the knowledge and skills needed to execute a program;
- developing an inventory of the knowledge and skills of existing staff;
- forecasting the knowledge and skills needed over time;

---

<sup>36</sup>[GAO-14-704G](#).

<sup>37</sup>See, for example, GAO, *Defense Management: Opportunities Exist to Improve DOD's Reform Efforts*, [GAO-21-532T](#) (Washington, D.C., Apr. 27, 2021).

<sup>38</sup>GAO, *Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations*, [GAO-03-669](#) (Washington, D.C.: July 2, 2003).

<sup>39</sup>GAO, *High-Risk Series: Key Practices to Successfully Address High-Risk Areas and Remove Them from the List*, [GAO-22-105184](#) (Washington, D.C., Mar.3, 2022).

<sup>40</sup>[GAO-14-704G](#). GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*, [GAO-17-63](#) (Washington, D.C., Dec. 1, 2016).

<sup>41</sup>See [GAO-16-593](#); [GAO-13-557](#); and [GAO-04-39](#).

- 
- analyzing the gaps in capabilities between the existing staff and future workforce needs, including consideration of evolving program and succession needs caused by turnover and retirement; and
  - formulating strategies for filling expected gaps.

---

## GAO Has Made Recommendations to Improve DOD's Management of its Business and Financial Systems

As previously noted, DOD financial management has been on our High Risk List since 1995.<sup>42</sup> Although DOD's spending makes up about half of the federal government's discretionary spending, and its physical assets represent more than 70 percent of the federal government's physical assets, it remains the only major agency that has never been able to accurately account for and report on its spending or physical assets.

IT remains a material weakness preventing DOD from efficient and effective financial management and preventing progress toward receiving a clean audit opinion.<sup>43</sup> Related to this high risk area, in September 2020, we made six recommendations intended to help address DOD's management of its portfolio of financial system investments.<sup>44</sup> DOD has implemented one of the recommendations, while the remaining five have not yet been implemented. Among those non-implemented recommendations are the following.

- We recommended that DOD 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. In August 2022, DOD reported that it published a new Financial Management Functional Strategy in February 2022 with goals and objectives for systems relevant to Financial Management. DOD also reported that the Office of the USD(C)/CFO is in the process of finalizing targets and time frames, along with data sources and mechanisms to capture and monitor performance. However, as of December 2022, DOD had

---

<sup>42</sup>[GAO-21-119SP](#).

<sup>43</sup>Department of Defense Office of Inspector General, *Understanding the Results of the Audit of the FY 2021 DOD Financial Statements* (Alexandria, VA: May 18, 2022).

<sup>44</sup>[GAO-20-252](#).



not yet demonstrated that it had completed all actions needed to address this recommendation.

- We recommended that DOD establish a specific time frame for developing an enterprise road map to implement its financial management systems strategy, and ensure that it is developed. Further, 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 also discuss performance gaps, resource requirements, and planned solutions, and it should map DOD's financial management systems strategy to projects and budget. Moreover, the plan should also document the tasks, time frames, and milestones for implementing new solutions, and include an inventory of systems. In August 2022, DOD reported that it completed an initial enterprise roadmap in June 2022 that included an inventory of systems with current migration and retirement plans. However, as of December 2022, DOD had not yet demonstrated that it had completed all actions needed to address this recommendation.
- We recommended that DOD 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. In September 2022, DOD reported that it was in the process of finalizing DOD guidance that would be responsive to the recommendation and that it expected the guidance to be finalized by the end of January 2023.

In addition, as noted, DOD's efforts to modernize its business systems have also been on GAO's High Risk list since 1995. Since that time, we have made at least 309 recommendations aimed at addressing issues associated with this high risk area.<sup>45</sup> Of the 309 recommendations, DOD has implemented 214 and not implemented 81, and 14 remain open.<sup>46</sup> These recommendations are associated with (1) improving business systems acquisition management, (2) improving business systems

---

<sup>45</sup>See, for example, [GAO-15-627](#); GAO, *Defense Business Systems: Further Refinements Needed to Guide the Investment Management Process*, [GAO-14-486](#) (Washington, D.C. May 12, 2014); [GAO-13-557](#); and GAO, *DOD Business Systems Modernization: Governance Mechanisms for Implementing Management Controls Need to Be Improved*, [GAO-12-685](#) (Washington, D.C.: June 1, 2012).

<sup>46</sup>Historically, we have closed recommendations as not implemented for a variety of reasons, including when conditions change that cause the recommendation to be overcome by events.

investment management, and (3) leveraging DOD's federated business enterprise architecture.

Of the 14 open recommendations, five are aimed at improving DOD's business enterprise architecture. For example:

- In June 2012, we recommended that DOD, among other things, establish a policy that clarifies the roles and responsibilities associated with the development of a federated business enterprise architecture.<sup>47</sup> This included clarifying the relationships among the CMO, deputy CMO, DOD and military department CIOs, principal staff assistants, military department CMOs, and the heads of military departments and defense agencies.

DOD has taken a variety of actions intended to address this recommendation. In August 2013, DOD established a Business Enterprise Architecture Configuration Control Board, which was the principal body for managing the disposition of proposed architecture requirements and change requests. However, the board's charter did not discuss roles and responsibilities associated with the development of the business enterprise architecture. More recently, in September 2018, the department stated that it was drafting a business enterprise architecture concept of operations that was to outline roles and responsibilities associated with the development of the architecture. However, DOD has not demonstrated that it developed a complete concept of operations. In July 2020, DOD reported that it had developed a draft Department of Defense Business Systems Modernization Digital Vision and Department of Defense Enterprise Architecture Blueprint/Transition Plan. However, DOD did not demonstrate that these documents were completed.

- In May 2013, we recommended that DOD define when and how it plans to develop an architecture that would extend to all defense components. This included, among other things, information about the specific business systems that support business enterprise architecture business activities and related system functions. It included business capabilities for the hire-to-retain and procure-to-pay business processes. It also included sufficient information about business activities to allow for more effective identification of potential overlap and duplication.<sup>48</sup> As discussed, DOD has taken a variety of actions over the years to update its business enterprise architecture,

---

<sup>47</sup>[GAO-12-685](#).

<sup>48</sup>[GAO-13-557](#).

but has not yet demonstrated that it has addressed this recommendation.

- In July 2015, we surveyed DOD portfolio managers and reported that the architecture was not effective in constraining system investments or enabling DOD to produce reliable and timely information for decision-making purposes, among other things.<sup>49</sup> We recommended that DOD utilize the results of our portfolio manager survey to determine additional actions that could improve the department's management of its business enterprise architecture activities.

In response to this recommendation, in January 2017, DOD awarded a contract to improve its business enterprise architecture. According to the department, the objective of the contract was to improve business and system optimization. It did so by providing mechanisms to ingest and discover enterprise architecture content from all department components and allow for cross-domain portfolio reviews to include duplication analysis. More specifically, the contract called for developing three major capabilities, including the ability to conduct process and system reviews within and across domains. In October 2019, the Office of the CMO demonstrated that it had completed development of the three planned capabilities and the office said it was working to host the capabilities in a government-approved cloud environment. However, DOD never demonstrated that it completed these efforts.

In a move that impacted all of these open recommendations, in September 2021, DOD reassigned responsibility for the business enterprise architecture to the Office of the CIO after the elimination of the CMO position in January 2021.<sup>50</sup> In April 2022, DOD reported that it planned to establish a business enterprise architecture modernization strategy in December 2022 and publish a new version of the architecture by June 2023. We will continue to follow-up on the status of DOD's efforts to address these open recommendations.

---

<sup>49</sup>[GAO-15-627](#).

<sup>50</sup>The CMO position was repealed by Section 901 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, division A, title IX, subtitle A, §901, 134 Stat. 3388, 3794 (2021).

## DOD Has Undertaken Multiple Initiatives To Modernize Its Business And Financial Systems

For over 30 years, DOD has undergone numerous organizational changes and initiated a variety of efforts intended to modernize its business and financial systems. For example, in November 1993, the NDAA for FY 1994 established the DOD Comptroller as the DOD CFO. Among other things, the CFO is responsible for developing and maintaining DOD financial systems that comply with applicable accounting principles, standards, and requirements. More recently, in September 2021, DOD reorganized the roles and responsibilities associated with overseeing business and financial system investments after the elimination of the CMO position.

Table 2 identifies organizational changes associated with the DOD’s efforts to improve its business and financial systems environment over the last 30 years.

**Table 2: Examples of Organizational Changes Associated with Improving DOD’s Business and Financial Systems Environment**

Action	Month and Year initiated	Description
DOD Establishes the Defense Finance and Accounting Service	January 1991	DOD established the Defense Finance and Accounting Service to standardize, consolidate, modernize, and improve accounting and financial functions throughout the DOD.
DOD Comptroller established as the DOD Chief Financial Officer (CFO)	November 1993	The National Defense Authorization Act (NDAA) for fiscal year (FY) 1994 established the DOD Comptroller as the DOD CFO. Among other things, at this time, agency CFOs were responsible for developing and maintaining agency financial management systems that comply with applicable accounting principles, standards, and requirements.
Financial Improvement and Audit Readiness Directorate established	2005	DOD established the Financial Improvement and Audit Readiness Directorate, located in the Office of the CFO, to develop, manage, and implement a strategic approach for addressing the department’s financial management weaknesses, achieving auditability, and integrating those efforts with other improvement activities, such as the department’s business system modernization efforts.
Business Transformation Agency established	October 2005	DOD established the Business Transformation Agency, in part, to advance DOD’s business and financial systems modernization efforts. Among other things, the agency was to be responsible for ensuring consistency and continuity across the department’s core business missions with respect to, for example, business process reengineering and related business system matters. This included assuming responsibility for developing DOD’s business enterprise architecture and guiding business transformation efforts at the DOD enterprise level.

Action	Month and Year initiated	Description
Deputy Chief Management Officer (CMO) Position established	October 2008	In response to provisions of the NDAA for FY 2008, DOD established the position of Deputy CMO. Prior to this designation, DOD also named the Deputy Secretary of Defense as the department's CMO. The Deputy CMO assumed responsibilities for managing the Business Transformation Agency. The agency continued to be responsible for matters such as developing the business enterprise architecture and guiding business transformation efforts at the DOD enterprise level.
Business Transformation Agency eliminated	September 2011	DOD eliminated the Business Transformation Agency and transferred roles and responsibilities such as developing the business enterprise architecture to the Office of the Deputy CMO.
Full-time CMO established	February 2018	The NDAA for FY 2017 established a standalone CMO position that would be distinct from the Deputy Secretary of Defense and assigned a number of key responsibilities to the CMO. These responsibilities included managing DOD's enterprise business operations. The CMO was also responsible for overseeing efforts associated with the business enterprise architecture and the business and financial systems certification and approval process.
CMO position repealed	January 2021	Section 901 of the William M. (Mac) Thornberry NDAA for FY 2021 repealed the position of CMO within DOD.
Business and financial system oversight responsibilities reassigned	September 2021	The Deputy Secretary of Defense reassigned responsibilities previously assigned to the Office of the CMO, including responsibilities associated with overseeing business and financial systems.

Source: GAO reports and Department of Defense (DOD) documentation. | GAO-23-104539

DOD has also initiated a variety of efforts intended to help modernize its business and financial systems environment. For example, in 1989, it initiated the Corporate Information Management Initiative to help improve its financial systems environment. More recently, it has focused on establishing guidance and tools to support its annual certifications of business and financial systems.

Table 3 describes examples of efforts DOD has undertaken to help improve its business and financial systems environment over the last 30 plus years.

**Table 3: Examples of Efforts DOD Has Undertaken Associated with Improving its Business and Financial Systems Environment**

Effort	Month and year initiated	Description
Corporate Information Management Initiative	October 1989	The initiative called for streamlining DOD business processes and developing modern information systems. Among other things, the initiative was to select its best existing systems for use as migratory financial systems. These systems were to be followed by target systems.

Letter

Effort	Month and year initiated	Description
Defense Business Operations Fund	October 1991	DOD established this fund by consolidating nine existing industrial and stock funds and five other activities operated throughout DOD. Through this consolidation, the fund was intended to bring greater visibility and management to the overall cost of carrying out certain critical DOD business operations.
Defense Reform Initiative	November 1997	This initiative represented a set of proposed actions aimed at improving the effectiveness and efficiency of DOD's business operations, particularly in areas that have been long-standing problems—including financial management.
Financial Management Improvement Plan	October 1998	DOD's first financial management improvement plan identified over 200 initiatives that were intended to improve the department's financial operations and systems. In 1999, we reported that the plan provided the first-ever vision of the department's future financial management environment.
Financial Management Modernization Program	July 2001	The modernization program was to provide the department's leaders with accurate and timely information through the development and implementation of a financial management enterprise architecture. On May 20, 2003, the Under Secretary of Defense (Comptroller) issued a memorandum that renamed and updated the Financial Management Modernization Program to the Business Management Modernization Program.
Financial Management Enterprise Architecture	Approximately 2002	DOD undertook the development and implementation of a financial management enterprise architecture to address its systemic problems and assist in the transformation of the department's business operations. In May 2003, the DOD Comptroller changed the name from the financial management enterprise architecture to the business enterprise architecture. This change was to reflect the transformation of department-wide business operations and supporting systems, including accounting and finance, budget formulation, acquisition, inventory management, logistics, personnel, and property management systems.
Investment Review Board for Business and Financial Systems	February 2005	DOD established the Defense Business Systems Management Committee as required by the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005. As DOD's highest-ranking business modernization governance body, the committee's responsibilities included overseeing DOD's business and financial management system investment management efforts. These responsibilities were subsequently subsumed by the Defense Business Council.
Business System Annual Certification and Review Guidance	April 2006	The guidance, <i>Investment Certification and Annual Review Process User Guidance</i> , complemented May 2005 guidance on DOD's investment review board process. DOD has updated the guidance multiple times since April 2006, with the most recent update occurring in June 2018.
Defense Information Technology Investment Portal	May 2013	DOD developed the portal as a tool for tracking business and financial system annual certification decisions. As of August 2022, DOD continued to use this tool.
Integrated Business Framework Data Alignment Portal	Approximately 2015	DOD developed this portal as a tool for consolidating information about its business enterprise architecture and business and financial system compliance information. DOD also used this portal to document associated functional strategies. According to officials from the office of the DOD CIO, DOD discontinued its use of this portal in September 2021.
Business Capability Acquisition Cycle	February 2017	DOD issued DOD Instruction 5000.75, which established policy for the use of a new acquisition cycle for business systems.

Source: GAO reports and Department of Defense (DOD) documentation. | GAO-23-104539

## DOD Established a Process for Overseeing Its Business and

## Financial Systems but Lacks Fully Developed Guidance and Reliable Data

As discussed, key elements of business and financial management systems oversight include establishing oversight processes, using and communicating quality information, sustaining leadership commitment, and managing risk.<sup>51</sup> DOD has taken steps to address each of these elements, but has not fully addressed all of the elements.

- **Oversight processes.** DOD has established a process for managing its portfolio of business and financial systems consistent with statutory requirements. However, DOD and military department guidance does not fully address how programs and decision-makers are to make and substantiate key decisions and excludes systems in sustainment from key requirements.
- **Quality information.** DOD maintains data about business and financial system compliance with statutory requirements, but the reliability of these data are limited. In addition, DOD has discontinued use of a tool intended to monitor detailed compliance with its business enterprise architecture.
- **Leadership commitment.** DOD has experienced frequent changes in leadership positions responsible for business and financial systems.
- **Managing risk.** DOD is taking steps to address identified risks and challenges associated with its modernizing its financial systems environment.

As a result, DOD does not have the guidance and information it needs to help ensure that it is developing systems that can support its efforts to achieve a clean audit opinion.

---

<sup>51</sup>Oversight processes contribute to improved acquisition management and include processes for managing portfolios of investments and enterprise architecture compliance. See, for example, [GAO-22-105184](#), [GAO-17-63](#), [GAO-14-704G](#), [GAO-10-846G](#), [GAO-04-394G](#), [GAO-03-669](#), and [AIMD-10.1.15](#). Also see Pub. L. No. 108-375, § 332, 118 Stat. at 1851 (2004), as amended in pertinent part by Pub. L. No. 114-92, § 883(a), 129 Stat. at 942 (2015).

