



September 2020

FINANCIAL MANAGEMENT

DOD Needs to
Implement
Comprehensive Plans
to Improve Its
Systems Environment

GAO Highlights

Highlights of [GAO-20-252](#), a report to congressional requesters

Why GAO Did This Study

DOD financial management has been on GAO's High Risk List since 1995 because of long-standing deficiencies found in, among other areas, its supporting information systems. DOD uses these systems to report its spending and assets.

GAO was requested to review DOD's financial management systems. The objectives of this review are to determine (1) to what extent the data produced by DOD financial management systems are reported to be reliable for presenting financial statements in accordance with generally accepted accounting principles, (2) to what extent DOD and the military departments have strategies and plans to address key information technology controls for their financial systems, and (3) how much money DOD reports spending on developing and maintaining its financial management systems.

To address these objectives, GAO analyzed (1) independent public auditors' findings resulting from the department's fiscal year 2019 audit; (2) DOD's financial management systems strategy and plans relative to OMB guidance and recent legislation; (3) data in DOD system and budget databases. GAO also interviewed relevant DOD and military service officials.

View [GAO-20-252](#). For more information, contact Kevin Walsh, 202-512-6151, walshk@gao.gov, or Asif Khan, 202-512-9869, khana@gao.gov.

September 2020

FINANCIAL MANAGEMENT

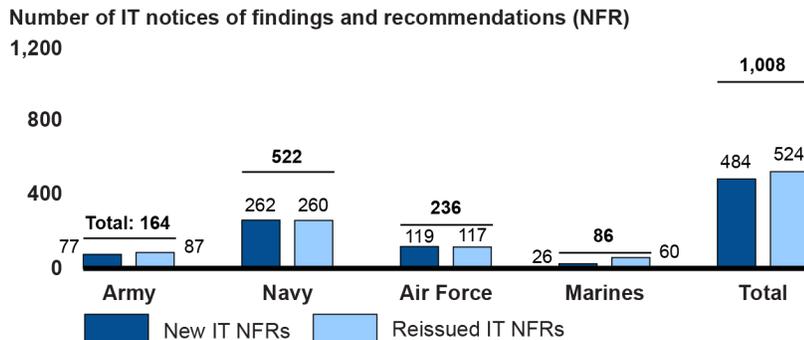
DOD Needs to Implement Comprehensive Plans to Improve Its Systems Environment

What GAO Found

Data supporting the Department of Defense's (DOD) fiscal year 2019 financial statements are not reliable, according to the DOD Office of Inspector General (OIG) and independent auditors. In January 2020, the OIG reported that the department had wide-ranging weaknesses in its financial management systems that prevented it from collecting and reporting financial and performance information that was accurate, reliable, and timely. Specifically, the OIG reported 25 material weaknesses that impacted DOD's ability to achieve an unmodified audit opinion on its fiscal year 2019 department-wide financial statements. These material weaknesses are based, in large part, on identified deficiencies and corresponding recommendations, also known as notices of findings and recommendations (NFRs).

In fiscal year 2019, independent public accountants issued 2,100 new and reissued NFRs to the military services and DOD remediated 26 percent of the military services' NFRs from fiscal year 2018. Of the 2,100 fiscal year 2019 NFRs, 1,008 were related to information technology (IT) and cybersecurity issues. Of the 1,008 NFRs, 484 were new and 524 were reissued from previous years. (See figure.)

Figure: IT Notices of Findings and Recommendations Issued by Independent Public Accountants Based on Audits of Military Services' Fiscal Year 2019 Financial Statements



Source: Department of Defense Office of Inspector General. | GAO-20-252

To address the NFRs and DOD's underlying financial management system weaknesses, the department has a strategy that fully addresses three requirements for a comprehensive and effective IT strategic plan; however, it does not include measures for tracking progress in achieving the strategy's goals. (See table on next page.)

What GAO Recommends

GAO made the following six recommendations to DOD:

1. Establish performance measures for DOD's financial management systems strategy, including targets and time frames, and how it plans to measure values and verify and validate those values.
2. Establish a specific time frame for developing an enterprise road map to implement DOD's financial management systems strategy and ensure that it is developed.
3. Develop detailed migration plans for certain key accounting systems.
4. Establish performance goals with performance indicators, targets and time frames, to monitor DOD's efforts to address IT-related audit findings.
5. Implement a mechanism for identifying a complete list of financial management systems and related budget data.
6. Limit investments in financial management systems to what is essential to maintain functional systems and help ensure system security until DOD implements the other recommendations.

DOD concurred with GAO's recommendations and described actions it plans to take to address them.

DOD Needs to Implement Comprehensive Plans to Improve Its Systems Environment

Table: GAO Ratings of DOD's IT Financial Management Systems Strategy

IT Strategic Plan Requirements ^a	GAO Ratings
Alignment with the agency's overall strategic plan	●
Results-oriented goals and performance measures	◐
Strategies to achieve desired results, including a clear narrative of how IT is enabling agency goals	●
Descriptions of dependencies within and across projects	●

Legend:

- Fully addressed: DOD provided evidence that it fully addressed this requirement.
- ◐ Partially addressed: DOD provided evidence that it addressed some, but not all, of this requirement.

Source: GAO analysis of Department of Defense documentation. | GAO-20-252

^aThe requirements for a comprehensive and effective IT strategic plan are based on Office of Management and Budget guidance and prior GAO research and reviews of federal agencies' IT strategic plans.

DOD has not developed an enterprise road map to implement its strategy, as called for by Office of Management and Budget guidance. Such a road map should document the current and future states of a systems environment that, among other things, describes business processes and rules, information needs and flows, and work locations and users; and a transition plan for moving from the current to the future. In response to recently enacted legislation requiring a comprehensive road map, DOD stated that it plans to develop one; however, it did not state by when.

DOD also does not have sufficiently detailed plans for migrating key military service legacy accounting systems to new systems. The Navy has developed a plan to migrate its system, but the plan is missing key elements consistent with Software Engineering Institute guidance. The Army and Air Force do not have detailed migration plans for their key accounting systems.

While DOD has developed a plan to address IT issues identified during annual audits, it has not established performance goals that include indicators, targets, and time frames. Officials said that it is challenging to develop such goals because issues identified by the IPAs vary widely. However, DOD has already grouped the issues by priority, facilitating the establishment of appropriate performance goals.

Moreover, DOD does not know how much it spends on the systems that support its financial statements because it does not have a way to reliably identify these systems in its systems inventory and budget data. GAO calculated that the department will spend at least \$2.8 billion on those systems in fiscal year 2020. However, that amount is understated—GAO identified 45 systems that were missing from the list of significant systems that DOD provided to GAO.

As a result of these deficiencies, the department faces challenges in ensuring accountability over its extensive resources and in effectively managing its assets and budgets. DOD also risks wasting funds on short-term fixes that might not effectively and efficiently support longer-term department goals.

Contents

Letter		1
	Background	6
	DOD Cannot Demonstrate That Data Supporting Financial Statements Are Reliable	16
	DOD and the Military Services Lack Comprehensive Plans for Improving Financial Management Systems	27
	DOD Does Not Know How Much It Spends on Financial Management Systems; GAO Calculated at Least \$2.4 Billion Annually, but Data Are Not Fully Reliable	40
	Conclusions	43
	Recommendations for Executive Action	44
	Agency Comments and Our Evaluation	45
Appendix I	Objectives, Scope, and Methodology	48
Appendix II	Summary of the Department of Defense's Financial Management Functional Strategy	55
Appendix III	Key Roles and Responsibilities of the DOD CFO, CIO, and CMO for Financial Management Systems	59
Appendix IV	DOD Spending On New and Legacy Accounting Systems, Fiscal Years 2016 through 2020	63
Appendix V	Comments from the Department of Defense	66
Appendix VI	GAO Contacts and Staff Acknowledgments	67

Tables

Table 1: Sections of the DOD Annual Financial Report	11
Table 2: Number of Issues Contained in the Fiscal Year 2019 Military Services' Financial Notices of Findings and Recommendations (NFR)	21
Table 3: Number of Issues Contained in the Fiscal Year 2019 Military Services' Information Technology (IT) Notices of Findings and Recommendations (NFR)	25
Table 4: GAO Ratings of IT Strategic Plan Requirements Compared to DOD's Financial Management Systems Strategy	29
Table 5: DOD Spending on Development and Modernization and Operations and Maintenance for Systems in DOD's Financial Improvement and Audit Readiness (FIAR) System Database, Fiscal Years 2016-2020	41
Table 6: Military Services Spending on New Financial Management Systems, Fiscal Years (FY) 2016 through 2020	64
Table 7: Department of Defense and the Military Services Spending on Legacy Accounting Systems, Fiscal Years (FY) 2016 through 2020	65

Figures

Figure 1: Transaction Level Data Flowing through Department of Defense (DOD) Financial Management Systems	12
Figure 2: Key Components of the Department of Defense Integrated Business Framework	15
Figure 3: Financial Notices of Findings and Recommendations Issued by Independent Public Accountants, Based on Audits of the Military Services' Fiscal Year 2019 Financial Statements	20
Figure 4: Information Technology (IT) Notices of Findings and Recommendations Issued by Independent Public Accountants, Based on Audits of the Military Services' Fiscal Year 2019 Financial Statements	23

Abbreviations

CFO	chief financial officer
CIO	chief information officer
CMO	chief management officer
DITPR	DOD Information Technology Portfolio Repository
DOD	Department of Defense
IPA	independent public accountant
IT	information technology
FFMIA	Federal Financial Management Improvement Act of 1996
FIAR	Financial Improvement and Audit Readiness
FISCAM	Federal Information System Controls Audit Manual
FMFIA	Federal Managers' Financial Integrity Act of 1982
NFR	notice of findings and recommendations
OIG	Office of Inspector General
OMB	Office of Management and Budget
SNAP-IT	Select and Native Programming-IT System

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.