---

## DOD and Military Departments Have Defined Processes to Oversee Systems, but Guidance Does Not Fully Address Key Decisions

### DOD and the Military Departments Have Issued Guidance to Define Oversight Processes

DOD and the military departments have issued guidance to define oversight processes for business and financial systems. Specifically, the guidance establishes a tiered process for reviewing its portfolio of business and financial management systems based on their expected costs, consistent with statutory requirements. As previously described, Title 10 U.S.C. § 2222 calls for DOD to annually review and certify compliance of covered defense business systems<sup>52</sup> with five statutory requirements.<sup>53</sup>

The guidance addresses DOD's portfolio of systems that expect to spend more than \$250 million over the course of the Future-Years Defense Program (FYDP) (referred to as "priority business systems"). The guidance also addresses DOD's portfolio of systems that expect to spend less than \$250 million over the course of the FYDP (referred to in this report as "non-priority business systems"). In general, DOD addresses initial approvals and annual certifications for all priority business systems and non-priority defense agency systems at the department-wide level, while military departments address these actions for non-priority systems. Specifically:

- **Defense-wide.** In January 2020, DOD issued its most recent version of DOD Instruction 5000.75, which describes the department's business capability acquisition cycle. In addition, in June 2018, DOD issued its most recent investment management and certification guidance. That guidance addresses, among other things, systems that plan to spend more than \$250 million over the course of the FYDP. The guidance also addresses covered systems that exist within a defense agency, field activity, or support more than one

---

<sup>52</sup>As discussed, business systems include financial systems.

<sup>53</sup>The five compliance requirements, as discussed in this report, are associated with business process reengineering, the business enterprise architecture, requirements plans, acquisition strategy, and addressing DOD's auditability requirements.



portion of DOD. It calls for systems to be certified if they plan to spend more than \$1 million over the course of the FYDP.<sup>54</sup>

- **Army.** The Army's January 2018 implementation guidance for DOD Instruction 5000.75 and May 2021 Defense Business System Annual Certification and Portfolio Review Guidance provides additional information on how Army systems are to implement the statutory requirements. Army guidance states that all Army business systems are subject to all certification requirements cited in 10 U.S.C. § 2222.
- **DON.** DON's February 2019 Defense Business Systems Investment Certification Manual V 1.2 provides additional guidance on how DON systems are to implement the statutory requirements. DON guidance states that all systems that expect to spend over \$10 million over the FYDP must undergo annual certifications.
- **Air Force.** In July 2018, the Air Force issued guidance on Business Capability Requirements, Compliance, and System Acquisition.<sup>55</sup> The guidance states that that it was updated, in part, to address the requirements of 10 U.S.C. § 2222. Further, in February 2021, the Air Force issued its most recent annual certification guidance. The guidance requires all systems that plan to spend \$1 million over the course of FYDP on development or sustainment to be reviewed for certification prior to obligating funds.

Title 10 U.S.C. § 2222 also gives DOD decision-makers the ability to enforce compliance with legislative requirements. In particular, it allows DOD to restrict a covered defense business system from obligating funds if the system does not comply with these requirements, which could encourage system owners to take appropriate steps to comply.

### DOD Guidance Does Not Describe How Priority Business Systems are to Address Statutory Requirements

The department's *June 2018 Defense Business Systems Investment Management Guidance, Version 4.1* describes tiered guidance to prioritize defense business systems for addressing the annual certification requirements as described in 10 U.S.C. § 2222. DOD has also issued DOD Instruction 5000.75, which governs the acquisition of business system investments. According to DOD guidance and officials, this

---

<sup>54</sup>In September 2020, DOD issued a memo changing the lower threshold to \$25 million for covered systems that exist within a defense agency, field activity, or support more than one portion of DOD.

<sup>55</sup>Air Force Manual 63-144, *Business Capability Requirements Compliance, and Systems Acquisition* (July 25, 2018).

guidance applies to approvals of priority business systems that are to be certified and approved at the corporate-DOD level and to initial approvals and annual certifications that occur throughout the department. This includes systems that expect to spend over \$250 million over the course of the FYDP (i.e., priority business systems).

However, DOD guidance for priority business systems does not fully address initial investment approval or describe expectations for documenting or substantiating compliance with statutory requirements for annual certifications. Specifically, the guidance discusses the requirements, but does not describe how systems are to demonstrate or how decision makers are to substantiate system compliance. For example, DOD’s guidance does not describe how approval authorities are to determine compliance with the auditability requirement.

Table 4 below provides an overview of our assessment of the department’s guidance relative to the initial approval and annual certification requirements for priority business systems. The department’s efforts to address these requirements are discussed in more detail in Appendix II.

**Table 4: Extent to Which the Department of Defense (DOD) Guidance Addresses Requirements for Initial Approval and Annual Certification for Priority Business Systems**

Statutory requirement	Extent to which DOD guidance addresses initial approval requirements	Extent to which DOD guidance addresses annual certification requirements
Business process reengineering and elimination of unique software requirements and interfaces	partially addressed	partially addressed
Compliance or planned compliance with the business enterprise architecture	partially addressed	partially addressed
Valid, achievable requirements and a viable plan for implementing those requirements	partially addressed	partially addressed
An acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems	partially addressed	partially addressed
Compliance with the Department’s auditability requirements	partially addressed	partially addressed

Legend:

- Fully addressed: Guidance explains how systems are to address and decision-makers are to substantiate this requirement.
- ⦿ Partially addressed: Guidance discusses the requirement, but does not fully describe how systems are to address and decision-makers are to substantiate this requirement.
- Not addressed: Guidance does not discuss this requirement.

Source: GAO Analysis of Department of Defense documentation. | GAO-23-104539

An official from the office of the DOD CIO stated that that the program manager collaborates with the appropriate decision authority to develop

necessary certification artifacts and prepare for certification as early as practical in the lifecycle. This official added that mandating specific documentation would be inefficient. Nevertheless, officials from the office of the DOD CIO stated that they recognize the guidance can be improved. They added that the office is newly responsible for updating the guidance after the elimination of the CMO position. In addition, they noted that they would address gaps identified by GAO.

Without fully developed guidance that addresses the initial approval and annual certification requirements for priority business systems, the department risks investing funds on developing and maintaining systems that may not meet these key statutory requirements. The department also risks continuing to develop and maintain systems that do not support the development of auditable financial statements. Moreover, without more fully defined DOD-level guidance, DOD risks that inconsistent initial approval and annual certification decisions will be made at other levels of the organization.

---

## DOD Guidance Does Not Fully Address Non-Priority Business System Compliance

Title 10 U.S.C. § 2222 calls for business systems that plan to spend between \$50 million and \$250 million over the FYDP to have their initial approvals and annual certifications approved by the CMO of their respective military department.<sup>56</sup> In addition, according to section 2222 and DOD guidance, the USD(C)/CFO and DOD CIO are the approval authorities for systems that exist within a Defense Agency, field activity, or support more than one portion of DOD. Section 2222 also states, among other things, that the CMO of each of the military departments is to issue and maintain supporting guidance, as appropriate.

DOD and military department-level guidance did not fully address how non-priority covered systems are to demonstrate or how decision-makers are to substantiate compliance with statutory requirements. For example, Army guidance for initial approvals describes how systems are to substantiate and approval authorities are to validate compliance with the requirement for having valid, achievable requirements and a viable plan for implementing them. Specifically, the Army's January 2018 Implementation Guidance for DOD Instruction 5000.75 states that, prior to Chief Management Officer certification, the functional sponsor will present

---

<sup>56</sup>As discussed, business systems include financial systems.

all IT functional requirements and resource needs to the Army Business Council – Senior Review Group. This group is to validate and approve the final IT functional requirements for the solution and may modify the requirements as needed. The guidance also calls for the functional sponsor to brief parts of the capability implementation plan as part of this discussion.

However, Army guidance for annual certifications does not fully describe how systems are to substantiate and approval authorities are to validate compliance with the business enterprise architecture compliance requirement. Specifically, the Army’s May 2021 Defense Business System Annual Certification and Portfolio Review Guidance states that Army business enterprise architecture assessments must be performed and documented in DOD’s Integrated Business Framework – Data Alignment Portal. In addition, the Army provided training materials for how systems are to document business enterprise architecture compliance. However, officials from the Office of the Department of Defense CIO stated that the portal is no longer being used.

In addition, Army guidance for initial approvals does not describe how systems are to substantiate and approval authorities are to validate compliance with the department’s auditability requirement. For example, the Army’s January 2018 Implementation Guidance for DOD Instruction 5000.75 and the Army’s May 2021 Defense Business System Annual Certification and Portfolio Review Guidance do not describe how systems are to substantiate or how approval authorities are to validate compliance with this requirement for initial approval prior to proceeding into development.

Appendix II describes our detailed assessments of this guidance. Tables 5 and 6 below provide an overview of our assessment of DOD and military department guidance relative to the initial approval and annual certification requirements.

**Table 5: Extent to Which Military Department and Defense Agency Guidance Addresses Initial Approval Requirements for Non-Priority Covered Business Systems**

Initial approval requirement	Army	Department of the Navy	Air Force	Defense Agencies
Business process reengineering and elimination of unique software requirements and interfaces	partially addressed	not addressed	partially addressed	partially addressed
Compliance or planned compliance with the business enterprise architecture	partially addressed	not addressed	partially addressed	partially addressed

---

Letter

---

---

<b>Initial approval requirement</b>	<b>Army</b>	<b>Department of the Navy</b>	<b>Air Force</b>	<b>Defense Agencies</b>
Valid, achievable requirements and a viable plan for implementing those requirements	fully addressed	not addressed	partially addressed	partially addressed
An acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems	partially addressed	not addressed	partially addressed	partially addressed
Compliance with the Department's auditability requirements	not addressed	not addressed	partially addressed	partially addressed

---

Legend:

● Fully addressed: Guidance explains how systems are to address and decision-makers are to substantiate this requirement.

⦿ Partially addressed: Guidance discusses the requirement, but does not fully describe how systems are to address and decision-makers are to substantiate this requirement.

○ Not addressed: Guidance does not discuss this requirement

Source: GAO Analysis of Department of Defense documentation. | GAO-23-104539

**Table 6: Extent to Which Military Department and Defense Agency Guidance Addresses Annual Certification Requirements for Non-Priority Covered Business Systems**

Annual certification requirement	Army	Department of the Navy	Air Force	Defense Agencies
Business process reengineering and elimination of unique software requirements and interfaces	partially addressed	fully addressed	partially addressed	partially addressed
Compliance or planned compliance with the business enterprise architecture	partially addressed	partially addressed	partially addressed	partially addressed
Valid, achievable requirements and a viable plan for implementing those requirements	partially addressed	partially addressed	partially addressed	partially addressed
An acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems	partially addressed	partially addressed	partially addressed	partially addressed
Compliance with the Department's auditability requirements	partially addressed	partially addressed	partially addressed	partially addressed

Legend:

- Fully addressed: Guidance explains how systems are to address and decision-makers are to substantiate this requirement.
- ⓘ Partially addressed: Guidance discusses the requirement, but does not fully describe how systems are to address and decision-makers are to substantiate this requirement.
- Not addressed: Guidance does not discuss this requirement.

Source GAO Analysis of Department of Defense documentation. | GAO-23-104539

Officials from DOD's Office of the CIO noted that they recognize gaps in the guidance and indicated that they would take steps to address gaps identified by GAO.

Military department officials either stated that existing guidance for these systems was sufficient or recognized gaps in the guidance. In particular:

- Army officials stated that the requirements for annual certification are sufficient to demonstrate that systems have addressed initial certification requirements shortly after systems have proceeded into system development. Army officials also pointed to additional guidance for financial systems. However, this guidance is not discussed in the Army's guidance for initial approval or annual certification.
- DON officials recognized that their guidance was outdated and needs to be updated.

- Air Force officials stated that their guidance was sufficient to demonstrate that systems have addressed initial approval and annual certification requirements. However, the guidance does not fully describe how systems are to address and decision-makers are to substantiate compliance with the requirements.

Without fully developed guidance for non-priority covered systems that addresses the initial approval and annual certification requirements as described in 10 U.S.C. § 2222, DOD risks investing funds on developing and maintaining systems that do not meet key statutory requirements. In addition, DOD risks developing and maintaining systems that do not support the broader goals of developing systems that are more likely to contribute to auditable financial statements.

Ensuring updated and comprehensive guidance exists is particularly important in light of the staff leadership turnover experienced within business and financial systems. For example, In June 2022, we reported that, among DOD's 25 major business IT systems, system officials reported that program managers remained with systems for an average of two years and five months.<sup>57</sup> Ensuring that system leadership understands expectations for initial approvals and annual certifications is critical for helping to ensure systems take the steps needed for fully complying with statutory requirements. Such compliance is important to achieving auditable financial statements.

### DOD Has Excluded Systems in Sustainment from Key Statutory Requirements

As discussed, 10 U.S.C. § 2222 calls for covered DOD business and financial systems to annually certify that programs meet five statutory requirements. Two of these statutory requirements include that systems have

- valid, achievable program requirements and a viable plan for implementing those program requirements, and
- an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique program requirements, incorporate unique program requirements, or incorporate unique interfaces to the maximum extent practicable.

Title 10 U.S.C. § 2222 does not describe a process for systems to be excluded from these statutory requirements. Systems in sustainment

---

<sup>57</sup>[GAO-22-105330](#).

would benefit from ensuring they have valid, achievable program requirements and taking steps to limit system customizations as they continue to evolve and address new program requirements.

However, DOD has excluded systems from meeting these statutory requirements as part of its annual portfolio oversight process. DOD's annual investment certification guidance provides the option for systems to select that they are in sustainment and do not have a compliance plan for these requirements. Moreover, DOD data indicates that 120 (58 percent) of the 208 business and financial systems relevant to the audit and included in the data were in sustainment and therefore did not need to comply with these requirements.

DOD officials stated that, in DOD's opinion, systems in sustainment are not subject to these two statutory requirements. They also noted that systems in sustainment do not require acquisition documentation. In addition, in September 2022, an official from DOD's office of the USD(C)/CFO stated that the Director of the Office of Administration and Management is currently coordinating proposed legislation to update 10 U.S.C. § 2222. According to this official, there is an opportunity to address that systems in sustainment are not subject to the acquisition strategy and requirements planning requirements.

However, by excluding application of these requirements, DOD may be missing important opportunities for improving its systems that are in sustainment. For example, systems in sustainment should routinely continue evolving to address new information security requirements. They may also seek other improvements, such as adapting to updated business processes or eliminating unnecessary customizations. DOD has the ability, via its implementing guidance, to define expectations for systems in sustainment that may help these systems limit complexity as they evolve to address new requirements or seek to eliminate unnecessary customizations. This may particularly be the case for efforts to improve how DOD uses commercial off-the-shelf systems. Without fully implementing statutory requirements to hold its systems accountable, DOD is likely limiting its efforts to achieve a more streamlined and efficient system environment. This in turn will further delay reaching the goal of a clean audit opinion.



---

---

## DOD Data Show Compliance with Statutory Requirements, but Its Reliability is Limited

Effective oversight includes using quality information to make decisions and communicating quality information, as appropriate, to help DOD ensure business and financial systems are meeting appropriate requirements. As previously described, 10 U.S.C. § 2222 calls for DOD to annually certify compliance of covered defense business systems with five statutory requirements.<sup>58</sup> These covered systems include business and financial systems that support DOD's efforts to achieve a clean audit opinion. In addition, the department's June 2018 investment management and certification guidance requires that precertification authorities utilize the Defense IT Investment Portal (DITIP) to document system assertions for compliance with these requirements.<sup>59</sup> GAO's *Standards for Internal Control in the Federal Government*<sup>60</sup> also call for organizations to use quality information when making decisions.

DOD uses DITIP to document the compliance status for the five statutory requirements across its covered business and financial system investments. According to the data documented in DITIP for systems that DOD identified as relevant to the annual financial audit and that identified that the requirements were required or applicable, DOD data shows significant compliance or planned compliance. For example:

- 187 of the 189 systems (99 percent) complied or planned to comply with the business process reengineering requirement.
- 190 of 192 systems (99 percent) complied or planned to comply with the business enterprise architecture requirement.
- 66 of 66 systems (100 percent) complied or planned to comply with the requirement plan requirement.
- 67 of 67 systems (100 percent) complied with the acquisition strategy requirement.