September 30, 2020

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 and its ability to efficiently and effectively manage its assets and budgets. However, DOD financial management has been on GAO's High-Risk List since 1995 because of long-standing deficiencies found in, among other areas, its systems.¹ For example, independent public accountants (IPAs) have long reported on the military services' inability to effectively implement information system controls to protect their financial data.²

In addition, the DOD Office of Inspector General (OIG) reported in fiscal years 2018 and 2019 that DOD did not comply with the Federal Financial Management Improvement Act of 1996 (FFMIA).³ Moreover, DOD remains one of the few entities in the federal government that cannot demonstrate its ability to accurately account for and reliably report its spending and assets. DOD's financial management problems remain one of three major impediments preventing GAO from expressing an opinion on the consolidated financial statements of the federal government.

Given the long-standing deficiencies in DOD's financial management, you asked us to review these systems. Our specific objectives were to determine (1) to what extent the data produced by DOD financial management systems are reported to be reliable for presenting financial statements in accordance with generally accepted accounting principles; (2) to what extent DOD and the military services have strategies and plans to address key information technology controls for their financial

¹GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High Risk Areas*, [GAO-19-157SP](#) (Washington, D.C.: March 6, 2019).

²The military services are the Army, Navy, Air Force, and Marine Corps.

³Department of Defense Office of Inspector General, *Understanding the Results of the Audit of the DOD FY 2019 Financial Statements* (Alexandria, VA: Jan. 28, 2020). FFMIA requires DOD and certain other federal agencies to implement and maintain financial management systems that comply substantially with (1) federal financial management systems requirements, (2) applicable federal accounting standards, and (3) the United States Government Standard General Ledger (USSGL) at the transaction level. Pub. L. No. 104-208, div. A, § 101(f), title VIII, 110 Stat. 3009, 3009-389 (Sep. 30, 1996).

management systems; and (3) how much money DOD reports spending on developing and maintaining its financial management systems.⁴

To determine to what extent the data produced by DOD's financial management systems are reported to be reliable for presenting financial statements in accordance with generally accepted accounting principles, we obtained and reviewed the notices of findings and recommendations (NFR) issued by the IPAs as part of their fiscal year 2019 audits of the military services' financial statements.⁵ The IPAs reported the NFRs in two broad categories, financial and information technology (IT). In assessing the financial findings, we used the condition statements documented by the IPAs within each NFR to categorize the financial NFRs.

In assessing the IT findings, we used the *Federal Information System Controls Audit Manual* (FISCAM).⁶ Specifically, we reviewed the IT NFRs and summarized them by FISCAM category to identify the key issues limiting financial data reliability. We also reviewed the DOD Office of Inspector General reports transmitting the results of the military services' audits. To determine what steps DOD is taking to address the NFRs, we reviewed the DOD OIG report describing the DOD components' NFR

⁴According to FFMIA, 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.

⁵A notice of findings and recommendations 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 information technology NFRs.

⁶GAO, *Federal Information System Controls Audit Manual* (FISCAM), [GAO-09-232G](#) (Washington, D.C.: February 2009). FISCAM presents a methodology for performing information system control audits of federal and other governmental entities in accordance with professional standards.

actions and the DOD *Financial Improvement and Audit Remediation Report*.⁷

To determine to what extent DOD and the military services have strategies and plans to address key IT controls, we evaluated the department's documents describing its strategy for improving its financial management systems. We also determined whether the department had an integrated road map to implement its strategy. In addition, we requested and reviewed any plans that the department had for effectively migrating legacy accounting systems to new systems. We also evaluated the department's plans for addressing IT control issues identified in the department's financial statement audit. These efforts are discussed in more detail below.

- To evaluate the department's strategy for improving its financial management systems, we reviewed the *Department of Defense Financial Management Functional Strategy for Fiscal Years 2019 to 2023* and the military services' fiscal year 2019 organization execution plans, which the department said comprise its financial management systems strategy. We compared the DOD financial management systems strategy with elements of a comprehensive and effective IT strategic plan, which we derived from Office of Management and Budget (OMB) guidance and our prior research and experience reviewing federal agencies' IT strategic plans.⁸

⁷Department of Defense Office of Inspector General, *Understanding the Results of the Audit of the DOD FY 2019 Financial Statements* (Alexandria, VA: Jan. 28, 2020); Office of the Under Secretary of Defense (Comptroller), *Financial Improvement and Audit Remediation (FIAR) Report*, June 2020.

⁸OMB, Circular No. A-11: *Preparation, Submission, and Execution of the Budget*, June 2018; Circular No. A-130: *Managing Information as a Strategic Resource* (Washington, D.C.: July 28, 2016); Memorandum M-13-09 *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management* (Washington, D.C.: Mar. 27, 2013); *Federal Enterprise Architecture Framework*, Version 2, Jan. 29, 2013; and *The Common Approach to Federal Enterprise Architecture*, May 2, 2012; and GAO, *Social Security Administration: Improved Planning and Performance Measures are Needed to Help Ensure Successful Technology Modernization*, [GAO-12-495](#) (Washington, D.C., April. 26, 2012); *Defense Business Transformation: Status of Department of Defense Efforts to Develop a Management Approach to Guide Business Transformation*, [GAO-09-272R](#) (Washington, D.C.: Jan. 9, 2009); *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses*, [GAO-15-315](#) (Washington, D.C., Mar. 31, 2015); and *NASA Information Technology: Urgent Action Needed to Address Significant Management and Cybersecurity Weaknesses*, [GAO-18-337](#) (Washington, D.C.: May 22, 2018).

-
- To determine if the department has an integrated road map to implement its financial management systems strategy, we evaluated the department's efforts to develop an enterprise road map, which is a document OMB requires federal agencies to develop annually to implement their IT strategic plans. OMB requires agencies to develop an integrated plan that documents the current and future states of a business and systems environment 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.⁹ We compared the information DOD provided to OMB's requirements.
 - To determine if DOD had migration plans for its key legacy accounting systems that we identified based on our past and ongoing oversight of DOD financial audits, we reviewed documentation to ascertain whether the department had developed plans for the Air Force, Army, and Navy¹⁰ legacy accounting systems.¹¹ We compared the information provided by DOD to leading practices for planning software migrations developed by the Software Engineering Institute.¹²
 - To determine to what extent DOD was effectively monitoring its efforts to remediate IT issues, we reviewed the department's June 2019 Financial Management Audit Support Plan, and July 3, 2019, memorandum signed by the Chief Information Officer (CIO), the Deputy Under Secretary of Defense (Comptroller) and the Acting Chief Management Officer, on addressing deficiencies in system access controls identified in IT NFRs.¹³ In addition, we obtained and

⁹Enterprise architecture is intended to provide a clear and comprehensive picture of a functional or mission area that cuts across more than one organization. It describes the enterprise in logical terms (such as interrelated business processes and business rules, information needs and flows, and work locations and users), as well as in technical terms (such as hardware, software, data, communications, security attributes, and performance standards).

¹⁰The Marine Corps was included in the Department of Navy.

¹¹These legacy accounting systems are systems that support the key functions of a military service's financial management and are integral to the financial reporting process, which are planned to be decommissioned, retired, or replaced.

¹²Software Engineering Institute, *DOD Software Migration Planning*, CMU/SEI-2001-TN-012 (Pittsburgh, PA: August 2001). SEI is a nationally recognized, federally funded research and development center established at Carnegie Mellon University in Pittsburgh, Pennsylvania, to address software development issues.

¹³The Acting Chief Management Officer was confirmed by the Senate on December 19, 2019, to be Chief Management Officer.

reviewed updates on the status of DOD's efforts to remediate IT issues, which were prepared for DOD officials between February and September 2019. We compared the content of these documents with OMB guidance on establishing performance goals and using them to measure progress.¹⁴ Specifically, we assessed the extent to which DOD's plans include performance goals with performance indicators, targets, and time frames, and the extent to which the status updates report progress.

- We also conducted interviews with relevant officials in the Office of the CIO, the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer (hereinafter referred to as the CFO), and the Office of the Chief Management Officer (CMO) to discuss the development of strategies and plans to guide financial management systems improvement efforts, including plans to address key information technology controls for their financial management systems.

To determine how much money DOD reports spending on developing and maintaining its financial management systems, we obtained DOD's list of significant financial and feeder systems from its Financial Improvement and Audit Readiness (FIAR) Systems Database. We matched the identification number in the list of significant financial and feeder systems with the identification number in the DOD IT Portfolio Repository to identify the unique investment identifier associated with each system. Using the unique investment identifiers, which are included in the budget data reported on the federal IT Dashboard, we identified the amount DOD reported spending on developing and modernizing and operating and maintaining the financial and feeder systems in fiscal years 2016 through 2018 and the amount DOD planned to spend in fiscal years 2019 and 2020.¹⁵ We also determined the total amount the department spent in fiscal years 2016 through 2018 and the amount it planned to spend in fiscal years 2019 and 2020 on new and legacy financial management systems.

We discussed our approach to determining the spending with officials in the Office of the CIO and in the Office of the CFO, and they provided

¹⁴OMB, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11, June 2018.

¹⁵The federal IT Dashboard is a website that enables federal agencies, industry, the general public, and other stakeholders to view details regarding the performance of federal IT investments.

comments, which we incorporated. We also assessed the reliability of the data we used to determine the spending. Specifically, we reviewed documentation related to the data systems (e.g., user training manuals), discussed the systems and the quality and reliability of the data in them with department officials, and reviewed the data for obvious issues, such as missing or questionable values.

We determined that the data in DOD's IT Portfolio Repository and the data reported on the IT Dashboard were sufficiently reliable for calculating the annual costs of the systems in the FIAR Systems Database. However, we determined that many systems and their associated costs were not included in this database. Accordingly, the total amount of costs we determined is understated. Further details about this issue are in the report. Appendix I contains additional details on our objectives, scope and methodology.

We performed this audit from March 2018 to August 2020, 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. For fiscal year 2020, DOD's enacted budget is \$712.6 billion; the President's Budget for fiscal year 2021 requests \$705.4 billion.¹⁶ DOD's discretionary spending is almost half of the federal government's and its reported assets represent approximately 75 percent of the federal government's. The department is one of the nation's largest employers, with over 2.1 million service members and over 770,000 civilians spread across approximately 4,500 DOD sites located in all 50 states, seven U.S. territories, and over 40 countries.

DOD's business systems include financial management systems, human resource management systems, logistics and supply chain management systems, property management systems, and acquisition management

¹⁶Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *Defense Budget Overview: United States Department of Defense Fiscal Year 2021 Budget Request*, February 2020.

systems. These systems contribute information that supports the department's efforts to prepare financial statements.

As we have previously reported, the DOD systems environment that supports its business functions, including financial management, has been overly complex and error prone, characterized by (1) little standardization across the department, (2) multiple systems performing the same tasks, (3) the same data stored in multiple systems, and (4) the need for data to be entered manually into multiple systems.¹⁷ For fiscal year 2020, the department requested about \$8.9 billion for its defense business systems.

DOD's Audit Requirements

The Chief Financial Officers Act of 1990 (CFO Act) required that, beginning with fiscal year 1991, certain federal agencies, including DOD, prepare financial statements covering their revolving funds, trust funds, and components performing substantial commercial functions, and have those statements audited by the agency's OIG or by an independent external auditor, as determined by the agency's OIG.¹⁸ The Government Management Reform Act of 1994, among other things, expanded the scope of these required statements to cover all accounts and associated activities of affected agencies, beginning with fiscal year 1996.¹⁹ This act also required the director of OMB to identify components of federal agencies required to prepare their own audited financial statements.²⁰

¹⁷GAO, *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).

¹⁸Besides initiating agency financial statement requirements, the CFO Act, Pub. L. No. 101-576, 104 Stat. 2838 (Nov. 15, 1990), also established a new federal financial management leadership structure, including chief financial officers to oversee financial management activities at 23 major executive departments and agencies. The list now includes 24 entities, which are often referred to collectively as "CFO Act agencies" and is codified, as amended, in section 901(b) of Title 31 of the United States Code.

¹⁹The Government Management Reform Act of 1994, Pub. L. No. 103-356, 108 Stat. 3410 (Oct. 13, 1994), also added a requirement for government-wide financial statements, beginning with fiscal year 1997, to be prepared by the Secretary of the Treasury and audited by GAO.

²⁰Within DOD, OMB currently requires separate financial statements for: the General Funds of the U.S. Navy, the U.S. Marine Corps, and the Departments of the Army and the Air Force; the Working Capital Funds of the Departments of the Army, the Navy, and the Air Force; the Military Retirement Fund; and the U.S. Army Corps of Engineers Civil Works Program. See OMB, Bulletin No. 19-03, *Audit Requirements for Federal Financial Statements*, app. B (Aug. 27, 2019).

After many years of working toward financial statement audit readiness, DOD underwent full financial statement audits in fiscal years 2018 and 2019.

Congress has periodically enacted laws that added additional conditions, requirements, and due dates for DOD's efforts to become auditable. Among other things, these have included reporting parameters to assist in monitoring the department's financial improvement efforts, specifications for financial statement audits, and audit readiness milestones. In addition, the department has taken steps to help improve its financial management. For example,

- The National Defense Authorization Act for Fiscal Year 2002 required the Secretary of Defense to annually report on whether a financial statement issued by DOD or a department component was reliable, and limited the audit procedures that the DOD OIG was allowed to perform on statements asserted to be unreliable. This provision allowed the DOD OIG to perform procedures required by generally accepted government auditing standards consistent with this assertion on reliability.²¹ Prior to fiscal year 2018, only a limited number of DOD components asserted that their information was ready for audit, such as the Military Retirement Fund financial statements and the U.S. Army Corps of Engineers-Civil Works financial statements.
- The DOD 2003 Financial Improvement Initiative was intended to fundamentally transform the department's financial management operations and achieve unmodified audit opinions on its financial statements.²²
- The DOD FIAR Directorate, located in the Office of the CFO, was established in 2005. Its purpose was 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.
- In 2009, the DOD CFO directed that the department focus on improving processes and controls supporting information that is most

²¹National Defense Authorization Act for Fiscal Year 2002, Pub. L. No. 107-107, div. A, § 1008(d), 115 Stat. 1012, 1206 (Dec. 28, 2001).

²²An 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.

often used to manage the department, while continuing to work toward financial improvements aimed at achieving unmodified audit opinions on the department's financial statements.

- The National Defense Authorization Act for Fiscal Year 2010 required DOD to develop and maintain the semi-annual FIAR plan.²³ The plan was prepared by the FIAR Directorate and its purpose was to lead the department's improvement of its financial management processes. The FIAR Directorate also developed and tracked the progress of the FIAR Plan, and reported on DOD's efforts to become audit-ready. The plan was intended to assist the department in improving its internal controls over financial reporting²⁴ and resolving material weaknesses identified in the financial audit reports.²⁵ Additionally, the FIAR Plan set milestones for resolving problems affecting the accuracy, reliability, and timeliness of DOD's financial information.
- The National Defense Authorization Act for Fiscal Year 2014 required the Secretary of Defense to ensure that a full-scope audit of the DOD financial statements was performed for fiscal year 2018.²⁶ Audit results for fiscal year 2018 were to be submitted to Congress no later than March 31, 2019. DOD OIG conducted and oversaw a full audit of DOD's financial statements for fiscal year 2018.
- The National Defense Authorization Act for Fiscal Year 2016 required DOD OIG to hire independent external auditors to audit the DOD

²³Pub. L. No. 111-84, div. A, § 1003(a), 123 Stat. 2190, 2439-40 (Oct. 28, 2009).

²⁴An entity's internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, the objectives of which are to provide reasonable assurance that: (1) transactions are properly recorded, processed, and summarized to permit the preparation of financial statements in accordance with U.S. generally accepted accounting principles, and assets are safeguarded against loss from unauthorized acquisition, use, or disposition; and (2) transactions are executed in accordance with provisions of applicable laws, including those governing the use of budget authority; regulations; contracts; and grant agreements, noncompliance with which could have a material effect on the financial statements.

²⁵A material weakness is a deficiency or combination of deficiencies in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

²⁶Pub. L. No. 113-66, div. A, § 1003, 127 Stat. 671, 842 (Dec. 26, 2013).

component financial statements.²⁷ As the overall auditor of the financial statements, referred to as the Agency-Wide Basic Financial Statements, the DOD OIG oversees these audits and performs additional procedures necessary to support the overall audit of the agency-wide basic financial statements. DOD OIG contracted with five IPA firms to perform a total of 21 DOD component financial statement audits for fiscal year 2018.

- The National Defense Authorization Act for Fiscal Year 2018 repealed the requirement for the semi-annual FIAR Plan and replaced it with a requirement for the new annual Financial Improvement and Audit Remediation Plan.²⁸ In the remediation plan, DOD is to describe the specific actions that it intends to take to address the NFRs, or audit findings, that auditors issue when they identify weaknesses in the department's business processes and financial statements. The remediation plan is to provide interim milestones for completing those actions and cost estimates for the remediation actions. This Act also explicitly required that DOD financial statements henceforth undergo annual audit.

DOD Financial Reporting

DOD, which includes the military services, prepares an annual financial report to describe and communicate its financial position and the results of DOD operations. The financial statements published in this financial report include information such as the Statement of Budgetary Resources, the Balance Sheet, the Statement of Net Cost, and the Statement of Changes in Net Position. Table 1 describes the sections of this annual report.