---

<sup>58</sup>The five compliance requirements, as discussed in this report, are associated with business process reengineering, the business enterprise architecture, requirements plans, acquisition strategy, and addressing DOD's auditability requirements.

<sup>59</sup>DOD uses the term precertification authority to address compliance determinations made by component level leadership before approval by the appropriate approval officials. For example, the component precertification authority is to make system and business system portfolio business enterprise architecture compliance determinations in advance of the appropriate approval official determinations based on precertification determinations.

<sup>60</sup>[GAO-14-704G](#).

- 128 of 136 systems (94 percent) complied or planned to comply with the auditability requirement.

Table 7 summarizes the DITIP data for systems that provided responses and indicated that the compliance requirements were required or applicable.

**Table 7: Partial Summary of DOD’s Data on Business System Compliance with Statutory Requirements**

Compliance responses	Business process reengineering compliance	Business enterprise architecture compliance	Requirement plan	Acquisition strategy	Auditability requirement
Compliant	179	145	60	67	84
Planned to comply	8	45	6	no responses	44
Not Compliant	2	no responses	no responses	no responses	3
Compliance assessment not completed	no responses	2	no responses	no responses	5
<b>Total</b>	<b>189</b>	<b>192</b>	<b>66</b>	<b>67</b>	<b>136</b>

Legend: A dash (“-”) indicates that there were no responses under the specified category.

Source: GAO analysis of Department of Defense (DOD) data. | GAO-23-104539

Note: These data do not include responses indicating no response, not required, or not applicable.

In addition to these compliance responses, some systems either did not provide a response or indicated certain requirements were not applicable. Table 8 summarizes the DITIP data for the entire set of systems that DOD identified as relevant to the annual financial audit, including systems that either did not respond or indicated that requirements were not applicable.

**Table 8: Complete Summary of DOD's Data on Business System Compliance with Statutory Requirements**

Compliance responses	Business process reengineering compliance	Business enterprise architecture compliance	Requirement plan	Acquisition strategy	Auditability requirement
Compliance required or applicable <sup>a</sup>	189	192	66	67	136
No Answer	1	1	1	1	1
Not required (Legacy system) <sup>b</sup>	18	15	21	20	-
Not required (System in sustainment) <sup>c</sup>	no responses	no responses	120	120	no responses
Not applicable	no responses	no responses	no responses	no responses	71
<b>Overall total</b>	<b>208</b>	<b>208</b>	<b>208</b>	<b>208</b>	<b>208</b>

Legend: A dash ("-") indicates that there were no responses under the specified category.

Source: GAO analysis of Department of Defense (DOD) data. | GAO-23-104539

<sup>a</sup>Systems indicated that compliance was required or applicable.

<sup>b</sup>DOD defines legacy systems as systems that it plans to phase out over the next 36 months. It does not require legacy systems to comply with certain requirements.

<sup>c</sup>DOD does not require systems that have proceeded past the development phase (i.e., systems in sustainment) to comply with selected requirements.

However, some data about systems were internally inconsistent or missing. For example:

- Nine systems did not assert compliance because DOD indicated they were legacy systems (a system that has a sunset date within 36 months). However, the "transition status" for these nine shows them as core business systems (an enduring system with a sunset date greater than 36 months) instead of legacy systems. In addition, within the DITIP data, the lifecycle end dates for these systems were over 36 months. According to DOD guidance, these systems should not be considered legacy systems.
- Data associated with one system indicated that the auditability criterion was not applicable because the system was in development. However, DOD guidance does not describe exceptions for systems that are in development. In addition, statutory requirements call for systems to assert compliance with all five requirements before proceeding into development.
- Data for one system did not include assertions for any of the five elements. This system did not provide any rationales in DITIP indicating why they did not report a status for these certification fields.

- Seventy-one of the systems that DOD identified as relevant to the annual financial audit indicated that the auditability requirement was not applicable.

Moreover, of the 71 systems that indicated that the auditability requirement was not applicable, we identified 58 that were identified in DOD's Financial Improvement and Audit Readiness (FIAR) Systems Database in May 2021 as systems that are relevant to the audit. DOD officials stated that this requirement should be applicable to these systems.

DOD officials stated that they are aware of issues with the DITIP data and are taking steps to improve it. For example, officials from the Office of the DOD CIO stated that they have submitted a request to change the logic in Defense IT Portfolio Repository (DITPR) so the portal will no longer allow a system that will be retired beyond 36 months to indicate that it is a legacy system.<sup>61</sup> According to DOD officials, system data in DITIP is maintained and imported from DITPR. In addition, they added that they are taking steps to streamline their data about business and financial systems. For example, they expect to move the data from the FIAR Systems Database into the DITPR environment in the spring of 2023.

DOD officials also stated that the department has already begun taking steps towards creating a more effective and integrated approach to policy, governance, and oversight of systems relevant to the annual financial audit. For example, DOD officials stated that, in December 2021, the department created the Defense Business Systems Committee as a permanent committee under its Defense Business Council. Among other things, the committee is chartered with facilitating the collection of data necessary to execute defense business system portfolio management activities.

However, DOD officials did not identify how or when they will complete efforts to improve the accuracy of the DITIP data, streamline the multiple oversight processes, and facilitate the collection of data to ensure that data on business and financial system certifications are complete and accurate. Without reliable data to manage its portfolio of business and financial systems, including reliable data on legacy systems and systems

---

<sup>61</sup>DITPR is DOD's authoritative repository for system information used to meet internal and external reporting requirements. Among other things, DITPR provides a common central repository for IT system information, such as system start and end dates, to support the certification process. It also supports component-level IT portfolio management.

that support the department's audit efforts, DOD lacks the information it needs to ensure that systems are fully complying with statutory requirements. In addition, it lacks the information needed to ensure that its oversight efforts are contributing to a more effective business and financial systems environment. Moreover, fully complying with each of the statutory requirements is important for DOD's efforts to achieve a clean audit opinion.

Further, as of January 2022, DOD reported that its Independent Public Accountants had identified 1,411 unresolved IT-related notices of findings and recommendations associated with 3,478 underlying IT-related issues.<sup>62</sup> The magnitude of these results raises further questions about data reliability, which may also impact the extent of compliance with statutory requirements.

#### DOD Has Discontinued Use of a Tool to Monitor Detailed Compliance with the Business Enterprise Architecture

As discussed, 10 U.S.C. § 2222 calls for covered business and financial systems to annually certify compliance with DOD's business enterprise architecture. In addition, as described, GAO's *Standards for Internal Control in the Federal Government*<sup>63</sup> call for organizations to use quality information when making decisions.

DOD uses its DITIP tool to document if a system complies with its business enterprise architecture (e.g., the system complies, plans to comply, or does not comply). Until recently, DOD also used a different tool, the Integrated Business Framework Data Alignment Portal (IBF-DAP), to document the details of how systems complied with the business enterprise architecture. However, DOD CIO officials reported that DOD had discontinued the use of this tool as of September 2021. DOD issued

---

<sup>62</sup>Department of Defense, Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *Financial Improvement and Audit Remediation Report* (June 2022). This report discusses the status of IT notices of findings and recommendations and underlying issues as of January 2022.

<sup>63</sup>[GAO-14-704G](#).

a memorandum in August 2022 directing systems to document business enterprise architecture compliance in a different tool, DITPR.<sup>64</sup>

However, the information captured in DITPR represents only alignment to elements of the architecture (e.g., selecting the business activities associated with the system) and does not include asserting compliance to more detailed elements. For example, the previous tool required systems to identify and assert compliance with, among other things, relevant laws, regulations and policies and also identify and assert compliance to relevant business rules.<sup>65</sup> This information is not captured in the new tool. Officials from the office of the DOD CIO stated that DOD is using the new tool as a baseline solution and is analyzing other options. DOD officials further reported that they are revisiting their approach to the business enterprise architecture and planned to issue a new modernization strategy for the architecture by the end of December 2022.

Without a tool that collects comprehensive business enterprise architecture compliance data to document in detail how systems comply with the architecture, DOD risks developing business and financial systems that continue to be limited in their ability to effectively share information and ultimately support the goal of achieving a clean audit opinion.

---

<sup>64</sup>As discussed previously in this report, DITPR is DOD's authoritative repository for system information used to meet internal and external reporting requirements.

<sup>65</sup>Title 10 U.S.C. § 2222(e) calls for the defense business enterprise architecture to include, among other things, policies, procedures, business data standards, and business information requirements that apply uniformly throughout DOD. As part of documenting compliance in IBF-DAP, a system identified relevant controls, including, among other things, regulations, policies, and business rules documented in the business enterprise architecture. The system then asserted compliance with these controls. Examples of regulations and policies documented in the architecture include, compliance with DOD Financial Management Regulations, volume 1, Chapter 4, Standard Financial Information Structure, and compliance with DOD Financial Management Regulations, volume 1, Chapter 9, Financial Records Retention. Examples of business rules include, "Core\_Systems\_Seven," which requires that the Core financial system must provide automated functionality to generate the Status of Funds query and report and "Asset\_Unique\_Identifier\_4," which requires that Each Real Property Unique Identifier must be an 18 character integer.

---

## Sustained DOD Leadership Commitment Is Essential to Success

As we have previously reported, demonstrating sustained leadership commitment is imperative for successful business transformation.<sup>66</sup> In our 2003 report on results-oriented cultures at federal agencies, we noted that people are at the center of any serious change management initiative.<sup>67</sup> This includes top leadership, which must drive the transformation. In addition, leadership commitment is a key practice for addressing high risk areas to support removing them from our high risk list.<sup>68</sup>

Over the last two decades, DOD has assigned responsibility for business systems modernization to top leadership within the department. However, as shown below, those responsibilities have frequently shifted over time.

- In September 2021, the Deputy Secretary of Defense reassigned responsibilities previously assigned to the Office of the CMO, including responsibilities associated with overseeing business and financial systems.
- In January 2021, section 901 of the William M. (Mac) Thornberry NDAA for FY 2021 repealed the position of CMO within DOD.
- In February 2018, the NDAA for FY 2017 established a standalone CMO position that would be distinct from the Deputy Secretary of Defense and assigned a number of key responsibilities to the CMO. These responsibilities included overseeing efforts associated with the business enterprise architecture and the business and financial systems certification and approval process.
- In September 2011, DOD eliminated the Business Transformation Agency and transferred roles and responsibilities, such as developing the business enterprise architecture, to the Office of the Deputy CMO.
- In October 2008, in response to provisions of the NDAA for FY 2008, DOD established the position of Deputy CMO. Prior to this designation, DOD also named the Deputy Secretary of Defense as the department's CMO. The Deputy CMO assumed responsibilities for managing the Business Transformation Agency.

---

<sup>66</sup>See, for example, [GAO-21-532T](#).

<sup>67</sup>[GAO-03-669](#).

<sup>68</sup>[GAO-22-105184](#).

- In October 2005, DOD established the Business Transformation Agency. The agency was established, in part, to advance DOD's business and financial systems modernization efforts. Among other things, the agency was to be responsible for ensuring consistency and continuity across the department's core business missions with respect to, for example, business process reengineering and related business system matters. This included assuming responsibility for developing DOD's business enterprise architecture and guiding business transformation efforts at the DOD enterprise level.

These changes have also limited DOD's ability to exercise consistent oversight over its business and financial systems. For example, DOD has initiated and restarted multiple efforts to improve its business enterprise architecture since 2015. As a result, efforts associated with improving oversight of these systems have made limited progress in recent years.

We will continue to monitor DOD's efforts to demonstrate sustained leadership commitment through our ongoing work, including our biennial high risk reports.

---

## DOD Is Taking Steps to Address System Risks

Effective oversight also includes identifying, analyzing, and responding to risks.<sup>69</sup> Office of Management and Budget Circular A-123 notes that risk management involves, among other things, identifying challenges and developing solutions.<sup>70</sup>

While not generalizable, officials from entities across DOD provided their perspectives on the challenges facing the department as it attempts to modernize its financial systems environment.<sup>71</sup> Examples of challenges reported by DOD officials included:

---

<sup>69</sup>GAO-14-704G and GAO-17-63.

<sup>70</sup>OMB, *Management's Responsibility for Enterprise Risk Management and Internal Control*, Circular No. A-123, (July 15, 2016).

<sup>71</sup>This includes Office of the Secretary of Defense-level officials and officials from the Departments of the Army, Air Force, and Navy responsible for managing DOD's portfolios of business and financial management systems, as well as officials representing the eight systems that we selected for review.



- **Legacy systems.** Department of the Navy (DON)<sup>72</sup> officials stated that a large number of disparate legacy financial systems do not adhere to data standards, transactional standards, or uniform processes. Officials representing the Army's General Fund Enterprise Business System stated that the potential to expose classified data and the increase in classification of aggregated data leads to increased costs to sustain legacy systems. Officials representing the office of the USD(C)/CFO and the Air Force's Defense Enterprise Accounting and Management System also cited legacy systems as a challenge.
- **Systems designed prior to DOD's audit requirements.** Air Force officials cited systems that were designed prior to DOD's audit requirements as a challenge. DON officials noted that many aging financially relevant and feeder systems were implemented prior to the establishment of OMB Federal Financial Management Improvement Act of 1996 and DOD Standard Financial Information Structure requirements to support the preparation of auditable financial statements.
- **System interfaces.** Air Force officials cited the lack of system interfaces as a challenge. Officials representing the Army's General Fund Enterprise Business System cited point-to-point interfaces that lead to system integration complexity and increased redesign costs, data latency, and reconciliation and translation efforts.
- **Human capital.** Army officials cited as a challenge not having a trained workforce with subject matter expertise in budget and accounting management and IT modernization opportunities. An official representing the Air Force's Defense Enterprise Accounting and Management System noted that as systems acquire new personnel, they have to work through training people who have not worked on financial statement audits. An official representing the Air Force's Financial Inventory Accounting and Billing System cited a lack of trained personnel. Officials representing the Defense Logistics Agency's Enterprise Business System stated that their system faced challenges similar to agencies across the federal workforce related to having technical skills from industry.
- **Budgets and resources.** Army officials cited the competition for resources among required mission improvements, emerging threats and requirements, and required business improvements within the financial management system environment. They also noted budget reductions that require a continued re-baselining of project requirements. Officials representing the Army's General Fund

---

<sup>72</sup>As noted, references in this report to DON reflect that DON encompasses both the Navy and the Marine Corps.

Enterprise Business System cited adequate planning, funding, and prioritization of enhancements to meet emerging auditability standards, business processes, and IT General Controls not previously implemented within the system as challenges. An Air Force official representing the Defense Enterprise Accounting and Management System referred to the number of audits the system encounters in a year. This official added that these audits require significant effort, which affects the ability of the system to complete its mission.

- **Systems not designed to be financial management systems.** Officials representing the Air Force's Defense Enterprise Accounting and Management System stated feeder systems that are not financial management systems at their core present challenges for reconciliation. Officials representing the Navy Standard Integrated Personnel System noted that the system went live in 1999 as a personnel system and later evolved to include interfaces with other financial systems. They stated that enforcing financial management-related controls after the system was designed and implemented leads to more inefficiencies for users and interface partners, along with higher sustainment costs.
- **Number of systems.** An official from the office of the USD(C)/CFO cited the number of systems as a challenge. This official stated that there are 200-300 systems relevant to the annual financial audit and many of them perform duplicative functions. The official also stated that some go back to the 1960s. Air Force officials also noted that the number of systems that feed the financial statements is a challenge.

These challenges present risks to DOD as it works to modernize its financial systems environment and achieve a clean audit opinion.

### DOD's Efforts to Address Identified Risks and Challenges

DOD has taken a number of steps to address risks and challenges identified by DOD officials. This includes establishing its annual business and financial system certification process and establishing other entities to provide additional guidance and support.