²⁷Pub. L. No. 114-92, div A, § 1005, 129 Stat. 726, 961-962 (Nov. 25, 2015).

²⁸National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, div. A, § 1002, 131 Stat. 1283, 1537-1540 (Dec. 12, 2017); 10 U.S.C. § 240b. This provision repealed many audit-readiness-related provisions in previous NDAAAs and instead enacted substantially similar provisions together as a new chapter 9A in Title 10, United States Code.

Table 1: Sections of the DOD Annual Financial Report

Section	Description
Management's Discussion & Analysis	Provides a high-level overview of the department's program and financial performance. This section also includes a summary of the department's mission and structure, the current status of financial management systems, compliance with laws and regulations, and management assurances regarding internal controls.
Financial	Includes the Principal Financial Statements and Notes, Required Supplementary Information, and the Independent Auditor's Report
Other Information	Provides a summary of the Financial Statement Audit and Management Assurances, and Management Challenges
Appendices	Provides acronyms and abbreviations, and an index of charts and tables

Source: Department of Defense Agency Financial Report (AFR) for Fiscal Year 2018. | GAO-20-252

DOD's Financial Audits

Financial audits are intended to provide independent assessments over the reliability of the financial statements included in the DOD financial report. For example, the audits help to provide Congress and the public with an assessment of how DOD uses its funds and provide transparency over how DOD spends its resources. The audits help identify instances of potential waste, fraud, and abuse. In addition, they help identify and contribute to needed improvements in information technology system vulnerabilities and cybersecurity. They also can identify opportunities for improving DOD's business processes.

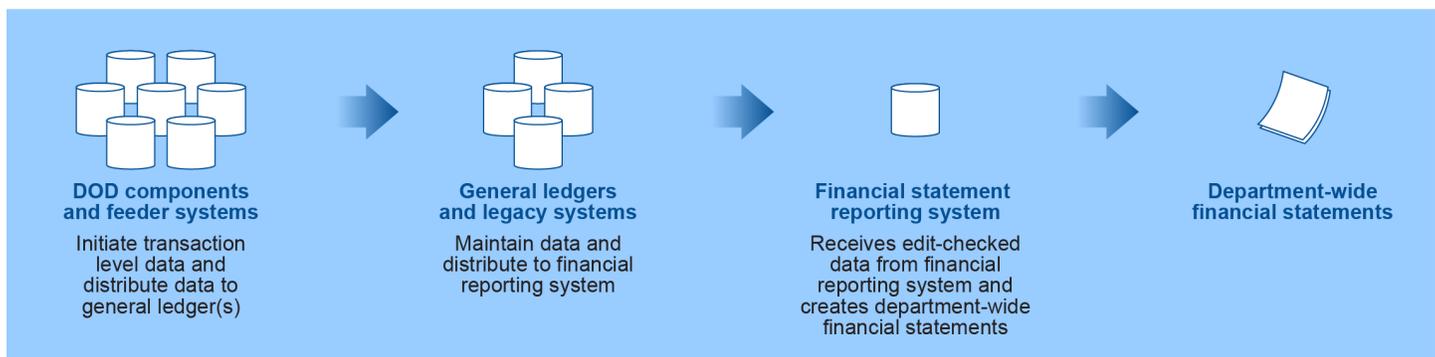
IPAs conducted audits of the military services' fiscal year 2019 and 2018 financial statements for the General and Working Capital Funds.²⁹ DOD OIG audited the fiscal year 2019 DOD Consolidated Financial Statements and relied, in part, on the results of the IPAs' audits of the military services to assist with rendering its final opinion.

²⁹General fund accounts are receipt accounts not dedicated to a specific purpose and expenditure accounts established to record transactions arising under congressional appropriations. Working Capital Funds are funds established to finance inventories of supplies, industrial-type activities, and commercial-type activities that provide common services within or among DOD components. These funds function primarily from the fees charged for the supplies and services they provide.

IT Systems Support DOD Financial Reporting and Audits

As we have previously reported, most military service transactions are initially processed and recorded in IT systems, called feeder systems.³⁰ For example, payroll transactions are processed in a military service's payroll system. Transactions processed in feeder systems should eventually be transferred to the military service's general ledger, where all transactions are accumulated. At the end of a reporting period, each military service's general ledger and legacy system data and other DOD components' general ledger and legacy system data are transferred to DOD's financial reporting system. That system summarizes the financial data according to the line items that are ultimately reported in the department-wide basic financial statements. Figure 1 illustrates the flow of transaction level data through multiple DOD financial management systems and ultimately presented in the department-wide financial statements.

Figure 1: Transaction Level Data Flowing through Department of Defense (DOD) Financial Management Systems



Source: GAO analysis of Department of Defense financial transaction data flow. | GAO-20-252

The CFO Act mandates that an agency CFO develop and maintain an integrated agency financial management system that complies with applicable accounting principles, standards, and requirements; internal control standards; and requirements of OMB.³¹ In addition, the Federal Managers' Financial Integrity Act of 1982 (FMFIA) requires each executive agency to perform ongoing evaluations and report on the

³⁰GAO, *DOD Financial Management: Significant Efforts Still Needed for Remediating Audit Readiness Deficiencies*, [GAO-17-85](#) (Washington, D.C.: Feb. 9, 2017).

³¹The Under Secretary of Defense (Comptroller) serves as the CFO for DOD. 10 U.S.C. § 135(b).

adequacy of its systems of internal accounting and administrative control.³² The Federal Financial Management Improvement Act of 1996 (FFMIA) further requires CFO Act agency management and financial statement auditors to report on whether the agency's financial management systems substantially comply with federal financial management systems requirements, federal accounting standards, and the United States Government Standard General Ledger.

Key Financial Management Systems

The following key systems are examples of systems considered relevant to DOD's and the military services' financial statement audits:

- Defense Departmental Reporting System (DDRS);
- Air Force's Defense Enterprise Accounting and Management System (DEAMS) and General Accounting and Finance System-Reengineered (GAFS-R);³³
- Marine Corps' Standard Accounting Budgeting and Reporting System (SABRS);
- Navy's Standard Accounting and Reporting System (STARS)³⁴ and Navy Enterprise Resource Planning (Navy ERP); and
- Army's General Fund Enterprise Business System (GFEB), Standard Finance System (STANFINS), and Standard Operation and Maintenance Army Research and Development System (SOMARDS).

Overview of DOD's Integrated Business Framework

The Office of the Chief Management Officer (CMO) developed its Integrated Business Framework (IBF) to provide an overarching structure for how DOD governs and manages business operations, including business systems. DOD uses a tool called the IBF-Data Alignment Portal (IBF-DAP) to document and link data related to defense business systems. The IBF-DAP allows users to link business system investments to the department's strategic initiatives and develop functional strategies and organizational execution plans.

³²31 U.S.C. § 3512(c), (d).

³³GAFS-R is owned by Defense Finance and Accounting Service (DFAS) but utilized by the Air Force.

³⁴According to the Navy's STARS-FL System GL Consolidation and System Decommissioning Plan issued in April 2020, STARS-FL is expected to be decommissioned at the end of first quarter fiscal year 2021.

Using the overarching goals of the department's *National Defense Business Operations Plan*,³⁵ principal staff assistants³⁶ develop functional strategies within the IBF-DAP for eight business areas, including financial management.³⁷ The functional strategies are to define the mission, vision, business outcomes, initiatives, and prior year business outcome and initiative progress for a given functional area within DOD.

The military services and other DOD organizations are to use the functional strategies to guide the development of organizational execution plans. These plans contain the component's business strategy for managing its portfolio of systems. Each plan is to be divided into chapters for each of the eight business areas, and is to include, among other things, key cost drivers and functional strategy outcomes. In addition, each organizational execution plan is to include a portfolio of defense business system investments organized by business area, and linkages between defense business system investments and functional strategy initiatives. Figure 2 illustrates the main components of the framework. Appendix II describes DOD's financial management functional strategy for fiscal years 2019 to 2023.

³⁵Department of Defense, *FY 2018-FY 2022 National Defense Business Operations Plan*, April 9, 2018.

³⁶Principal staff assistants are senior advisors to the Secretary of Defense who are responsible for developing functional strategies that are to describe business functions, outcomes, measures and standards for their respective business areas.

³⁷The business areas are financial management, acquisition and contract management, logistics and supply chain management, real property management, defense security enterprise, human resources management, defense health, and enterprise information technology infrastructure. Principal staff assistants also may develop other functional strategies as the business alignment process evolves.

Figure 2: Key Components of the Department of Defense Integrated Business Framework



Source: GAO analysis of DOD documentation. | GAO-20-252

Roles and Responsibilities of Key Entities for DOD Financial Management Systems

The DOD CFO, CIO, and CMO have responsibilities for the department's financial management systems. For example:

- The 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 information technology, networking, information assurance, cybersecurity, and cyber capability architectures.
- The CMO is responsible for management of the department's enterprise business operations and shared services.

For more information about the CFO, CIO, and CMO roles and responsibilities for the department's financial management systems, see appendix III.

DOD Cannot Demonstrate That Data Supporting Financial Statements Are Reliable

Federal standards on internal control call for management to use and communicate quality information to achieve an entity's objective.³⁸ According to the standards, management should have accurate and complete information for decision-making, such as reliable financial statements that are produced using financial management systems with reliable data. In addition, DOD's financial statements should be prepared and fairly presented, in all material respects, in accordance with generally accepted accounting principles, which are promulgated for federal entities by the Federal Accounting Standards Advisory Board (FASAB).³⁹

Financial statement audits conducted by the DOD OIG and IPAs in fiscal year 2019 indicate that DOD could not demonstrate that the data produced by the department's financial management systems were reliable. Specifically, in January 2020, the DOD OIG reported that DOD had wide-ranging weaknesses in its financial management systems that prevented the department from collecting and reporting financial and performance information that was accurate, reliable, and timely.⁴⁰ Based in part on this finding, the DOD OIG issued a disclaimer of opinion on DOD's fiscal year 2019 department-wide basic financial statements.⁴¹

When combined, the disclaimers of opinion issued by the IPAs that audited each of the military services' fiscal year 2019 financial statements were material to the DOD Agency-Wide Basic financial statements. As a result, the DOD OIG was unable to obtain sufficient, appropriate audit

³⁸GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#), (Washington, D.C.: September 2014).

³⁹FASAB was established by agreement between GAO, OMB, and Treasury, which have adopted its standards and other pronouncements as applicable to federal entities, under their respective legal authorities. Further, the American Institute of Certified Public Accountants has recognized FASAB as the accounting standards-setting body for federal government entities. The *FASAB Handbook of Accounting Standards and Other Pronouncements, as Amended* is the most up-to-date, authoritative source of generally accepted accounting principles developed for federal entities.

⁴⁰Department of Defense Office of Inspector General, *Understanding the Results of the Audit of the DOD FY 2019 Financial Statements* (Alexandria, VA: Jan. 28, 2020).

⁴¹A disclaimer means that the DOD OIG was unable to express an opinion because of a lack of sufficient appropriate evidence to provide a basis for an audit opinion.

evidence for an audit opinion.⁴² The IPAs cited numerous financial management system and other IT-related deficiencies. Additionally, the DOD OIG and IPAs reported that DOD, including the military services, was not fully compliant with the FMFIA or FFMIA. The lack of financial management system integration and reconciliation prevented management from obtaining timely, accurate, and reliable information on the results of its business operations.

The DOD OIG has reported several material weaknesses, which are based, in part, on numerous financial and IT NFRs issued by the IPAs to the military services. These financial and IT NFRs report issues that hinder or limit DOD's and the military services' ability to present financial statements in accordance with generally accepted accounting principles. Further, for the fiscal year 2019 financial statement audit, IPAs reissued approximately 75 percent of the financial and IT NFRs to the military services that had been issued for the fiscal year 2018 financial statement audit, but were not remediated by military services within the next fiscal year.⁴³

Reported Material Weaknesses Limit Financial Data Reliability

In January 2019, the DOD OIG reported 20 material weaknesses that impacted DOD's ability to achieve an unmodified audit opinion on its fiscal year 2018 department-wide financial statements.⁴⁴ These material weaknesses were based, in part, on approximately 1,400 financial and IT NFRs issued by the IPAs to the military services based on their fiscal year 2018 financial statement audits.

More recently, in January 2020, the DOD OIG reported 25 material weaknesses that impacted DOD's ability to achieve an unmodified audit

⁴²Audit evidence is all the information used by the auditor in arriving at the conclusions on which the audit opinion is based and includes the information contained in the accounting records underlying the financial statements and other information. Auditors are not expected to examine all information that may exist. Audit evidence, which is cumulative in nature, includes evidence obtained from audit procedures performed during the course of the audit and may include evidence obtained from other sources, such as previous audits and a firm's quality control procedures for client acceptance and continuance.

⁴³The approximate 75 percent reissue rate of financial and IT NFRs at the military services was calculated as follows: 1,067 NFRs (543 financial and 524 IT) reissued for 2019 total compared to the 1,405 total NFRs at the military services for 2018 is approximately 75 percent.

⁴⁴Department of Defense Office of Inspector General, *Understanding the Results of the Audit of the DOD FY 2018 Financial Statements* (Alexandria, VA: Jan. 8, 2019).

opinion on its fiscal year 2019 department-wide financial statements.⁴⁵ These material weaknesses were based, in part, on approximately 2,100 financial and IT NFRs issued by the IPAs to the military services based on their fiscal year 2019 financial statement audits. The increase in material weaknesses and NFRs for fiscal year 2019 occurred for several reasons, of which the most common related to auditors (1) performing expanded testing, which resulted in new findings that led to additional material weaknesses, and (2) presenting material weaknesses at a more granular level.

These material weaknesses have a direct impact on DOD's ability to present financial statements in accordance with generally accepted accounting principles. The material weaknesses reported by the DOD OIG included, but are not limited to, the following audit areas:

- **Universe of transactions.** DOD was unable to provide a complete universe of transactions that reconciled to its accounting records.
- **Entity-level controls.** DOD did not design and implement effective entity-level controls to establish an internal control system that would support reliable financial reporting.
- **Unsupported Accounting Adjustments.** DOD did not have effective control to provide reasonable assurance that accounting adjustments were valid, complete, and accurately recorded in its accounting and general ledger systems.⁴⁶
- **Oversight and monitoring.** DOD did not perform effective oversight and monitoring of the consolidation of the component-level information or have adequate time to perform verification of the component-level information.
- **Financial management systems and information technology.** DOD had wide-ranging weaknesses in financial management systems that prevented the department from collecting and reporting that financial and performance information was accurate, reliable, and timely.

⁴⁵Department of Defense Office of Inspector General, *Understanding the Results of the Audit of the DOD FY 2019 Financial Statements* (Alexandria, VA: Jan. 28, 2020).

⁴⁶GAO, *Department of Defense: Actions Needed to Reduce Accounting Adjustments*, [GAO-20-96](#), (Washington, D.C.: Jan. 10, 2020).

-
- **Accounts payable.** DOD did not have sufficient policies, procedures, and internal controls to properly record accounts payable transactions.

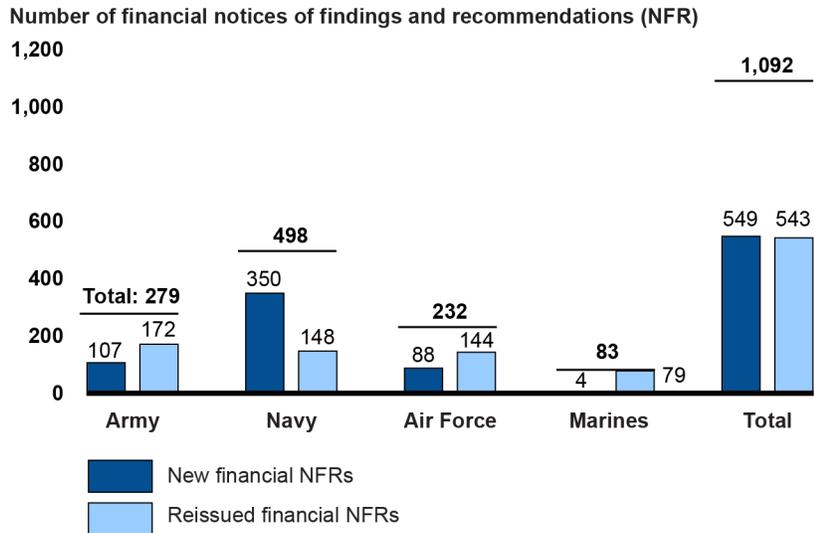
As noted previously, these material weakness are based, in part, on numerous financial and IT NFRs issued by IPAs in connection with their audits of the military services' fiscal year 2019 financial statements. Understanding the nature and extent of these NFRs and how they limit the reliability of DOD financial management system data is essential to the department in developing and implementing corrective actions to remediate the NFRs.

Issues Identified in Financial Audit Findings Impact Financial Data Reliability

Financial NFRs report financial issues that limit the department's ability to present financial statements in accordance with generally accepted accounting principles. Of the 2,100 NFRs that the IPAs issued to the military services for fiscal year 2019, 1,092 (52 percent) were related to financial issues. Of these 1,092 NFRs, 549 were new and 543 were reissued from previous years.⁴⁷ These new and reissued financial NFRs resulted from the IPAs' fiscal year 2019 audits of the military services' general funds and working capital funds. The numbers of financial NFRs issued to the military services for fiscal year 2019 are shown in figure 3.

⁴⁷New NFRs could include consolidated NFRs from prior years. Specifically, new NFRs issued during the fiscal year 2019 audit may have consolidated several NFRs from prior years. NFRs are considered reissued if the weakness or inefficiency noted in the NFR was identified during a prior year audit, but which had not yet been corrected. New and reissued NFRs were determined by the DOD OIG and IPAs.