As discussed, DOD's annual business and financial system certification process is a key department-wide oversight mechanism intended, in part, to help proactively address some of its modernization challenges.<sup>73</sup> For example, DOD guidance calls for covered systems to certify that they

---

<sup>73</sup>This process is called for by 10 U.S.C. § 2222.

have met, or plan to meet, requirements such as complying with DOD's business enterprise architecture, limiting the number of unique interfaces, and complying with the department's auditability requirements.<sup>74</sup> Proactively addressing requirements such as these could help address some of the challenges associated with legacy systems and interfaces described above. However, as discussed in this report, DOD needs to improve its guidance and data associated with its efforts to implement these requirements.

In addition, with respect to its business and financial systems, we reported in June 2022 that DOD finalized its updated Defense Business Council charter in January 2022 and DOD officials stated that the department has identified a permanent subcommittee to guide defense business systems.<sup>75</sup> Doing so may help the department as it takes steps to address risks to modernizing its systems environment.

With respect to its larger systems environment, we also reported that DOD recognizes the many challenges facing programs as they develop software and are taking steps to help address those challenges. For example, DOD has implemented a senior steering group to lead department-wide collaboration on software modernization activities. According to the group's December 2021 charter, its scope includes defining better ways to program and budget for software development, which may assist in DOD's efforts to respond more quickly and effectively to system-related risks.<sup>76</sup>

In addition, we reported that DOD released its software modernization strategy in February 2022.<sup>77</sup> Among other things, the strategy recognizes the need for DOD to review and modernize its requirements, budget, acquisition, and security processes to take advantage of new software development approaches and technologies. It also includes objectives

---

<sup>74</sup>The guidance exempts systems that the department plans to retire within 36 months from these requirements and refers to these systems as legacy systems.

<sup>75</sup>GAO, *Business Systems: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning*, [GAO-22-105330](#) (Washington, D.C., June 14, 2022).

<sup>76</sup>Department of Defense, *Software Modernization Senior Steering Group (SSG) Charter* (Dec. 9, 2021).

<sup>77</sup>Department of Defense, *Department of Defense Software Modernization* (Washington, D.C.: Feb. 1, 2022).

---

associated with managing commercial off-the-shelf software for efficiencies and effectiveness.

We will continue to monitor DOD's efforts to address its business and financial system risks as part of our ongoing work, including our annual DOD IT "Quick Look" series of reports.<sup>78</sup>

---

## DOD Has Taken Steps to Improve Its Financial Management Systems Workforce but Lacks a Strategic Approach for Gaps

Taking a strategic approach to workforce planning is another key element of business and financial systems oversight. GAO has previously identified key practices for effective strategic workforce planning:<sup>79</sup> Key practices include the following:

- assess the knowledge and skills needed to execute a program;
- inventory the knowledge and skills of existing staff;
- forecast the knowledge and skills needed over time;
- analyze the gaps in capabilities between the existing staff and future workforce needs, including consideration of evolving program and succession needs caused by turnover and retirement; and
- formulate strategies for filling expected gaps.

DOD officials reported that they do not have a strategic approach for workforce planning for the collective set of staff that support financial

---

<sup>78</sup>See [GAO-21-182](#), [GAO-21-351](#), and [GAO-22-105330](#).

<sup>79</sup>See [GAO-16-593](#); [GAO-13-557](#); and [GAO-04-39](#).

management systems.<sup>80</sup> Specifically, they do not (1) assess the knowledge and skills needed to execute a program; (2) inventory the knowledge and skills of existing staff; (3) forecast the knowledge and skills needed over time; (4) analyze the gaps in capabilities between the existing staff and future workforce needs, including consideration of evolving program and succession needs caused by turnover and retirement; or (5) formulate strategies for filling expected gaps for the government and contractor staff that are collectively needed to support these systems.

Instead, DOD officials explained that they have a variety of efforts under way to help ensure that the government and contractor staff who support its financial management systems have the requisite skills and expertise for specific roles.<sup>81</sup> For government staff, these roles include acquisition, IT management, and financial management. For example:

- **Acquisition.** DOD's Defense Acquisition University is responsible for providing the training necessary to develop qualified DOD acquisition personnel. The University delivers this training through traditional classroom-based courses, online training modules, and acquisition workshops where instructors develop and deliver customized training to support a particular acquisition. Additionally, the University provides a variety of tools and resources to assist personnel performing acquisition-related functions, including the Acquisition Requirements Roadmap Tool, the Defense Acquisition Guidebook, and the Service Acquisition Mall. DOD has established certifications and certification levels for acquisition-related career fields. DOD's certification

---

<sup>80</sup>In this section, financial management systems refer to the business and financial systems that support audit-related activities. According to the Federal Financial Management Improvement Act of 1996, financial management systems are the financial systems and the financial portions of mixed systems necessary to support financial management. The financial portions include automated and manual processes, procedures, controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions. A financial system is an information system, comprised of one or more applications, that is used for collecting, processing, maintaining, transmitting, or reporting data about financial events; supporting financial planning or budgeting activities; accumulating and reporting costs information; or supporting the preparation of financial statements. A mixed system is an information system that supports both financial and nonfinancial functions. The DOD Financial Management Regulation refers to some mixed systems as feeder systems. The regulation defines feeder systems as the manual or automated programs, procedures and processes which develop data required to initiate an accounting or financial transaction but do not perform an accounting operation, such as personnel, property, or logistics systems.

<sup>81</sup>We did not assess DOD's efforts to address human capital needs for each of these specific categories of staff.

programs address acquisition-related functional areas such as contracting and program management.

- **IT specialists.** DOD’s Cyber Workforce Framework describes work roles associated with categories and specialty areas. For example, the “data analyst” work role is associated with the “data administration” specialty area under the broader category of “operate and maintain.” Each work role is assigned a core set of knowledge, skills, abilities, and tasks. Among other things, this framework is intended to be used for DOD-wide workforce management and planning activities, such as facilitating supply and demand analyses.
- **Financial management.** DOD’s Financial Management Strategy for FYs 2022-2026 includes the goal to “cultivate a skilled and inspired financial management workforce.” This goal includes related strategic objectives such as “optimize and evolve financial management training solutions.” The strategy also includes measures associated with each objective. For example, the strategy identifies the metric “increase the percentage of the workforce holding relevant certifications, test-based where possible.” According to the Director, USD(C)/CFO Human Capital and Resource Management, as of May 2022, DOD had identified metrics for the financial management workforce. These metrics included a goal of 95 percent compliance for financial management workforce certification requirements and a stretch goal of 98 percent compliance. The Director noted that, as of May 2022, 95 percent of the financial management workforce was in compliance with certification requirements.

In regards to contractor staff, an official from the office of the DOD CIO stated that the DOD Statement of Work for acquiring contractor support identifies the types and qualifications of contractors needed. The *Department of Defense Handbook, Preparation of Statement of Work* states that the Statement of Work is to specify requirements clearly to, among other things, permit a contractor to determine the levels of expertise, personnel, and other resources needed to accomplish technical objectives and goals.<sup>82</sup>

However, the efforts described by DOD officials did not address the collective set of contractor staff, government acquisition and program management staff, IT specialists, and business area subject matter experts needed to support its financial management systems. While not a

---

<sup>82</sup>Department of Defense, *Department of Defense Handbook, Preparation of Statement of Work*. MIL-HDBK-245E with change 1 (Sept. 12, 2022). According to the handbook, it is for guidance only and is not to be cited as a requirement.

generalizable sample, staff from four of eight selected DOD financial management systems cited human capital challenges. For example, as discussed, an official representing the Air Force’s Financial Inventory Accounting and Billing System cited a lack of trained personnel. In addition, officials representing the Air Force’s Defense Enterprise Accounting and Management System noted that there are always challenges allocating human capital resources.

In addition, in June 2021, GAO reported on DOD’s challenges with software and development staffing for major DOD IT business systems, including systems that support auditability.<sup>83</sup> Specifically, of 22 systems that were developing new software, 18 reported that they faced software development workforce challenges. While this included responses from a mix of business systems, including those that may not support audit-related efforts, it further demonstrates related human capital challenges. Table 9 summarizes these responses.

**Table 9: The Department of Defense (DOD) Business System Officials Reported Challenges with Software Development Staffing**

Challenge	Number of systems that reported experiencing challenges (with government staff)	Number of systems that reported experiencing challenges (with contractor staff)
Concurrency/overlap in staff	11 of 22	13 of 22
Difficult to find staff with required expertise	12 of 22	13 of 22
Difficult to hire enough staff to complete software development	9 of 22	13 of 22
Difficult to hire staff in time to perform planned work	10 of 22	14 of 22
Difficult to obtain necessary staff training	6 of 22	5 of 22
Software engineering staff plans were not realized as expected	10 of 22	13 of 22
Other	4 of 22	2 of 22

Source: GAO analysis of DOD-reported staffing challenges. Initially reported in [GAO-21-351](#). | GAO-23-104539

<sup>83</sup>GAO, *Software Development: DOD Faces Risks and Challenges in Implementing Modern Approaches and Addressing Cybersecurity Practices*, [GAO-21-351](#) (Washington, D.C.: June 23, 2021.)

---

Until DOD takes a strategic approach to the government and contract workforce that support the systems that support auditability, DOD and the military departments will likely not have sufficient information to understand gaps in skills and capabilities between the existing staff and future workforce needs. As a result, DOD further risks the department's efforts to develop and maintain systems that can help achieve a clean audit opinion.

---

## Conclusions

DOD spends billions of dollars each year on its business and financial systems environment, and has spent over 30 years taking steps intended to modernize it. DOD's financial management and business systems modernization efforts have been on GAO's list of high risk programs and initiatives since 1995 and remain a key impediment to the department's efforts to achieve a clean audit opinion.

Although DOD has a process to help ensure that systems address key auditability requirements, the key guidance that DOD and the military departments have developed to guide decision-makers as they make initial approval and annual certification decisions is limited. The lack of detailed guidance puts DOD at risk of making decisions based on a "check the box" exercise that does little to make meaningful improvements.

In addition, DOD allows systems in sustainment to indicate that certain annual requirements are not applicable. Nevertheless, the statutory requirements do not provide an exception for systems in sustainment. Without fully implementing statutory requirements to hold its systems accountable, DOD is limiting its efforts to achieve a more streamlined and efficient system environment.

Moreover, the data generated by the process are not reliable. As a result, DOD risks making decisions about systems based on faulty information. DOD has also discontinued the tool that systems used to document detailed alignment to and compliance with the department's business enterprise architecture. Without a tool to document more detailed compliance with DOD's business enterprise architecture, the department risks developing business and financial systems that continue to be limited in their ability to support the goal of achieving a clean audit opinion.



Lastly, DOD's stovepiped approach to improving the workforce that supports its financial management systems does not take into account the complex needs of individual systems. It also does not account for ensuring that each system has the appropriate mix of government and contract skills needed for developing and maintaining them. As a result, while individual staff in specific lines of work may have training they need to be successful, the financial systems risk not having the right mix of staff and skills needed to be successful.

---

## Recommendations for Executive Action

We are making the following nine recommendations to the Department of Defense:

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 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)

The Secretary of Defense should direct the DOD CIO and USD(C)/CFO 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)

---

## Agency Comments and Our Evaluation

We provided a draft of this report to DOD for review and comment. We received written comments from DOD that are reprinted in appendix III and summarized below.

In its comments, the department concurred with seven of our nine recommendations and partially concurred with two recommendations. Specifically, DOD concurred with our recommendations that DOD and the military departments update guidance for business and financial systems to ensure that it fully addresses the statutory requirements discussed in this report (recommendations 1, 2, 3, 4, and 5). DOD stated that it will focus on efforts to enhance guidance for initial approvals and annual certifications of business systems.

DOD also concurred with the recommendations to improve the data it maintains about business and financial system certifications and to

develop and implement plans for documenting detailed system compliance with business enterprise architecture (recommendations 7 and 8). DOD stated that it will improve data collection reliability related to business and financial system compliance with statutory requirements. As discussed below, DOD partially concurred with the two remaining recommendations.

- For our recommendation calling for DOD to develop guidance related to statutory requirements for systems in sustainment, DOD stated that as its CIO examines its modernization activities, it will conduct an analysis on the potential need to develop additional, supplemental guidance for systems in sustainment. Based upon the department's completed analysis, DOD stated that its CIO will then determine whether to implement the recommendation. DOD also stated that its CIO will continue to review its systems architectures, code, infrastructure, processes, to reduce the tailoring of commercial off-the-shelf systems.

By not fully committing to developing needed guidance, DOD is likely missing important opportunities for improving its systems that are in sustainment. More specifically, without fully implementing statutory requirements such as limiting the customization of commercial off-the-shelf systems, the department is constraining its efforts to achieve a more streamlined and efficient system environment. This in turn will further delay reaching the goal of a clean audit opinion. Consequently, we maintain that our recommendation is appropriate.

- Regarding our recommendation on DOD taking a strategic approach to workforce planning, DOD reiterated that functional community (i.e., acquisition, financial management, and cyber-excepted workforce) oversight provides strategic workforce plans, strategic certification, and training requirements for each of these professional series. DOD also noted that these and additional staff assist independent auditors in gathering and reviewing the defense business systems within the department, including for the annual audits of the components and defense entities. We acknowledge DOD has existing workforce planning and oversight activities underway, as described in our report. However, DOD does not take a strategic approach to the collective set of staff needed to support its financial management systems.

Until DOD takes a strategic approach to its financial management systems workforce, DOD and the military departments will likely not have sufficient information to understand gaps between existing and needed skills and capabilities. Without such an understanding, the department further risks its efforts to develop and maintain systems

---

**Letter**

---

that can help achieve an unmodified audit opinion. As a result, we maintain that our recommendation is appropriate.

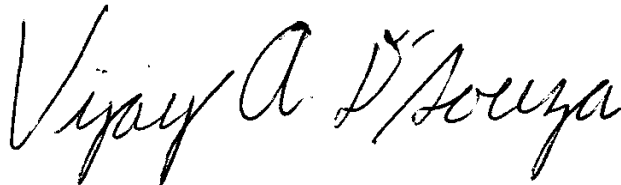
---

We are sending copies of this report to the appropriate congressional committees; the Secretary of Defense; the Secretaries of the Army, Navy, and Air Force; the Under Secretary of Defense (Comptroller)/Chief Financial Officer; the DOD Chief Information Officer; and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact Kevin Walsh at (202) 512-6151 or [walshk@gao.gov](mailto:walshk@gao.gov) or Vijay A. D'Souza at (202) 512-7650 or [dsouzav@gao.gov](mailto:dsouzav@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.



Kevin Walsh  
Director, Information Technology and Cybersecurity



Vijay A. D'Souza  
Director, Information Technology and Cybersecurity

---

*List of Requesters*

The Honorable Charles E. Grassley  
Ranking Member  
Committee on the Budget  
United States Senate

The Honorable Bernard Sanders  
United States Senate

The Honorable Ron Wyden  
United States Senate

## Appendix I: Objectives, Scope and Methodology

Our objectives for this review were to (1) describe the Department of Defense's (DOD) efforts to improve its business and financial systems; (2) assess the extent to which DOD is effectively overseeing its business and financial systems; and (3) assess the extent to which DOD is taking a strategic approach to managing human capital needed for developing and maintaining its financial management systems.

To address the first objective, we reviewed related laws, GAO reports, and DOD and military department documentation associated with DOD's business and financial systems. For example, we reviewed and summarized relevant laws, such as the National Defense Authorization Acts for Fiscal Year 1994 and 2008. In addition, we obtained and reviewed documentation such as DOD's September 2021 memorandum that detailed DOD's efforts to reorganize former Chief Management Officer (CMO) responsibilities throughout the department and its June 2018 Investment Management and Certification guidance.<sup>1</sup> We also reviewed relevant information contained in related GAO reports.<sup>2</sup>

To address the second objective, we reviewed prior GAO reports and guidance and relevant statutes to identify key elements of business and

---

<sup>1</sup>DOD, *Disestablishment of the Chief Management Officer, Realignment of Functions and Responsibilities, and Related Issues* (Washington, D.C.: Sept. 1, 2021); DOD, *Office of the Deputy Chief Management Officer, Defense Business Systems Investment Management Guidance, Version 4.1* (Jun.26, 2018).