Figure 3: Financial Notices of Findings and Recommendations Issued by Independent Public Accountants, Based on Audits of the Military Services' Fiscal Year 2019 Financial Statements



Source: Department of Defense Office of Inspector General. | GAO-20-252

Note: New NFRs could include consolidated NFRs from prior years. New NFRs issued during FY 2019 may have consolidated several NFRs from prior years. NFRs are considered reissued if the weakness or inefficiency noted in the NFR was identified during a prior year audit, but had not yet been corrected. New and reissued NFRs were determined by the DOD Office of Inspector General (OIG) and independent public accountants.

Based on our review of the condition statements in the financial NFRs delivered to the military services, we categorized the NFRs into four issue areas:

Internal control, which comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the entity. Internal control helps an entity run its operations efficiently and effectively, report reliable information about its operations, and comply with applicable laws and regulations. Internal control also serves as the first line of defense in safeguarding assets. NFRs categorized in this issue area report deficiencies in internal control and are not identified in the other categories.

Accounting policies and procedures, which are controls that management establishes to achieve objectives and respond to risks in the internal control system, including the entity's information systems. NFRs

categorized in this issue area report deficiencies in accounting policies and procedures.

Reconciliation and integration of financial management systems, which reasonably assure that the entire population of financial transactions has been recorded in the financial statements. The lack of an integrated system prevents management from obtaining timely, accurate, and reliable information on the results of its business operations. NFRs categorized in this issue area report deficiencies in financial management systems reconciliation and integration.

Financial statement preparation, which consists of processes and internal controls to reasonably assure that complete and accurate component financial statements, including related note disclosures, are prepared prior to the compilation of the agency-wide annual financial report. NFRs categorized in this issue area report deficiencies in preparing the financial statements.

Table 2 details the number of issues by categories found for the financial NFRs issued by the IPAs in the fiscal year 2019 audits for the military services.

Table 2: Number of Issues Contained in the Fiscal Year 2019 Military Services' Financial Notices of Findings and Recommendations (NFR)

NFR Category	Army		Navy		Air Force		Marine Corps		Totals		Percent of Total NFRs	
	New	Reissued	New	Reissued	New	Reissued	New	Reissued	New	Reissued	Total	
Internal control ^a	76	136	283	99	56	99	3	59	418	393	811	75
Accounting policies and procedures ^b	15	17	45	27	7	4	1	6	68	54	122	11
Reconciliation and integration of financial management systems	3	7	12	19	15	17	0	8	30	51	81	7
Financial statement preparation	0	0	4	3	3	5	0	6	7	14	21	2
Other ^c	13	12	6	0	7	19	0	0	26	31	57	5
Total	107	172	350	148	88	144	4	79	549	543	1092	100

Source: GAO analysis of information provided by DOD military services' independent public accountants. | GAO-20-252

Note: New NFRs could include consolidated NFRs from prior years. New NFRs issued during FY 2019 may have consolidated several NFRs from prior years. NFRs are considered reissued if the weakness or inefficiency noted in the NFR was identified during a prior year audit, but had not yet been corrected. New and reissued NFRs were determined by the DOD Office of Inspector General and independent public accountants.

^aFor example, Army management needs to improve entity level controls to establish an internal control system that will produce reliable financial reporting. These entity level control improvements are needed in the control environment, risk assessment, information and communication, and monitoring areas.

^bFor example, as a result of the Navy's non-compliance with the Support Statement of Federal Financial Accounting Standards (SFFAS) 48, the Inventory and Related Property line item on the financial statements and the footnote may be misstated. The Navy has not adequately implemented a consistent approach to evaluate valuation packages to enable proper comparison.

^cOther NFRs could include NFRs identified as related to classified or sensitive activities or not provided by the military services for review.

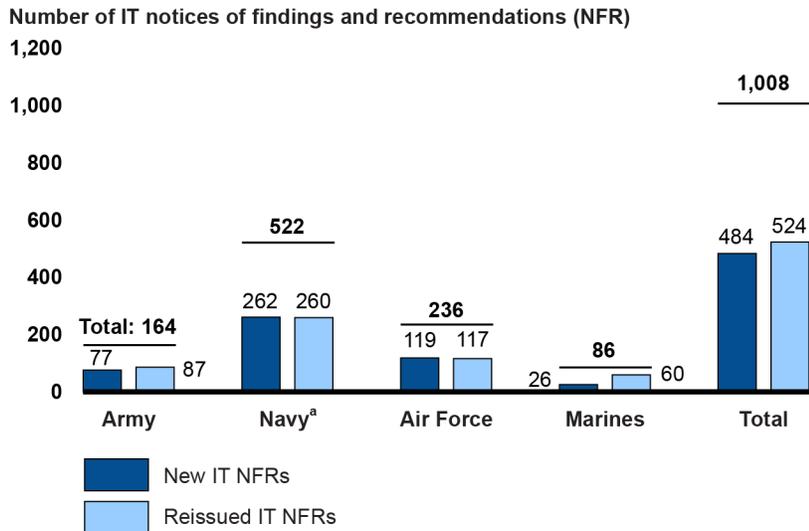
As noted in table 2, of the 1,092 issues identified in the fiscal year 2019 new and reissued financial NFRs, most (811 issues, or 75 percent) related primarily to the military services' internal control. More specifically, a number of these were related to the military services' lack of controls to validate that financial transactions were completely and accurately reported in the financial statements. In addition, as noted in the table, issues were identified for all of the military services related to the deficiencies in internal control and accounting policies and procedures.

Overall, as noted in the table, the Army accounted for 279 total issues (25 percent); the Navy accounted for 498 total issues (46 percent); the Air Force accounted for 232 total issues (21 percent); and the Marine Corps accounted for 83 total issues (8 percent).

Issues Identified in Information Technology Audit Findings Impact Financial Data Reliability

IT NFRs report IT and cybersecurity issues that limit the department's ability to present financial statements in accordance with generally accepted accounting principles. Of the 2,100 NFRs that the IPAs issued to the military services for fiscal year 2019, 1,008 (48 percent) were related to IT and cybersecurity issues. Of these 1,008 NFRs, 484 were new and 524 were reissued from previous years. These IT NFRs resulted from the IPAs' fiscal year 2019 audits of the military services' general funds and working capital funds. The numbers of IT NFRs issued to the military services for fiscal year 2019 are shown in figure 4.

Figure 4: Information Technology (IT) Notices of Findings and Recommendations Issued by Independent Public Accountants, Based on Audits of the Military Services' Fiscal Year 2019 Financial Statements



Source: Department of Defense Office of Inspector General. | GAO-20-252

Note: New NFRs could include consolidated NFRs from prior years. New NFRs issued during fiscal year 2019 may have consolidated several NFRs from prior years. NFRs are considered reissued if the weakness or inefficiency noted in the NFR was identified during a prior year audit, but had not yet been corrected. New and reissued NFRs were determined by the DOD Office of the Inspector General and independent public accountants.

^aIn FY 2019, the Navy's FY 2019 Working Capital Fund Financial Statements includes U.S. Marine Corps financial information.

Based on our review of the IT NFRs delivered to the military services, we identified 1,414 issues.⁴⁸ We grouped the issues into seven issue areas, based on control categories contained in GAO's FISCAM as follows:⁴⁹

Access controls, which provide reasonable assurance that access to computer resources (data, equipment, and facilities) is restricted to authorized individuals. Access control policies and procedures should be formally developed, documented, disseminated, and periodically updated.

Security management, which provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning

⁴⁸Some of the NFRs addressed multiple issues. Therefore, the number of issues is greater than the number of NFRs.

⁴⁹[GAO-09-232G](#).

responsibilities, and monitoring the adequacy of the entity's computer-related controls. It involves reasonably assuring that data, reports, and other outputs are safeguarded against unauthorized access; that information is safeguarded against improper modification or destruction; and that data, reports, and other relevant information are readily available to users when needed.

Configuration management, which prevents unauthorized changes to information system resources (for example, software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended. This involves the identification and management of security features for all hardware, software, and firmware components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle.

Segregation of duties, which provides reasonable assurance that incompatible duties are effectively segregated through formal operating procedures, supervision, and review.

Interface controls, which include controls over the timely, accurate, and complete processing of information between applications and other feeder and receiving systems on an on-going basis, and the complete and accurate migration of clean data during conversion. Interfaces result in the structured exchange of data between two computer applications.

Business process controls, which are automated and/or manual controls applied to business transaction flows. These controls relate to the completeness, accuracy, validity, and confidentiality of transactions and data during application processing. They typically cover the structure, policies, and procedures that operate at a detailed business process (cycle or transaction) level and operate over individual transactions or activities across business processes.

Contingency planning, which includes controls to ensure that when unexpected events occur, critical operations continue without disruption or are promptly resumed and critical and sensitive data are protected. Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an entity's ability to accomplish its mission. If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information.

Table 3 details the number of issues, by FISCAM IT control category, that we found in the IT NFRs that IPAs issued in the fiscal year 2019 audits for the military services.

Table 3: Number of Issues Contained in the Fiscal Year 2019 Military Services' Information Technology (IT) Notices of Findings and Recommendations (NFR)

IT Control Category per FISCAM	Army		Navy		Air Force		Marine Corps		Totals		Percent of Total Issues	
	New	Reissued	New	Reissued	New	Reissued	New	Reissued	New	Reissued		Totals ^a
Access ^b	52	73	171	172	68	82	16	23	307	350	657	46
Security management ^c	10	15	79	91	26	23	5	29	120	158	278	20
Configuration management	8	12	64	37	26	25	4	12	102	86	188	13
Segregation of duties	5	16	47	52	15	33	3	8	70	109	179	13
Interface	0	0	24	37	2	9	1	3	27	49	76	5
Business process	1	0	12	9	0	3	0	2	13	14	27	2
Contingency planning	1	0	0	0	0	1	1	6	2	7	9	1
Total	77	116	397	398	137	176	30	83	641	773	1414	100

Source: GAO analysis of NFRs provided by the Department of Defense. | GAO-20-252

Note: New NFRs could include consolidated NFRs from prior years. New NFRs issued during fiscal year 2019 may have consolidated several NFRs from prior years. NFRs are considered reissued if the weakness or inefficiency noted in the NFR was identified during a prior year audit, but had not yet been corrected. New and reissued NFRs were determined by the DOD Office of Inspector General (OIG) and independent public accountants

^aSome of the NFRs addressed multiple issues. Therefore, the number of issues presented is greater than the number of NFRs.

^bFor example, access to Navy systems was not always restricted to authorized users and was not assigned in accordance with the principle of least privilege. Least privilege is the principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of a system. Also, multiple systems had a significant number of administrator users (i.e., database administrators, developers) who were able to complete an entire functional process by inputting, processing, and approving transactions. Weaknesses in access controls can compromise the integrity of sensitive data and increase the risk that such data may be inappropriately used and/or reported.

^cFor example, Air Force management did not have documented policies and procedures related to management's review of the service provider's reports and activities. Without policies and procedures in place to review third-party services, the risk increases that inappropriate activity or transactions performed by third parties would not be identified for resolution.

As noted in table 3, of the 1,414 issues identified in the fiscal year 2019 new and reissued IT NFRs, most related primarily to the military services' access controls (657 issues, or 46 percent). In addition, as noted in the

table, the Army accounted for 193 total issues (14 percent); the Navy accounted for 795 total issues (56 percent); the Air Force accounted for 313 total issues (22 percent); and the Marine Corps accounted for 113 total issues (8 percent).

DOD Plans to Address Audit Findings

DOD has efforts underway to address the NFRs by developing and implementing corrective action plans to remediate deficiencies identified by the auditors in fiscal year 2018. In January 2020, the DOD OIG reported that DOD had remediated approximately 26 percent of the military services' NFRs from fiscal year 2018. Specifically, the DOD OIG and IPAs validated that a total of 373 fiscal year 2018 NFRs had been remediated.⁵⁰ The auditors validated the closed NFRs based on a variety of reasons, including that the department took sufficient actions and the condition no longer existed; the condition no longer existed because the process or systems used were eliminated; or because the department accepted the risk associated with the condition.

The Office of the CFO has developed an NFR database, in which audit findings are uploaded. This database contains NFRs, corrective action plans,⁵¹ and the status of actions taken. The DOD OIG reported that the department uses this information to categorize and prioritize findings and corrective actions. The DOD OIG also reported that the department is currently focusing its remediation efforts on addressing deficiencies related to IT, real property, inventory and operating material and supplies, and government property in the possession of contractors.⁵²

In its June 2020 *Financial Improvement and Audit Remediation Report*,⁵³ DOD reported that in fiscal year 2020, the department will continue to develop and complete corrective actions using material weaknesses to

⁵⁰Department of Defense Office of Inspector General, *Understanding the Results of the Audit of the DOD FY 2019 Financial Statements* (Alexandria, VA: Jan. 28, 2020).

⁵¹According to OMB guidance, corrective action plans (CAPs) are plans developed by management to address the risk associated with a control deficiency. An Agency's ability to correct control deficiencies is an indicator of the strength of its internal control environment. CAPs should include a root-cause analysis of the deficiency, a cost-benefit analysis, resources needed, responsible personnel for completing CAPs, and critical path milestones. See OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 15, 2016.

⁵²Department of Defense Office of Inspector General, *Fiscal Year 2020 Top DOD Management Challenges* (Alexandria, VA: Oct. 15, 2019).

⁵³Office of the Under Secretary of Defense (Comptroller), *Financial Improvement and Audit Remediation (FIAR) Report*, June 2020.

prioritize corrective actions. In addition to the audit priorities listed above, remediation work will focus on four additional priorities: (1) Fund Balance with Treasury, (2) financial reporting internal controls, (3) Joint Strike Fighter Program, and (4) audit opinion progression.

We are not making recommendations related to the reliability of information in DOD's financial systems because the department is taking steps to address the NFRs identified by the DOD OIG and IPAs. Moving forward, it will be important for DOD to address the NFRs in order to improve the reliability of its financial statements.

DOD and the Military Services Lack Comprehensive Plans for Improving Financial Management Systems

DOD has a financial management systems strategy that is aligned with the department's overall business operations strategy and has results-oriented goals to improve its financial management systems environment. However, the department has not established measures to determine if its strategy is succeeding. DOD also does not have an enterprise road map to implement its financial management systems strategy. In addition, the military services do not have detailed plans for migrating legacy financial systems to new systems. Moreover, while DOD has a plan to address IT issues identified in its audit, it lacks performance goals to effectively monitor the status of remediating issues.

DOD Has a Strategy to Improve Its Financial Management Systems Environment, but Lacks Measures to Determine if the Strategy is Succeeding

Leading practices from OMB guidance and prior GAO research and experience reviewing federal agencies' IT strategic plans demonstrate that an agency should have a comprehensive and effective IT strategic

plan.⁵⁴ The plan should (1) be aligned with the agency's overall strategy; (2) identify results-oriented goals and performance measures that permit the agency to determine whether implementation of the plan is succeeding; (3) identify strategies that the agency intends to use to achieve desired results; and (4) provide descriptions of interdependencies within and across projects so that they can be understood and managed. Related to identifying performance measures, the agency should document targets and time frames and how it intends to accurately and reliably measure progress toward its strategic goals.⁵⁵

Of these four elements of a comprehensive and effective IT strategic plan, DOD's financial management systems strategy addresses three elements and partially addresses one element. Specifically, the strategy is aligned with DOD's overall strategic plan, identifies strategies the department intends to use to achieve desired results, and describes dependencies within and across projects. In addition, the strategy includes results-oriented goals. However, it does not include performance measures to determine whether the plan is succeeding.

Table 4 provides GAO's ratings of how DOD's financial management systems strategy, which is documented in its financial management functional strategy and the associated military services' organizational execution plans (OEP), compared to a comprehensive and effective IT strategic plan.

⁵⁴OMB, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11 (June 2018); *Managing Information as a Strategic Resource*, Circular No. A-130 (July 28, 2016); *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management*, Memorandum M-13-09 (Mar. 27, 2013); Federal Enterprise Architecture Framework Version 2 (Washington, D.C.: Jan. 29, 2013; and *The Common Approach to Federal Enterprise Architecture* (May 2, 2012); and GAO, *Social Security Administration: Improved Planning and Performance Measures are Needed to Help Ensure Successful Technology Modernization*, [GAO-12-495](#) (Washington, D.C.: April. 26, 2012); *Defense Business Transformation: Status of Department of Defense Efforts to Develop a Management Approach to Guide Business Transformation*, [GAO-09-272R](#) (Washington, D.C.: Jan. 9, 2009); *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses*, [GAO-15-315](#) (Washington, D.C.: Mar. 31, 2015); and *NASA Information Technology: Urgent Action Needed to Address Significant Management and Cybersecurity Weaknesses*, [GAO-18-337](#) (Washington, D.C.: May 22, 2018).

⁵⁵OMB, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11 (June 2018) and *Managing Information as a Strategic Resource*, Circular No. A-130 (July 28, 2016).

Table 4: GAO Ratings of IT Strategic Plan Requirements Compared to DOD’s Financial Management Systems Strategy

IT Strategic Plan Requirements ^a	GAO Ratings
Alignment with the agency’s overall strategic plan	●
Results-oriented goals and performance measures to determine whether implementation of the plan is succeeding.	◐
Strategies the agency will use to achieve desired results, including providing a clear narrative of how IT is enabling agency goals.	●
Descriptions of dependencies within and across projects	●

Legend:

- Fully addressed: DOD provided evidence that it fully addressed this requirement.
- ◐ Partially addressed: DOD provided evidence that it addressed some, but not all, of this requirement.

Source: GAO analysis of Department of Defense documentation. | GAO-20-252

^aThe requirements for a comprehensive and effective IT strategic plan are based on Office of Management and Budget guidance and prior GAO research and experience at federal agencies.

DOD’s financial management systems strategy is aligned with the department’s overall strategic plan. The department has an overall strategic objective to undergo an audit and improve the quality of budgetary and financial information, and a related priority goal, which is to complete yearly audits, gain actionable feedback, and remediate findings toward achieving a positive audit opinion.⁵⁶ The financial management functional strategy includes a goal to enhance and implement financial policies and processes to improve, simplify, and standardize the financial management business and systems environment. That strategy also identifies a related objective, which is to improve and standardize business processes and data for decision-making.