<sup>2</sup>See, for example, GAO, *DOD Business Systems Modernization: Additional Action Needed to Achieve Intended Outcomes*, [GAO-15-627](#) (Washington, D.C.: July 16, 2015); *Defense Business Systems: Further Refinements Needed to Guide the Investment Management Process*, [GAO-14-486](#) (Washington, D.C. May 12, 2014); *DOD Business Systems Modernization: Further Actions Needed to Address Challenges and Improve Accountability*, [GAO-13-557](#) (Washington, D.C.: May 17, 2013); and *DOD Business Systems Modernization: Governance Mechanisms for Implementing Management Controls Need to Be Improved*, [GAO-12-685](#) (Washington, D.C.: June 1, 2012).

financial management systems oversight.<sup>3</sup> In doing so, we identified establishing oversight processes, using and communicating quality information, sustaining leadership commitment, and managing risk.

For establishing oversight processes, we reviewed documentation from DOD and the military departments associated with their oversight of business and financial management systems. For example, we reviewed documentation such as the January 2020 *DOD Instruction 5000.75, Business Systems Requirements and Acquisitions* and DOD's June 2018 *Investment Management and Certification Guidance*.<sup>4</sup> In addition, we reviewed related guidance established by the Departments of the Air Force, the Army, and the DON for certifying and approving their business and financial systems. We also met with DOD and military department officials to discuss relevant oversight processes.

Based on those discussions and documentation, we focused on DOD's initial approval and annual certification of business and financial systems discussed in 10 U.S.C. § 2222. We chose this oversight process because of its long-standing association with DOD's efforts to achieve a clean audit opinion. We focused broadly on DOD's business and financial systems because, collectively, this environment includes systems associated with compiling and reporting financial information, as well as systems that provide information to those core systems.

We evaluated DOD and military department guidance for initial approvals and annual certifications of business and financial systems. These approvals and certifications are associated with the requirements outlined in 10 U.S.C. § 2222. This statute requires that the Secretary of Defense ensure that a covered defense business system not proceed into

---

<sup>3</sup>GAO, *Defense Management: Opportunities Exist to Improve DOD's Reform Efforts*, [GAO-21-532T](#). (Washington, D.C., April 27, 2021); *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014). *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0)*, [GAO-10-846G](#) (Washington, D.C., August 5, 2010); *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, [GAO-04-394G](#) (Washington, D.C., March 1, 2004); *Business Process Reengineering Assessment Guide--Version 3*, [AIMD-10.1.15](#). (Washington, D.C., April 1, 1997); *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, [GAO-04-394G](#) (Washington, D.C., March 1, 2004); and Pub. L. No. 108-375, § 332, 118 Stat. at 1851 (2004), as amended in pertinent part by Pub. L. No. 114-92, § 883(a), 129 Stat. at 942 (2015).

<sup>4</sup>DOD, *DOD Instruction 5000.75: Business Systems Requirements and Acquisition* (Jan. 24, 2020) and DOD, *Office of the Deputy Chief Management Officer, Defense Business Systems Investment Management Guidance, Version 4.1* (Jun.26, 2018).



development (or, if no development is required, into production or fielding) unless the appropriate approval official determines that the system meets five requirements. In addition, for any fiscal year in which funds are expended for development or sustainment pursuant to a covered defense business or financial system, the appropriate approval official is to review the system to determine if the system

- has been, or is being, reengineered to be as streamlined and efficient as practicable, and whether the implementation of the system will maximize the elimination of unique software requirements and unique interfaces;
- is in compliance with the business enterprise architecture or will be in compliance as a result of planned modifications;
- has valid, achievable requirements, and a viable plan for implementing those requirements (including, as appropriate, market research, business process reengineering, and prototyping activities);
- has an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable; and
- is in compliance with the department's auditability requirements.

In addition, 10 U.S.C. § 2222 calls for systems that plan to spend between \$50 million and \$250 million over the Future-Years Defense Program (FYDP) to have their initial approvals and annual certifications approved by the CMO of their respective military department.<sup>5</sup> Further, according to the code and DOD guidance, the Undersecretary of Defense (Comptroller)/Chief Financial Officer (USD(C)/CFO) and DOD CIO are the approval authorities for systems that exist within a Defense Agency, field activity, or support more than one portion of DOD. The code also states that, among other things, the CMO of each of the military departments is to issue and maintain supporting guidance, as appropriate, within their respective areas of responsibility.

We reviewed DOD guidance to determine the extent to which the guidance described how covered systems are to assert and document compliance with the requirements and how decision-makers are to

---

<sup>5</sup>The future-years defense program is to be submitted to Congress by the Secretary of Defense each year, at or about the time that the President's budget is submitted to Congress. It is to reflect the estimated expenditures and proposed appropriations included in the DOD budget, and cover the budget-submission fiscal year and at least the four succeeding fiscal years. Further, systems that plan to spend over \$250 million over the course of the future-years defense program are referred to as priority business systems. DOD can also designate systems additional as priority.

substantiate compliance. In addition, we compared the guidance established by the Departments of the Air Force, Army, and Navy for approving and certifying their business and financial systems with the five requirements described in the code. In evaluating the guidance, we determined that the guidance fully addressed the legislative requirements if it explained how systems are to address and decision-makers are to substantiate this requirement; partially addressed the requirements if the guidance discussed the requirement, but did not fully describe how systems are to address the requirement and decision-makers are to substantiate; and not addressed if the guidance did not discuss the requirement.

For quality information, we reviewed the data DOD collects and reports about its business systems certifications and its efforts to document detailed business enterprise architecture compliance. To conduct our assessment, we evaluated DOD's data on system compliance with statutory requirements. Specifically, we reviewed data from two of the department's authoritative data sources—the Defense Information Technology Investment Portal (DITIP) and Financial Improvement and Audit Readiness (FIAR) Systems Database. DITIP is DOD's authoritative data source for its business system certification process, including information on system assertions of compliance to the requirements described in 10 U.S.C § 2222. The FIAR Systems Database documents, among other things, DOD's list of significant financial and feeder systems. We obtained DITIP data as of August 2021 and we obtained FIAR Systems Database data as of May 2021.<sup>6</sup> We reviewed and summarized certification compliance data in DITIP for business and financial systems relative to the five statutory requirements from 10 U.S.C. § 2222.

To assess the reliability of the data in DITIP, we first reviewed the DITIP data for obvious errors or omissions. For example, we performed data searches to look for cells that did not contain data or contained data that were inconsistent. We also reviewed the data to identify potentially duplicative data. In addition, we reviewed data reliability questionnaires completed by relevant DOD officials to identify potential issues with the data or determine reasons for any issues we found in our review of the data. We also compared the list of systems in DITIP that indicated that compliance to the auditability requirement was not applicable to the list of systems in the FIAR Systems Database. In doing so, we identified

---

<sup>6</sup>DOD provided DITIP data for systems that it identified as being relevant to the annual financial audit.

systems that DOD identified as relevant to the audit that indicated in DITIP that the auditability requirement was not applicable. Further, we interviewed officials from the Office of the Under Secretary for Defense (Comptroller) and Office of the DOD CIO to discuss the accuracy and comprehensiveness of information contained in DITIP, the discrepancies between the information contained in DITIP and the FIAR Systems Database, and efforts under way or planned to address these discrepancies. As discussed in this report, we determined that the data we obtained from DITIP was not fully reliable. We also evaluated DOD's efforts to collect detailed information on business enterprise architecture compliance by comparing DOD guidance to DOD's current practices and plans for collecting such data.

We also interviewed officials responsible for overseeing defense business and financial system investments at DOD and the military departments. Specifically, we interviewed officials in the Office of the Under Secretary for Defense (Comptroller), the Office of the CIO and the Departments of the Air Force, Army, and Navy. We did not interview Marine Corps officials about Marine Corps oversight because Marine Corps systems are included in the DON portfolio as part of this oversight mechanism. As a result, DON guidance and processes applies to the Marine Corps systems.

For sustained leadership commitment and managing risks, we reviewed information from recent GAO reports.<sup>7</sup> We also selected a random non-generalizable sample of eight financial management systems from both the military departments and defense agencies. To make this selection, we used data from DOD's Financial Improvement and Audit Readiness (FIAR) Systems Database and the Federal IT Dashboard.<sup>8</sup> We used the data from the federal IT dashboard to develop a list of DOD IT systems. We then compared this list to the data in DOD's FIAR Systems Database to identify the systems that DOD had identified as being relevant to the

---

<sup>7</sup>See GAO, *Business Systems: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning*, [GAO-22-105330](#) (Washington, D.C., June 14, 2022) and *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, [GAO-21-119SP](#) (Washington, D.C.: Mar. 2, 2021).

<sup>8</sup>DOD's FIAR System Database contains DOD's list of significant financial and feeder systems. We obtained data as of May 2021. The Federal IT Dashboard is a public, federal government website previously operated by the Office of Management and Budget and currently operated by the General Services Administration at <https://itdashboard.gov>. The dashboard includes information on major IT investments across the federal government, including DOD investments.

audit (referred to in this report as “financial management systems”).<sup>9</sup> Because we used this data to identify a non-generalizable sample of systems, we did not evaluate the reliability of the data contained in the federal IT dashboard or the FIAR systems database. We subsequently used a random number generator to select one major financial management system and one non-major financial management system from each of the military departments.<sup>10</sup> We also selected one major and one non-major financial management system from the set of systems managed by defense agencies. The eight systems we selected are identified in Table 10 below.

**Table 10: Eight Selected Financial Management Systems Managed by Military Department and Defense Agencies**

System name	System Owner	System Type (major)	System Type (non-major)
Enterprise Business System	Defense Logistics Agency	x	not applicable

<sup>9</sup>Financial management systems refer to the business and financial systems that support audit-related activities. According to the Federal Financial Management Improvement Act of 1996, financial management systems are the financial systems and the financial portions of mixed systems necessary to support financial management, including automated and manual processes, procedures, controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions. A financial system is an information system, comprised of one or more applications that is used for collecting, processing, maintaining, transmitting, or reporting data about financial events; supporting financial planning or budgeting activities; accumulating and reporting costs information; or supporting the preparation of financial statements. A mixed system is an information system that supports both financial and nonfinancial functions. The Department of Defense Financial Management Regulation refers to some mixed systems as feeder systems. The regulation defines feeder systems as the manual or automated programs, procedures and processes which develop data required to initiate an accounting or financial transaction but do not perform an accounting operation, such as personnel, property, or logistics systems.

<sup>10</sup>According to officials from the office of the DOD Chief Information Officer (CIO) and DOD guidance, the department’s major IT investments include: (1) major determined to be IT investments by the DOD CIO; (2) IT programs with a budget greater than \$43 million for fiscal year (FY) 2022 or greater than \$569.2 million greater across the future-years defense plan (defined subsequently in this appendix); and (3) IT investments designated as major by department leadership. DOD, *FY 2023 Information Technology/Cyberspace Activities Budget Guidance* (Washington, D.C.: July 15, 2021). As discussed in [GAO-22-105330](#), DOD officials stated that the FY23 Guidance reflected the latest guidelines applied to the FY22 list of major IT investments. DOD officials added that this definition of a “major” IT investment was not reflected in the FY22 guidance because it was implemented after the guidance was released. Non-major IT investments are investments that are not designated as major. See GAO, *Business Systems: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning*, [GAO-22-105330](#) (Washington, D.C.: June 14, 2022).

**Appendix I: Objectives, Scope and Methodology**

<b>System name</b>	<b>System Owner</b>	<b>System Type (major)</b>	<b>System Type (non-major)</b>
Defense Enterprise Accounting and Management System	Air Force	x	not applicable
General Fund Enterprise Business System	Army	x	not applicable
Navy Standard Integrated Personnel System	Navy	x	not applicable
Defense Military Pay Office	Defense Finance and Accounting Service	not applicable	x
Financial Inventory Accounting and Billing System	Air Force	not applicable	x
Rock Island Arsenal Joint Manufacturing Technology Center Automated Storage and Retrieval System	Army	not applicable	x
Decision Knowledge Programming for Logistics Analysis and Technical Evaluation	Navy	not applicable	x

Legend: A dash (“-”) indicates that the system designation is not applicable.

Source: GAO analysis of Department of Defense (DOD) data. | GAO-23-104539

We then conducted interviews with military department and defense agency officials responsible for the eight systems we selected. We used these interviews to gain an understanding of officials’ perspectives on, among other things, challenges related to governing and managing DOD financial management systems.

In addition, we met with officials with oversight responsibilities associated with DOD business and financial systems. Specifically, we met with officials from the offices of the Under Secretary of Defense (Comptroller), the Chief Information Officer (CIO), and officials from the Department of the Air Force, Department of the Army, and Department of the Navy (DON). We reviewed and summarized these interviews and associated written responses to develop a list of challenges related to modernizing the department’s business and financial management systems environment. The list of challenges is not intended to be comprehensive; rather, it reflects a summary of challenges cited by DOD staff.

To address the third objective, we assessed DOD and the military department’s approach for determining the government and contractor human capital skills needed to develop and maintain its financial

management systems against GAO's guidance that identifies the following key practices on effective strategic workforce planning:<sup>11</sup>

- assess the knowledge and skills needed to execute a program;
- inventory the knowledge and skills of existing staff;
- forecast the knowledge and skills needed over time;
- analyze the gaps in capabilities between the existing staff and future workforce needs, including consideration of evolving program and succession needs caused by turnover and retirement; and
- formulate strategies for filling expected gaps.

We reviewed human capital strategies and plans supporting department and military department financial management systems, including, among other things, the *Department of Defense's Financial Management Strategy for FY 2022-2026*, the *Department of the Air Force's Financial Management Strategic Plan for FY 2022-2026*, *Navy's Command Implementation Guidance: Navy Enterprise Resource Planning Program V 3.0*, and the *Army Finance Strategy 2026*.<sup>12</sup> We compared these strategies and plans to GAO's key practices for strategic workforce planning. We also reviewed and summarized workforce related challenges documented in interviews with system officials representing the eight systems we selected for review as part of our non-generalizable sample. In addition, we also interviewed cognizant officials from the Office of the Under Secretary of Defense (Comptroller), the Office of the CIO and the Departments of Air Force, Army and Navy about their respective workforce planning strategies and plans. In addition, we reviewed recent GAO reports to identify previously-reported workforce issues associated with DOD business and financial systems.<sup>13</sup>

---

<sup>11</sup>See GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, [GAO-04-39](#) (Washington, D.C.: Dec. 11, 2003). Also see GAO, *Joint Information Environment: DOD Needs to Strengthen Governance and Management*, [GAO-16-593](#) (Washington, D.C.: Oct. 25, 2016); and *DOD Business Systems Modernization: Further Actions Needed to Address Challenges and Improve Accountability*, [GAO-13-557](#) (Washington, D.C.: May 17, 2013).

<sup>12</sup>Department of Defense, *Financial Management Strategy for Fiscal Years 2022-2026*; Department of the Air Force, *Financial Management Strategic Plan for Fiscal Years 2022-2026*; Department of the Navy, *Command Implementation Guidance: Navy Enterprise Resource Planning Program V 3.0* (Aug. 10, 2010); and Department of the Army, *Army Finance Strategy 2026* (November 2020).

<sup>13</sup>See, for example, GAO, *Software Development: DOD Faces Risks and Challenges in Implementing Modern Approaches and Addressing Cybersecurity Practices*, [GAO-21-351](#) (Washington, D.C.: June 23, 2021).

---

**Appendix I: Objectives, Scope and  
Methodology**

---

We conducted this performance audit from October 2020 to February 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Appendix II: Evaluation of DOD Guidance for Business and Financial System Initial Approvals and Annual Certifications

Tables 11 through 20 describe our assessments of the extent to which the Department of Defense (DOD) and military department guidance addresses initial certification and annual certification requirements for defense business systems covered under 10 U.S.C. § 2222. The guidance distinguishes between systems that plan to spend more than \$250 million over the course of the future-years defense program and systems with lower levels of planned expenditures. In addition, the guidance expands the lower threshold for systems subject to these requirements below the \$50 million threshold called for in 10 U.S.C. § 2222.

**Table 11: Assessment of DOD Guidance for Initial Approval Requirements for Systems That Plan to Spend More Than \$250 Million over the Future-Years Defense Program (FYDP)**

Initial Approval Requirement	Extent to Which the Guidance Addresses the Requirement	Assessment Summary
Business process reengineering and maximizing the elimination of unique software requirements and interfaces	partially addressed	<p>DOD Instruction 5000.75 does not describe how systems are to substantiate compliance with the requirement at initial approval.</p> <p>The department's June 2018 investment management guidance states that systems must comply with the department's business process reengineering requirements and that systems seeking initial approvals should submit documents used as part of the acquisition authority to proceed phase documented in DOD instruction 5000.75. However, it does not specify how those documents are to be used to document or substantiate compliance with the business process reengineering requirement. In addition, the guidance does not indicate what the department's business process reengineering requirements include.</p>



**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

<b>Initial Approval Requirement</b>	<b>Extent to Which the Guidance Addresses the Requirement</b>	<b>Assessment Summary</b>
Compliance or planned compliance with the business enterprise architecture	partially addressed	DOD Instruction 5000.75 indicates that a system is to demonstrate alignment and submission to the business enterprise architecture as a consideration at the solutions analysis authority-to-proceed decision point. However, it does not specify how systems are to substantiate compliance with the requirement.  The department's June 2018 investment management guidance states that systems must comply with the department's business enterprise architecture requirements and that systems seeking initial approvals should submit documents used as part of the acquisition authority-to-proceed phase documented in DOD instruction 5000.75. However, it does not specify how those documents are to be used to document or substantiate compliance with the business enterprise architecture. In addition, the guidance does not indicate what the department's business enterprise architecture requirements include.
Valid, achievable requirements and a viable plan for implementing those requirements	partially addressed	DOD Instruction 5000.75 does not describe how systems are to substantiate or how approval authorities are to validate compliance with the requirement for initial approval.  The department's June 2018 investment management guidance states that systems seeking initial approvals should submit documents used as part of the acquisition authority-to-proceed phase documented in DOD instruction 5000.75 and that systems must demonstrate compliance with 10 U.S.C. § 2222. However, it does not specify how those documents are to be used to document or substantiate compliance with the requirement that systems have valid, achievable requirements, and a plan for implementing those requirements. Moreover, the guidance does not indicate what the department requires for a system to have valid, achievable requirements and a plan for implementing those requirements.
An acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems	partially addressed	DOD Instruction 5000.75 does not describe how systems are to substantiate compliance or how approval authorities are to validate compliance with the requirement at initial approval.  The department's June 2018 investment management guidance states that systems must comply with the department's acquisition strategy requirement. It also states that systems seeking initial approvals should submit documents used as part of the acquisition authority-to-proceed phase documented in DOD instruction 5000.75. However, it does not specify how those documents are to be used to document or substantiate compliance with the requirement that systems have a documented acquisition strategy that meets statutory requirements. Moreover, the guidance does not indicate what the department's requirements for a system to have an acquisition strategy include.
Compliance with the Department's auditability requirements	partially addressed	DOD Instruction 5000.75 does not describe how systems are to substantiate compliance or how approval authorities are to validate compliance with the requirement at initial approval.  The department's June 2018 investment management guidance states that systems seeking initial approvals should submit documents used as part of the acquisition authority-to-proceed phase documented in DOD instruction 5000.75 and that systems should demonstrate compliance with 10 U.S.C. § 2222. However, it does not specify how those documents are to be used to substantiate compliance with the department's auditability requirements. Moreover, the guidance does not indicate what the department's auditability requirements include.

**Legend:**

- Fully addressed: Guidance explains how systems are to address and decision-makers are to substantiate this requirement.
- ⓘ Partially addressed: Guidance discusses the requirement, but does not fully describe how systems are to address and decision-makers are to substantiate this requirement.
- Not addressed: Guidance does not discuss this requirement.

Source: GAO Analysis of Department of Defense (DOD) Guidance. | GAO-23-104539

**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

**Table 12: Assessment of DOD Guidance for Annual Certification Requirements for Systems That Plan to Spend More Than \$250 Million over the Future-Years Defense Program (FYDP)**

<b>Annual Certification Requirement</b>	<b>Extent to Which the Guidance Addresses the Requirement</b>	<b>Assessment Summary</b>
Business process reengineering and maximizing the elimination of unique software requirements and interfaces	partially addressed	The department's June 2018 Defense Business Systems Investment Management Guidance, Version 4.1 requires that, systems are to assert compliance with the requirements of 10 U.S.C. § 2222, including the business process reengineering requirement. Further, the guidance requires that assertions for compliance be documented within the Defense IT Investment Portal (DITIP). However, the guidance does not describe how systems are to substantiate or how approval authorities are to validate compliance with the requirement.
Compliance or planned compliance with the business enterprise architecture	partially addressed	The department's June 2018 Investment Management Guidance requires that the organization must ensure that defense business systems are compliant with all applicable business enterprise architecture regulations, policy, data standards, and business rules. Further, the guidance states that organizations must perform business enterprise architecture assessments in the Integrated Business Framework-Data Alignment Portal and must assert compliance in DITIP to ensure business enterprise architecture assessments are consistent and rigorous. However, the guidance does not describe how systems are to substantiate or how approval authorities are to validate compliance with the requirement. In addition, DOD is no longer using the Integrated Business Framework-Data Alignment Portal tool.
Valid, achievable requirements and a viable plan for implementing those requirements	partially addressed	The department's June 2018 Investment Management Guidance states systems must certify that they have valid, achievable requirements and a viable plan for implementing those requirements. Further, the guidance requires that assertions for compliance be documented within DITIP. However, the guidance does not describe how systems are to substantiate or how approval authorities are to validate compliance with the requirement.
An acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems	partially addressed	The department's June 2018 Investment Management Guidance states systems are to assert compliance with the requirements that they have an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems. Further, the guidance requires that assertions for compliance be documented within DITIP. However, the guidance does not describe how systems are to substantiate or how approval authorities are to validate compliance with the requirement.
Compliance with the Department's auditability requirements	partially addressed	The department's June 2018 Investment Management Guidance states that systems are to assert compliance with the requirement that the system complies with the department's auditability requirements. Further, according to the guidance, compliance assertions should be documented in DITIP. However, the guidance does not describe how systems are to substantiate or how approval authorities are to validate compliance with the requirement.

**Legend:**

- Fully addressed: Guidance explains how systems are to address and decision-makers are to substantiate this requirement.
- ⦿ Partially addressed: Guidance discusses the requirement, but does not fully describe how systems are to address and decision-makers are to substantiate this requirement.
- Not addressed: Guidance does not discuss this requirement.

Source: GAO Analysis of Department of Defense (DOD) Guidance. | GAO-23-104539

**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

**Table 13: Assessment of DOD Guidance for Initial Approval Requirements for Defense Agency Systems that Plan to Spend Between \$25 Million and \$250 Million over the Future-Years Defense Program (FYDP)**

Initial Approval Requirement	Extent to Which the Guidance Addresses the Requirement	Assessment Summary
Business process reengineering and maximizing the elimination of unique software requirements and interfaces	partially addressed	<p>DOD Instruction 5000.75 does not describe how systems are to substantiate compliance with the requirement at initial approval.</p> <p>The department's June 2018 investment management guidance states that systems must comply with the department's business process reengineering requirements and that systems seeking initial approvals should submit documents used as part of the acquisition authority to proceed phase documented in DOD instruction 5000.75. However, it does not specify how those documents are to be used to document or substantiate compliance with the business process reengineering requirement. In addition, the guidance does not indicate what the department's business process reengineering requirements include.</p>
Compliance or planned compliance with the business enterprise architecture	partially addressed	<p>DOD Instruction 5000.75 indicates that a system is to demonstrate alignment and submission to the business enterprise architecture as a consideration at the solutions analysis authority-to-proceed decision point. However, it does not specify how systems are to substantiate compliance with the requirement.</p> <p>The department's June 2018 investment management guidance states that systems must comply with the department's business enterprise architecture requirements and that systems seeking initial approvals should submit documents used as part of the acquisition authority-to-proceed phase documented in DOD instruction 5000.75. However, it does not specify how those documents are to be used to document or substantiate compliance with the business enterprise architecture. In addition, the guidance does not indicate what the department's business enterprise architecture requirements include.</p>
Valid, achievable requirements and a viable plan for implementing those requirements	partially addressed	<p>DOD Instruction 5000.75 does not describe how systems are to substantiate or how approval authorities are to validate compliance with the requirement for initial approval.</p> <p>The department's June 2018 investment management guidance states that systems seeking initial approvals should submit documents used as part of the acquisition authority-to-proceed phase documented in DOD instruction 5000.75 and that systems must demonstrate compliance with 10 U.S.C. § 2222. However, it does not specify how those documents are to be used to document or substantiate compliance with the requirement that systems have valid, achievable requirements, and a plan for implementing those requirements. Moreover, the guidance does not indicate what the department requires for a system to have valid, achievable requirements and a plan for implementing those requirements.</p>
An acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems	partially addressed	<p>DOD Instruction 5000.75 does not describe how systems are to substantiate or how approval authorities are to validate compliance with the requirement at initial approval.</p> <p>The department's June 2018 investment management guidance states that systems must comply with the department's acquisition strategy requirement. It also states that systems seeking initial approvals should submit documents used as part of the acquisition authority-to-proceed phase documented in DOD instruction 5000.75. However, the guidance does not specify how those documents are to be used to document or substantiate compliance with the requirement that systems have a documented acquisition strategy that meets statutory requirements. Moreover, the guidance does not indicate what the department's requirements for a system to have an acquisition strategy include.</p>

**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

<b>Initial Approval Requirement</b>	<b>Extent to Which the Guidance Addresses the Requirement</b>	<b>Assessment Summary</b>
Compliance with the Department's auditability requirements	partially addressed	DOD Instruction 5000.75 does not describe how systems are to substantiate or how approval authorities are to validate compliance with the requirement at initial approval. The department's June 2018 investment management guidance states that systems seeking initial approvals should submit documents used as part of the acquisition authority-to-proceed phase documented in DOD instruction 5000.75 and that systems should demonstrate compliance with 10 U.S.C. § 2222. However, it does not specify how those documents are to be used to substantiate compliance with the department's auditability requirements. Moreover, the guidance does not indicate what the department's auditability requirements include.

Legend:

- Fully addressed: Guidance explains how systems are to address and decision-makers are to substantiate this requirement.
- ⦿ Partially addressed: Guidance discusses the requirement, but does not fully describe how systems are to address and decision-makers are to substantiate this requirement.
- Not addressed: Guidance does not discuss this requirement.

Source: GAO Analysis of Department of Defense (DOD) Guidance. | GAO-23-104539

**Table 14: Assessment of DOD Guidance for Annual Certification Requirements for Defense Agency Systems That Plan to Spend between \$25 Million and \$250 Million over the Future-Years Defense Program (FYDP)**

<b>Annual Certification Requirement</b>	<b>Extent to Which the Guidance Addresses the Requirement</b>	<b>Assessment Summary</b>
Business process reengineering and maximizing the elimination of unique software requirements and interfaces	partially addressed	The department's June 2018 Defense Business Systems Investment Management Guidance requires that, systems are to assert compliance with the requirements of 10 U.S.C. § 2222, including the business process reengineering requirement. Further, the guidance requires that assertions for compliance be documented within the Defense IT Investment Portal (DITIP). However, the guidance does not describe how systems are to substantiate or how approval authorities are to validate compliance with the requirement that a system has conducted business process reengineering and maximized the elimination of unique software requirements and interfaces.
Compliance or planned compliance with the business enterprise architecture	partially addressed	The department's June 2018 Defense Business Systems Investment Management Guidance requires that the organization must ensure that defense business systems are compliant with all applicable business enterprise architecture regulations, policy, data standards, and business rules. Further, the guidance states that organizations must perform business enterprise architecture assessments in the Integrated Business Framework-Data Alignment Portal and must assert compliance in DITIP to ensure business enterprise architecture assessments are consistent and rigorous. However, the guidance does not describe how programs are to substantiate or how approval authorities are to validate compliance with the requirement. In addition, DOD is no longer using the Integrated Business Framework-Data Alignment Portal.
Valid, achievable requirements and a viable plan for implementing those requirements	partially addressed	The department's June 2018 Investment Management Guidance states programs must certify that they have a valid, achievable requirements and a viable plan for implementing those requirements. Further, the guidance requires that assertions for compliance be documented within DITIP. However, the guidance does not describe how programs are to substantiate or how approval authorities are to validate compliance with the requirement.

**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

<b>Annual Certification Requirement</b>	<b>Extent to Which the Guidance Addresses the Requirement</b>	<b>Assessment Summary</b>
An acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems	partially addressed	The department's June 2018 Investment Management Guidance states systems are to assert compliance with the requirements that they have an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems. Further, the guidance requires that assertions for compliance be documented within DITIP. However, the guidance does not describe how systems are to substantiate or how approval authorities are to validate compliance with the requirement.
Compliance with the Department's auditability requirements	partially addressed	The department's June 2018 Investment Management Guidance states that systems are to assert compliance with the requirement that the system complies with the department's auditability requirements. Further, according to the guidance, compliance assertions should be documented in DITIP. However, the guidance does not describe how systems are to substantiate or how approval authorities are to validate compliance with the requirement.

Legend:

- Fully addressed: Guidance explains how systems are to address and decision-makers are to substantiate this requirement.
- ⓘ Partially addressed: Guidance discusses the requirement, but does not fully describe how systems are to address and decision-makers are to substantiate this requirement.
- Not addressed: Guidance does not discuss this requirement.

Source: GAO Analysis of Department of Defense (DOD) Guidance. | GAO-23-104539

**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

**Table 15: Assessment of Air Force Guidance for Initial Approval Requirements for Systems That Plan to Spend between \$1 Million and \$250 Million over the Future-Years Defense Program (FYDP)**

Initial Approval Requirement	Extent to Which the Guidance Addresses the Requirement	Assessment Summary
Business process reengineering and maximizing the elimination of unique software requirements and interfaces	partially addressed	<p>The Air Force’s July 2018 guidance on Business Capability Requirements, Compliance, and System Acquisition states that Air Force updated the guidance, in part, to address the requirements of 10 U.S.C. § 2222. The guidance states, among other things, that thorough business process reengineering should be conducted during the business system functional requirements and acquisition planning phase to identify the IT functional requirements that drive the acquisition and deployment of a business system. However, it does not describe how systems are to document business process reengineering prior to proceeding into development. Moreover, it does not discuss how systems are to document or how approval authorities are to validate compliance with business process reengineering or that the system has maximized the elimination of unique software requirements before a system proceeds into development. According to an Air Force official, all required functional requirements and acquisition planning documents are provided to the milestone decision authority for review and approval to proceed into acquisition. Further, this official stated that all phase and milestone activities are also reviewed and approved by entities such as the business mission area council prior to milestone decision authority decisions. However, the Air Force did not substantiate that this approval and validation process is documented in the guidance cited in this assessment.</p> <p>Air Force officials also provided a November 2021 business process reengineering form. This form discusses eliminating or reducing the need for unique requirements or interfaces. In addition, the Air Force issued a December 2021 business process reengineering study aid to assist programs and functional portfolios in preparing responses to the questions in the business process reengineering form. This study aid contains sample answers to each question in the business process reengineering form for programs in development to utilize in completing their forms. However, the business process reengineering form and study aid do not specify which portions of the form are required to be completed at which development phase or how the form is to be evaluated. In addition, the Air Force’s Fiscal Year (FY) 2022 annual certification guidance does not discuss initial approval of systems before they proceed into development.</p>
Compliance or planned compliance with the business enterprise architecture	partially addressed	<p>The Air Force’s June 2018 Business Capability Acquisition Cycle Body of Knowledge: Capability Requirements Document Framework recommends that systems begin to align their business capabilities with the current DOD business enterprise architecture or their functional area’s enterprise architecture before proceeding into development. However, it does not call for systems to assert compliance or planned compliance with the business enterprise architecture prior to proceeding into development. For example, the framework does not specifically call for systems to comply with the architecture and does not describe the validation process. According to an Air Force official, all required functional requirements and acquisition planning documents are provided to the milestone decision authority prior to acquisition. However, this process is not documented in the Air Force’s June 2018 framework. In addition, the framework does not discuss initial approval of systems before they proceed into development. Further, the Air Force’s FY 2022 annual certification guidance does not discuss initial approval of programs before they proceed into development.</p>

**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

Initial Approval Requirement	Extent to Which the Guidance Addresses the Requirement	Assessment Summary
Valid, achievable requirements and a viable plan for implementing those requirements	partially addressed	The Air Force's July 2018 guidance on Business Capability Requirements, Compliance, and System Acquisition states that it was updated, in part, to address the requirements of 10 U.S.C. § 2222. The guidance states that, among other things, as part of the business system functional requirements and acquisition planning phase, systems are to update their implementation plan to include all necessary requirements. According to Air Force officials, systems are also required to provide a project plan via a capabilities implementation plan for implementing their requirements as part of obtaining authority to proceed to solutions analysis. However, the guidance does not discuss how systems are to assert or how approval authorities are to validate that a system has valid, achievable requirements and a viable plan for implementing those requirements before the system proceeds into development. In addition, the Air Force's FY 2022 annual certification guidance does not discuss initial approval of systems before they proceed into development.
An acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems	partially addressed	The Air Force's July 2018 guidance on Business Capability Requirements, Compliance, and System Acquisition states that it was updated, in part, to address the requirements of 10 U.S.C. § 2222. The guidance states that, among other things, as part of the business system acquisition, testing, and deployment phase, systems are to minimize modifications to the commercial off-the-shelf systems. In addition, the draft Department of the Air Force Instruction 63-144 provides additional guidance on minimizing customization. However, the July 2018 guidance and the draft instruction do not call for systems to develop an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems prior to proceeding into development. According to an Air Force official, all required documents are provided to the milestone decision authority for review and approval to proceed to development. In addition, this official stated that phase and milestone activities are also reviewed and approved by entities such as the business mission area council. However, this process is not documented in the July 2018 guidance or the draft instruction. In addition, the Air Force's FY 2022 annual certification guidance does not discuss initial approval of systems before they proceed into development.
Compliance with the Department's auditability requirements	partially addressed	The Air Force's July 2018 guidance on Business Capability Requirements, Compliance, and System Acquisition states that it was updated, in part, to address the requirements of 10 U.S.C. § 2222. The guidance states that systems should work with appropriate organizations and subject matter experts to prepare content for review at authority-to-proceed decision points, such as coordinating with subject matter experts to prepare for Clinger-Cohen Act of 1996 confirmation. The Clinger Cohen Act requires, among other things, that agencies establish policies and procedures to ensure that the accounting, financial, and asset management systems and other information systems of the agency are designed, developed, maintained, and used effectively to provide financial or system performance data for financial statements of the executive agency. However, the guidance does not discuss how systems are to assert or how approval authorities are to validate that a system complies with the department's auditability requirements before proceeding into acquisition. In addition, the Air Force's FY 2022 annual certification guidance does not discuss initial approval of systems before they proceed into development.

Legend:

- Fully addressed: Guidance explains how systems are to address and decision-makers are to substantiate this requirement.
- ⦿ Partially addressed: Guidance discusses the requirement, but does not fully describe how systems are to address and decision-makers are to substantiate this requirement.
- Not addressed: Guidance does not discuss this requirement.

Source: GAO Analysis of Department of Defense (DOD) Guidance. | GAO-23-104539

**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

**Table 16: Assessment of Air Force Guidance for Annual Certification Requirements for Systems That Plan to Spend between \$1 Million and \$250 Million over the Future-Years Defense Program (FYDP)**

Annual Certification Requirement	Extent to Which the Guidance Addresses the Requirement	Assessment Summary
Business process reengineering and maximizing the elimination of unique software requirements and interfaces	partially addressed	<p>The Air Force fiscal year (FY) 2022 annual certification guidance called for Air Force defense business systems to assert compliance with the business process reengineering requirement. Further, the guidance states that program managers should ensure that either the Office of the Secretary of Defense business process reengineering assessment form is completed, updated, and accurate; business process reengineering efforts are thoroughly documented in a business case analysis; or business process reengineering efforts are thoroughly documented in a Defense Business Council or Air Force Chief Management Officer approved problem statement/requirements capability document. Further, the guidance also requires that business process reengineering documentation and supporting artifacts are to be uploaded to the Air Force's Resource library. According to an Air Force official, minimizing interfaces is a key component of the solution analysis phase of the business capability acquisition cycle. However, the guidance does not address how systems are to demonstrate or how approval authorities are to validate that a system has maximized the elimination of unique software requirements or interfaces.</p>
Compliance or planned compliance with the business enterprise architecture	partially addressed	<p>The Air Force FY 2022 annual certification guidance called for Air Force defense business systems to assert compliance with the business enterprise architecture requirement for the annual certification cycle. The Air Force also issued a supplemental memorandum in April 2022 that documents business enterprise architecture compliance guidance for systems seeking annual certification. The guidance memorandum documents the process for determining business enterprise architecture compliance, including how systems found to be non-compliant are to develop a plan to address deficiencies.</p> <p>The guidance memorandum also acknowledges that DOD's Integrated Business Framework-Data Alignment Portal has been decommissioned and will no longer be used and includes an interim solution. For example, the memorandum documents that new defense business systems not previously assessed for business enterprise architecture version 11.2 compliance will be assessed as planned compliant upon review of system documentation and supporting architecture artifacts. The guidance also states that systems previously assessed as compliant with the business enterprise architecture version 11.2 will remain compliant. However, this solution is only temporary and the guidance does not describe a path forward for business enterprise architecture compliance.</p>
Valid, achievable requirements and a viable plan for implementing those requirements	partially addressed	<p>The Air Force FY 2022 annual certification guidance called for Air Force defense business systems to assert compliance with the requirements plan requirement for the annual certification cycle. In addition, according to an Air Force official, a functional sponsor prepares a capability requirements document during a system's capability need identification phase. The Air Force official also stated that management reviews this document during preparation for the solution authority-to-proceed milestone and provides a recommendation to approve or disapprove it. Further, an Air Force official stated that systems are also required to provide a project plan for implementing their requirements. However, the FY 2022 annual certification guidance does not describe how systems are to document or how approval authorities are to validate compliance with this requirement.</p>



**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

Annual Certification Requirement	Extent to Which the Guidance Addresses the Requirement	Assessment Summary
An acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems	partially addressed	The Air Force FY 2022 annual certification guidance called for Air Force defense business systems to assert compliance with the acquisition strategy requirement for the annual certification cycle. An Air Force official stated that an acquisition plan/strategy is developed at the onset of a system and is reviewed and approved by the milestone decision authority prior to, but no later than, the acquisition authority to proceed milestone. According to an Air Force official, all required functional requirements and acquisition planning documents are provided to the milestone decision authority for review and approval before proceeding to acquisition. This official also stated that phase and milestone activities are also reviewed and approved by entities such as the business mission area council prior to milestone decision authority decisions. However, the Air Force annual certification guidance does not describe how systems are to document or how approval authorities are to validate compliance with this requirement.
Compliance with the Department's auditability requirements	partially addressed	The Air Force FY 2022 annual certification guidance called for Air Force defense business systems to assert compliance with the auditability requirement for the annual certification cycle. In addition, the guidance also requires that mandatory data elements be entered within the Air Force's IT Investment Portfolio Suite. According to an Air Force official, the system includes questions for each financial system program office to answer. According to Air Force officials, department-wide guidance does not specify criteria for what systems are required to demonstrate to achieve compliance with the department's auditability requirement. Therefore, the Air Force determined the best approach for substantiating systems assertions for auditability was to inherit the compliance assessment process that the Deputy Assistant Secretary for Financial Operations developed for complying with Air Force's Chief Financial Officer requirements. This includes, among other things, systems completing a Federal Information Systems Control Audit Manual and the Federal Financial Management Improvement Act self-assessment. However, the Air Force annual certification guidance does not describe how systems are to document or how approval authorities are to validate compliance with this requirement.

Legend:

- Fully addressed: Guidance explains how systems are to address and decision-makers are to substantiate this requirement.
- ⦿ Partially addressed: Guidance discusses the requirement, but does not fully describe how systems are to address and decision-makers are to substantiate this requirement.
- Not addressed: Guidance does not discuss this requirement.

Source: GAO Analysis of Department of Defense (DOD) Guidance. | GAO-23-104539

**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

**Table 17: Assessment of Army Guidance for Initial Approval Requirements for Systems That Plan to Spend up to \$250 Million over the Future-Years Defense Program (FYDP)**

Initial Approval Requirement	Extent to Which the Guidance Addresses the Requirement	Assessment Summary
Business process reengineering and maximizing the elimination of unique software requirements and interfaces	partially addressed	<p>The Army's Acting Director for Financial Information Management stated that the Army leverages Department of Defense (DOD) Instruction 5000.75 through all phases of the business capability acquisition cycle. However, as discussed, DOD Instruction 5000.75 does not describe how systems are to substantiate or how approval authorities are to validate compliance with this requirement for initial approval prior to proceeding into development.</p> <p>The Army's January 2018 implementation guidance for DOD Instruction 5000.75 discusses business process reengineering and describes related documentation that should be updated prior to entering into development. The guidance also indicates that the Army Office of Business Transformation is responsible for ensuring appropriate business process reengineering has been conducted. However, the guidance does not describe how decision authorities are to validate that appropriate business process reengineering has been conducted before a system proceeds into development.</p>
Compliance or planned compliance with the business enterprise architecture	partially addressed	<p>The Army's January 2018 Implementation Guidance for the DOD Instruction 5000.75 states that programs are to document alignment with the Army business enterprise architecture prior to completing the business solution analysis phase. The guidance also indicates that the Office of Business Transformation is to review the system for alignment with the business enterprise architecture as part of the functional requirements and acquisition phase. In addition, the guidance states the DOD's Integrated Business Framework – Data Alignment Portal is used for documenting business enterprise architecture alignment. However, an official from the Office of the DOD Chief Information Officer stated that the portal is no longer being used.</p>
Valid, achievable requirements and a viable plan for implementing those requirements	fully addressed	<p>The Army's January 2018 Implementation Guidance for DOD Instruction 5000.75 describes how systems are to substantiate and how approval authorities are to validate compliance with this requirement for initial approval prior to a system proceeding into development. For example, prior to Chief Management Officer certification, the guidance states that as part of the functional requirements and acquisition phase, the functional sponsor will present all IT functional requirements and resource needs to the Army Business Council – Senior Review Group. This group is to validate and approve the final IT functional requirements for the solution and may modify the requirements as needed. The guidance also calls for the functional sponsor to brief parts of the capability implementation plan as part of this discussion.</p>
An acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems	partially addressed	<p>The Army's January 2018 Implementation Guidance for DOD Instruction 5000.75 states that, among other things, a system's acquisition approach, documented in the Acquisition strategy that is developed in the business system functional requirements and acquisition planning phase, is to leverage, where possible, the use of commercial-off-the-shelf software. The guidance for the acquisition, testing, and deployment phase calls for systems to minimize customization by, among other things, employing configuration management to review and approve changes beyond the existing capabilities of the commercial off-the-shelf software. The guidance also states that the Office of Business Transformation is responsible for ensuring that solutions attempt to prevent and minimize commercial off-the-shelf customization. However, the guidance does not describe how systems are to document or decision authorities are to validate that the system has developed an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems prior to entering development.</p>

**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

<b>Initial Approval Requirement</b>	<b>Extent to Which the Guidance Addresses the Requirement</b>	<b>Assessment Summary</b>
Compliance with the Department's auditability requirements	not addressed	DOD Instruction 5000.75, the Army's January 2018 Implementation Guidance for DOD Instruction 5000.75, and the Army's May 2021 Defense Business System Annual Certification and Portfolio Review Guidance do not describe how systems are to substantiate or how approval authorities are to validate compliance with this requirement for initial approval prior to proceeding into development.

**Legend:**

- Fully addressed: Guidance explains how systems are to address and decision-makers are to substantiate this requirement.
- ◐ Partially addressed: Guidance discusses the requirement, but does not fully describe how systems are to address and decision-makers are to substantiate this requirement.
- Not addressed: Guidance does not discuss this requirement.

Source: GAO Analysis of Department of Defense (DOD) Guidance. | GAO-23-104539

**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

**Table 18: Assessment of Army Guidance for Annual Certification Requirements for Systems That Plan to Spend up to \$250 Million over the Future-Years Defense Program (FYDP)**

Annual Certification Requirement	Extent to Which the Guidance Addresses the Requirement	Assessment Summary
Business process reengineering and maximizing the elimination of unique software requirements and interfaces	partially addressed	The Army's May 2021 Defense Business System Annual Certification and Portfolio Review Guidance calls for, among other things, a full business process reengineering to be conducted for all defense business systems in development and once every three years as part of continuous improvement in capability support. The guidance also describes evidence that systems are to submit to demonstrate that a system has conducted sufficient business process reengineering. Further, the guidance indicates where systems are to save supporting documentation. However, the guidance does not indicate how systems are to substantiate or how approval authorities are to validate compliance with the requirement to maximize the elimination of unique software requirements and interfaces prior to a system proceeding into development.
Compliance or planned compliance with the business enterprise architecture	partially addressed	The Army's May 2021 Defense Business System Annual Certification and Portfolio Review Guidance states that Army business enterprise architecture assessments must be performed and documented in DOD's Integrated Business Framework – Data Alignment Portal. It also states that the assessments are for all Army defense business system investments that, among other things, do not have an existing assessment and do not have a replacement target identified but have budget development/modernization funding. In addition, the Army provided training materials for how systems are to document business enterprise architecture compliance. However, officials from the Office of the Department of Defense Chief Information Officer stated that the portal is no longer being used.
Valid, achievable requirements and a viable plan for implementing those requirements	partially addressed	The Army's May 2021 Defense Business System Annual Certification and Portfolio Review Guidance states that all systems seeking certification should demonstrate that they have valid requirements and a plan for implementing those requirements. The guidance further indicates that systems are to upload documentation to a specific Army portal to substantiate compliance. Nevertheless, the guidance does not discuss how approval authorities are to validate that system documentation is sufficient for has valid, achievable requirements and a viable plan for implementing those requirements before the system proceeds into development. The Army's Acting Director for Financial Information Management confirmed that Army has not specified what documentation is required to substantiate this requirement.
An acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems	partially addressed	The Army's May 2021 Defense Business System Annual Certification and Portfolio Review Guidance states that all systems seeking certification should demonstrate that they have an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems. Army guidance calls for systems to upload documentation to an Army portal to demonstrate that this requirement has been met. Nevertheless, the guidance does not discuss how approval authorities are to validate that system documentation is sufficient for demonstrating for validating that a system has developed acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems before the system proceeds into development.

**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

<b>Annual Certification Requirement</b>	<b>Extent to Which the Guidance Addresses the Requirement</b>	<b>Assessment Summary</b>
Compliance with the Department's auditability requirements	partially addressed	The Army's May 2021 Defense Business System Annual Certification and Portfolio Review Guidance states that all audit-related defense business systems seeking certification must upload information to an Army portal documenting that the system is in compliance with audit requirements. Army officials also provided November 2021 guidance for financial management systems. This guidance includes additional steps and documentation associated with asserting that systems comply with the department's auditability requirements. However, Army guidance does not discuss how approval authorities are to validate that system documentation is sufficient for demonstrating compliance with the department's auditability requirements.

Legend:

- Fully addressed: Guidance explains how systems are to address and decision-makers are to substantiate this requirement.
- ⦿ Partially addressed: Guidance discusses the requirement, but does not fully describe how systems are to address and decision-makers are to substantiate this requirement.
- Not addressed: Guidance does not discuss this requirement.

Source: GAO Analysis of Department of Defense (DOD) Guidance. | GAO-23-104539

**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

**Table 19: Assessment of Department of the Navy (DON) Guidance for Initial Approval Requirements for Systems That Plan to Spend Between \$10 Million and \$250 Million over the Future-Years Defense Program (FYDP)**

<b>Initial Approval Requirement</b>	<b>Extent to Which the Guidance Addresses the Requirement</b>	<b>Assessment Summary</b>
Business process reengineering and maximizing the elimination of unique software requirements and interfaces	not addressed	DON's February 2019 Defense Business System Investment Certification Manual V 1.2 does not indicate how systems are to substantiate or how approval authorities are to validate compliance with this requirement for initial approval prior to a system proceeding into development.
Compliance or planned compliance with the business enterprise architecture	not addressed	DON's February 2019 Defense Business System Investment Certification Manual does not indicate how systems are to substantiate or how approval authorities are to validate compliance with this requirement for initial approval prior to a system proceeding into development.
Valid, achievable requirements and a viable plan for implementing those requirements	not addressed	DON's February 2019 Defense Business System Investment Certification Manual does not indicate how systems are to substantiate or how approval authorities are to validate compliance with this requirement for initial approval prior to a system proceeding into development.
An acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems	not addressed	DON's February 2019 Defense Business System Investment Certification Manual does not indicate how systems are to substantiate or how approval authorities are to validate compliance with this requirement for initial approval prior to a system proceeding into development.
Compliance with the Department's auditability requirements	not addressed	DON's February 2019 Defense Business System Investment Certification Manual does not indicate how systems are to substantiate or how approval authorities are to validate compliance with this requirement for initial approval prior to a system proceeding into development.

Legend:

- Fully addressed: Guidance explains how systems are to address and decision-makers are to substantiate this requirement.
- ⦿ Partially addressed: Guidance discusses the requirement, but does not fully describe how systems are to address and decision-makers are to substantiate this requirement.
- Not addressed: Guidance does not discuss this requirement.

Source: GAO Analysis of Department of Defense (DOD) Guidance. | GAO-23-104539

**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

**Table 20: Assessment of Department of the Navy (DON) Guidance for Annual Certification Requirements for Systems That Plan to Spend between \$10 Million and \$250 Million over the Future-Years Defense Program (FYDP)**

Annual Certification Requirement	Extent to Which the Guidance Addresses the Requirement	Assessment Summary
Business process reengineering and maximizing the elimination of unique software requirements and interfaces	fully addressed	DON's February 2019 Investment Certification Manual states that annual defense business system investment certification requires the DON Office of the Chief Management Officer (CMO) to document compliance with 10 U.S.C. § 2222. This includes compliance with the requirement that systems conduct business process reengineering. The guidance also states that this assertion is to be documented in the Department of Defense IT Investment Portal (DITIP). In addition, the guidance states that business process reengineering is to be complete and appropriate documentation is to be uploaded into the DOD IT Portfolio Repository-DON. The guidance also refers to additional guidance on business process reengineering, which describes the documentation needed for substantiating that a system has conducted appropriate business process reengineering.
Compliance or planned compliance with the business enterprise architecture	partially addressed	DON's February 2019 Investment Certification Manual states that annual defense business system investment certification requires the DON Office of the CMO to document compliance with 10 U.S.C. § 2222. This includes compliance with the requirement that systems demonstrate compliance or planned compliance with the business enterprise architecture. The guidance also states that this assertion is to be documented in the Integrated Business Framework-Data Alignment Portal. However, officials from the Office of the DOD Chief Information Officer stated that the portal has been sunset and will no longer be used.
Valid, achievable requirements and a viable plan for implementing those requirements	partially addressed	DON's February 2019 Investment Certification Manual states that annual defense business system investment certification requires the DON Office of the CMO to document compliance with 10 U.S.C. § 2222. This includes compliance with the requirement that systems have valid, achievable requirements and a viable plan for implementing those requirements. The guidance also states that this assertion is to be documented in DITIP. In addition, the guidance states that, among other things, approved business capability requirement documents are relevant for investment certification request and notes that the "viable plan" is the capability implementation plan, which matures over time after the system obtains its authority to proceed to functional requirements. Nevertheless, the guidance provided by DON does not discuss how systems are to substantiate or how approval authorities are to validate compliance with the requirement that the system assert that it has valid, achievable requirements and a viable plan for implementing those requirements.
An acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems	partially addressed	DON's February 2019 Investment Certification Manual states that annual defense business system investment certification requires the DON Office of the CMO to document compliance with 10 U.S.C. § 2222. This includes compliance with the requirement that systems have an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems. The guidance also states that this assertion is to be documented in DITIP. The guidance further refers to an approved business capabilities requirement document, acquisition strategy, or obtaining at least one acquisition authority to proceed decision in support of this requirement. However, the guidance provided by DON does not discuss how systems are to substantiate or how approval authorities are to validate compliance with the requirement that a system has developed an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems.

**Appendix II: Evaluation of DOD Guidance  
for Business and Financial System Initial  
Approvals and Annual Certifications**

Annual Certification Requirement	Extent to Which the Guidance Addresses the Requirement	Assessment Summary
Compliance with the Department's auditability requirements	partially addressed	DON's February 2019 Investment Certification Manual states that annual defense business system investment certification requires the DON Office of the CMO to document compliance with 10 U.S.C. Section 2222. This includes compliance with the department's auditability requirements. The guidance also states that this assertion is to be documented in DITIP. In addition, the guidance explains how the status of independent public auditor findings and associated corrective action plans support decisions regarding this requirement. Nevertheless, the guidance does not discuss how systems are to substantiate or how approval authorities are to validate compliance with the requirement that a system complies with the department's auditability requirements.

Legend:

- Fully addressed: Guidance explains how systems are to address and decision-makers are to substantiate this requirement.
- ⦿ Partially addressed: Guidance discusses the requirement, but does not fully describe how systems are to address and decision-makers are to substantiate this requirement.
- Not addressed: Guidance does not discuss this requirement.

Source: GAO Analysis of Department of Defense (DOD) Guidance. | GAO-23-104539



---

# Appendix III: Comments from the Department of Defense

Appendix III: Comments from the Department of Defense



COMPTROLLER

OFFICE OF THE UNDER SECRETARY OF DEFENSE

1100 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1100

25 JAN 2023

Mr. Kevin Walsh  
Director, IT and Cybersecurity  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Kevin Walsh,

This is the Department of Defense (DOD) response to the GAO Draft Report, GAO 23-104539, "FINANCIAL MANAGEMENT: DOD Needs to Improve Systems Oversight," dated December 2022.

The Department appreciates the opportunity to review this draft report. We have concurred with seven of the recommendations and partially concurred with two of the recommendations. While progress has been made to improve oversight of our priority Financial Management systems, we acknowledge evolving and enhancing our oversight is critical to DOD's efforts to achieve an unmodified audit opinion. The Department will drive this by focusing on efforts to enhance guidance for initial approvals and annual certifications of business systems. Additionally, DOD will improve data collection reliability related to business and financial system compliance with statutory requirements. DOD will also assess its approach to workforce planning, analyzing gaps in capabilities between existing staff and future needs.

Attached are the Department's proposed technical comments to the subject report. My point of contact is Ms. Erica Thomas who can be reached at [erica.e.thomas@mail.mil](mailto:erica.e.thomas@mail.mil) and phone (703) 697-6419.

Sincerely,

Robin Farley, PhD

Dr. Robin Farley  
(Acting) Deputy Comptroller for Enterprise  
Financial Transformation

Digitally signed by Robin Farley, PhD  
DN: cn=Robin Farley, PhD, o=DoD, ou=OS&S&C,  
Funds Directorate, ou=OS&S&C,  
email=robin.farley.d@mail.mil, c=US  
Date: 2023.01.27 12:27:53 -0500

Enclosure:  
Response to GAO Draft Report GAO 23-104539 Consolidated.pdf

**GAO DRAFT REPORT DATED DECEMBER 1, 2022  
GAO-23-104539**

**“FINANCIAL MANAGEMENT: DOD NEEDS TO IMPROVE SYSTEM OVERSIGHT”**

**DEPARTMENT OF DEFENSE COMMENTS  
TO THE GAO RECOMMENDATION**

**RECOMMENDATION 1:** The GAO recommends that 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 to ensure guidance for priority business and financial systems fully addresses the statutory requirements discussed in this report.

**DOD RESPONSE:** The DOD concurs with this recommendation.

**RECOMMENDATION 2:** The GAO recommends that 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.

**DOD RESPONSE:** The DOD concurs with this recommendation.

**RECOMMENDATION 3:** The GAO recommends that 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.

**DOD RESPONSE:** The Secretary of the Army concurs with this recommendation.

**RECOMMENDATION 4:** The GAO recommends that 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.

**DOD RESPONSE:** The Secretary of the Navy concurs with this recommendation.

**RECOMMENDATION 5:** The GAO recommends that the Secretary of the Air Force should direct the Chief Management Officer of the Department of the Air Force to update guidance for

initial approvals 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.

**DOD RESPONSE:** The Secretary of the Air Force concurs with this recommendation.

**RECOMMENDATION 6:** The GAO recommends that 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.

**DOD RESPONSE:** The DOD partially concurs with comments to this recommendation. As the DOD CIO looks at its modernization activities to include technical refresh, an analysis on the potential need to develop additional, supplemental guidance for systems in sustainment will be taken into consideration. Based upon the completed analysis, CIO will then determine whether to implement the recommendation to develop guidance directing the compliance with statutory requirements for having valid, achievable requirements and eliminating or reducing the need to tailor COTS systems. As the Departments lead for IT modernization and authorities for business capabilities and system certification DOD CIO will continue to review its systems architectures, code, infrastructure, processes, to reduce the tailoring of COTS systems.

**RECOMMENDATION 7:** The GAO recommends that 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.

**DOD RESPONSE:** The DOD concurs with this recommendation.

**RECOMMENDATION 8:** The GAO recommends that the Secretary of Defense should direct the DOD CIO to develop and implement plans for documenting detailed system compliance with business enterprise architecture.

**DOD RESPONSE:** The DOD concurs with this recommendation.

**RECOMMENDATION 9:** The GAO recommends that the Secretary of Defense should direct the DOD CIO and USD(C)/CFO 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.

**DOD RESPONSE:** The DOD partially concurs with comments to this recommendation. The development and maintenance of DOD financial management systems leverages the same workforce as all DOD IT acquisitions and oversight. As stated during the engagement, the workforce with development and maintenance execution and oversight responsibilities is comprised of members of the DOD acquisition, financial management, and cyber-excepted

---

**Appendix III: Comments from the Department  
of Defense**

3

workforce within each DOD Component. Functional community oversight provides strategic workforce plans, strategic certification, and training requirements for each of these professional series. In addition, the Department, in accordance with Pub. L. 115-232, div. A, title X, §1004, Aug. 13, 2018, 132 Stat. 1947 assists independent auditors in gathering and reviewing the Defense Business Systems within the Department to include the annual audits of the components and defense entities. This support is done by the professional workforce described above and other members of the 300 and 500 series.

# Accessible Text for Appendix III: Comments from the Department of Defense

25 JAN 2023

Mr. Kevin Walsh  
Director, IT and Cybersecurity  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Kevin Walsh,

This is the Department of Defense (DOD) response to the GAO Draft Report, GAO 23-104539, "FINANCIAL MANAGEMENT: DOD Needs to Improve Systems Oversight," dated December 2022.

The Department appreciates the opportunity to review this draft report. We have concurred with seven of the recommendations and partially concurred with two of the recommendations. While progress has been made to improve oversight of our priority Financial Management systems, we acknowledge evolving and enhancing our oversight is critical to DOD's efforts to achieve an unmodified audit opinion. The Department will drive this by focusing on efforts to enhance guidance for initial approvals and annual certifications of business systems. Additionally, DOD will improve data collection reliability related to business and financial system compliance with statutory requirements. DOD will also assess its approach to workforce planning, analyzing gaps in capabilities between existing staff and future needs.

Attached are the Department's proposed technical comments to the subject report. My point of contact is Ms. Erica Thomas who can be reached at [erica.e.thomas@mail.mil](mailto:erica.e.thomas@mail.mil) and phone (703) 697-6419.

Sincerely,

Dr. Robin Farley  
(Acting) Deputy Comptroller for Enterprise Financial Transformation

Enclosure:

Response to GAO Draft Report GAO 23-104539 Consolidated.pdf

GAO DRAFT REPORT DATED DECEMBER 1, 2022 GAO-23-104539

“FINANCIAL MANAGEMENT: DOD NEEDS TO IMPROVE SYSTEM OVERSIGHT”  
DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The GAO recommends that 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 to ensure guidance for priority business and financial systems fully addresses the statutory requirements discussed in this report.

DOD RESPONSE: The DOD concurs with this recommendation.

RECOMMENDATION 2: The GAO recommends that 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.

DOD RESPONSE: The DOD concurs with this recommendation.

RECOMMENDATION 3: The GAO recommends that 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.

DOD RESPONSE: The Secretary of the Army concurs with this recommendation.

RECOMMENDATION 4: The GAO recommends that 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.

DOD RESPONSE: The Secretary of the Navy concurs with this recommendation.

RECOMMENDATION 5: The GAO recommends that the Secretary of the Air Force should direct the Chief Management Officer of the Department of the Air Force to update guidance for initial approvals 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.

DOD RESPONSE: The Secretary of the Air Force concurs with this recommendation.

RECOMMENDATION 6: The GAO recommends that 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.

DOD RESPONSE: The DOD partially concurs with comments to this recommendation. As the DOD CIO looks at its modernization activities to include technical refresh, an analysis on the potential need to develop additional, supplemental guidance for systems in sustainment will be taken into consideration. Based upon the completed analysis, CIO will then determine whether to implement the recommendation to develop guidance directing the compliance with statutory requirements for having valid, achievable requirements and eliminating or reducing the need to tailor COTS systems. As the Departments lead for IT modernization and authorities for business capabilities and system certification DOD CIO will continue to review its systems architectures, code, infrastructure, processes, to reduce the tailoring of COTS systems.

RECOMMENDATION 7: The GAO recommends that 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.

DOD RESPONSE: The DOD concurs with this recommendation.

RECOMMENDATION 8: The GAO recommends that the Secretary of Defense should direct the DOD CIO to develop and implement plans for documenting detailed system compliance with business enterprise architecture.

DOD RESPONSE: The DOD concurs with this recommendation.

RECOMMENDATION 9: The GAO recommends that the Secretary of Defense should direct the DOD CIO and USD(C)/CFO 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.

DOD RESPONSE: The DOD partially concurs with comments to this recommendation. The development and maintenance of DOD financial management systems leverages the same workforce as all DOD IT acquisitions and oversight. As stated during the engagement, the workforce with development and maintenance execution and oversight responsibilities is comprised of members of the DOD acquisition, financial management, and cyber-excepted workforce within each DOD Component. Functional community oversight provides strategic workforce plans, strategic certification, and training requirements for each of these professional series. In addition, the Department, in accordance with Pub. L. 115–232, div. A, title X, §1004, Aug. 13, 2018, 132 Stat. 1947 assists independent auditors in gathering and reviewing the Defense Business Systems within the Department to include the annual audits of the components and defense entities. This support is done by the professional workforce described above and other members of the 300 and 500 series.

---

# Appendix IV: GAO Contacts and Staff Acknowledgments

---

## GAO Contacts

Kevin Walsh at (202) 512-6151 or [walshk@gao.gov](mailto:walshk@gao.gov) and Vijay A. D'Souza, (202) 512-7650 or [dsouzav@gao.gov](mailto:dsouzav@gao.gov).

---

## Staff Acknowledgments

Principal contributors to this report were Michael Holland (Assistant Director), Neha Bhatt (Analyst in Charge), Tasha Beyzavi, Christopher Businsky, Donna Epler, Camille Garcia, Emmet Ryan, Andrew Weiss, and Haley Weller. Other contributors included Beatrice Alff, Cheryl Andrew, David Ballard, Heather Barker Miller, Margaret Best, Nicole Burkart, Season Burris, Virginia Chanley, Ahmad Ferguson, Franklin Jackson, Jason Kirwan, Phillip McIntyre, Monica Perez Nelson, Scott Pettis, Zsaroq Powe, Adam Vodraska, and Shawn Ward.

---

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).  
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).  
Visit GAO on the web at <https://www.gao.gov>.

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

---

---

## Congressional Relations

A. Nicole Clowers, Managing Director, [ClowersA@gao.gov](mailto:ClowersA@gao.gov), (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

---

## Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, [spel@gao.gov](mailto:spel@gao.gov), (202) 512-4707  
U.S. Government Accountability Office, 441 G Street NW, Room 7814,  
Washington, DC 20548



**Please Print on Recycled Paper.**