In addition, DOD fully addressed the element requiring its financial management systems strategic plan to document the strategies the department intends to use to achieve desired results. For example, the department’s goal to enhance and implement financial policies and processes to improve, simplify, and standardize the financial management business and systems environment has a related objective,

⁵⁶Department of Defense, *FY 2018-FY 2022 National Defense Business Operations Plan*, April 9, 2018, *FY 2018-FY 2022 National Defense Business Operations Plan Appendices*, and *Fiscal Year (FY) 2020 Annual Performance Plan & FY 2018 Annual Performance Report*, Feb. 22, 2019.

which is to simplify the financial management information technology business systems and interface environment. The strategy identifies the approaches the department intends to use to achieve the desired results, such as retiring legacy systems and leveraging existing financial management target system capabilities to consolidate systems with duplicative and similar capabilities.

DOD has also addressed the element requiring its financial management systems strategy to identify dependencies within and across projects. Specifically, the financial management functional strategy initiative titled Financial Management Information Technology Systems Environment identifies such dependencies. The initiative's purpose is to reduce the number of legacy financial management systems by investing in current enterprise resource planning systems and target financial management systems.⁵⁷ The initiative identifies the implementation of direct Treasury disbursements and intragovernmental transactions as dependencies.⁵⁸

In addition, the military services' financial management OEPs demonstrated that projects link to the strategy and dependencies and risks have been identified. For example, the Army OEP identifies systems that are linked to the Financial Management Information Technology Systems Environment initiative. It also documents dependencies and risks. For example, the OEP documents a risk to reducing the cost of financial management operations. The risk is that, if interfaces are not replaced or subsumed, the result will be, among other things, additional system integration complexity. According to the OEP, in order to mitigate this risk, the Army will continue to replace the number of interfaces by reducing the need for legacy financial management systems and non-Army financial management domain systems.

However, DOD did not fully address the element requiring that an IT strategic plan include results-oriented goals and performance measures that permit the department to determine whether plan implementation is succeeding. The financial management functional strategy documents results-oriented goals and includes expected business outcomes and possible success indicators related to the goals. For example, for its goal

⁵⁷The February 2019 DOD Financial Management Functional Strategy documents 12 financial management enterprise initiatives.

⁵⁸Intragovernmental Transactions is a financial management initiative intended to properly account for, reconcile, and eliminate intragovernmental transaction imbalances from the consolidated financial statements.

to enhance and implement financial policies and processes to improve, simplify, and standardize the financial management business and systems environment, the strategy documents associated business outcomes, which include

- reduced reconciliation work
- supportable transactions
- stronger internal controls
- timely, accurate and reliable financial data
- improved interoperability between systems
- end-to-end funds traceability between budget and expenditures
- a cost effective business environment

The strategy also identifies 12 possible success indicators, including percent reduction of legacy financial management business systems, associated with the goal.

Another goal documented in the strategy is to achieve a sustainable unmodified audit opinion by improving financial processes, controls, and information via audit remediation. To achieve this goal, the strategy documents associated business outcomes, which include

- auditable business environment
- timely, accurate, and reliable property, inventory, and financial data for decision-makers
- supportable transactions (eliminations)
- reduced reconciliation work
- improved interoperability between systems
- stronger internal controls
- strengthened mission capabilities
- enhanced stewardship and public trust
- unmodified audit opinion

The strategy further identifies 20 possible success indicators associated with this goal, including percent of NFRs closed, percent of unsupported journal vouchers, and percent of DOD organizations that have achieved an unmodified audit opinion.

However, DOD is not using its documented success indicators to measure progress toward achieving its goals. In this regard, it has not documented targets and time frames to define the level of performance to be achieved. The department also has not documented how it plans to measure expected outcomes, such as by identifying data sources, how it intends to measure values, and how it will verify and validate values that it does measure.

Officials in the Office of the CFO explained that they are not using indicators, targets, and time frames because they believe that measuring remediated NFRs is sufficient. Specifically, they said that, to measure success in achieving the goals in the financial management functional strategy, DOD is measuring the number of remediated NFRs and the number of unmodified audit opinions. While the department's fiscal year 2020 Annual Performance Plan includes the percentage of NFR conditions closed as a performance measure with annual targets, the performance measure is not documented in the department's financial management functional strategy.⁵⁹

Furthermore, measuring the percentage of NFRs closed does not indicate how DOD is making progress relative to its goal to enhance and implement financial policies and processes to improve, simplify, and standardize the financial management business and systems environment. This goal, which is described in its financial management functional strategy, has business outcomes and potential success indicators aligned with it. However, the indicators are only provided as examples that could be used to measure success and are not metrics the department is using to evaluate progress towards the goal. Without fully and consistently documented performance measures, DOD cannot adequately measure its progress in achieving the planned business outcomes associated with its financial management systems goals.

DOD Does Not Have an Enterprise Road Map to Implement its Financial Management Systems Strategy

According to OMB guidance, DOD should have an enterprise road map to implement its financial management systems strategy. An enterprise road map is an integrated plan that documents the current and future states of a business and systems environment at a high level, from an architecture perspective, and presents a transition plan for moving from the current to

⁵⁹The number or percent of DOD organizations achieving unmodified audit opinions is not a performance measure in DOD's annual performance plan or its financial management functional strategy.

the future in an efficient, effective manner.⁶⁰ Such a road map should discuss performance gaps, resource requirements, and planned solutions, and it should map the strategy to projects and budget. The road map should document the tasks, time frames, and milestones for implementing new solutions. In addition, it should contain an inventory of systems.⁶¹

In addition, Congress recently passed legislation that includes requirements that are similar to OMB's guidance for an enterprise road map. Specifically, the National Defense Authorization Act (NDAA) for Fiscal Year 2020 requires DOD to develop and maintain a plan known as the Defense Business Systems Audit Remediation Plan.⁶² The plan is to include a current accounting of defense business systems that will be introduced, replaced, updated, modified, or retired in connection with the full financial statement audit. The plan is also to include a comprehensive road map that displays

- in-service, retirement, and other pertinent dates for affected systems
- cost estimates for each affected system;
- dependencies between the various systems; and
- dependencies between the introduction, replacement, update, modification, and retirement of such systems.

DOD was to submit its first report to Congress on the plan by June 30, 2020, and annually, thereafter, the department is to provide an updated report. In addition, the department is to provide semi-annual briefings on the status of the plan.

⁶⁰Enterprise architecture is intended to provide a clear and comprehensive picture of a functional or mission area that cuts across more than one organization. It describes the enterprise in logical terms (such as interrelated business processes and business rules, information needs and flows, and work locations and users), as well as in technical terms (such as hardware, software, data, communications, security attributes, and performance standards).

⁶¹OMB, *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management*, Memorandum M-13-09 (Washington, D.C.: Mar. 27, 2013); *Federal Enterprise Architecture Framework* Version 2, Jan. 29, 2013; and *The Common Approach to Federal Enterprise Architecture*, May 2, 2012; and *FY 2019 IT Budget – Capital Planning Guidance*, August 1, 2017.

⁶²Pub. L. No. 116-92, § 1002, 133 Stat. 1198, 1570 (Dec. 20, 2019).

DOD has a business enterprise architecture that includes content describing aspects of the current and target business system environments and a transition plan to get from the current to the target environment. For example, the DOD IT Portfolio Repository (which includes data the department considers to be part of its business enterprise architecture) includes business system attributes, such as

- whether a system is a legacy system (i.e., is to be terminated in less than 3 years from the end of the current fiscal year) or is a core system (i.e., is to be terminated in more than 3 years from the end of the current fiscal year);
- what the target systems are for legacy system migration;
- whether migration is planned to be full or partial;
- what users or functions are not migrating with the system if a partial migration is planned; and
- when the migration will be completed.

The military services and other DOD entities use this information to develop high-level diagrams that show the year when their respective legacy financial management systems are planned to migrate to target systems.⁶³

In addition, the department has taken steps to develop a Defense Business Systems Audit Remediation Plan, in accordance with the NDAA for Fiscal Year 2020. For example, in its June 2020 report to Congress, the department identified an inventory of audit-relevant systems from its FIAR Systems Database, and a list of interfacing systems for these systems. In addition, the plan identified a list of 48 legacy business systems planned for retirement in fiscal years 2020 through 2024, and their retirement dates.

However, DOD does not have an integrated cohesive department-wide plan, such as an enterprise road map, for its financial management business and systems environment. Specifically, it has not updated the Enterprise Roadmap that it submitted to OMB in March 2014 to include its financial management business and systems environment. It also has not

⁶³These high-level diagrams are called SV-8s. An SV-8 is one of several systems viewpoint models included in the DOD Architecture Framework that department components use to develop their architectures.

yet developed a road map in accordance with the NDAA for Fiscal Year 2020.

In March 2014, the DOD CIO submitted the department's Enterprise Roadmap for 2013 to 2014 to OMB. The road map focused primarily on the department's Joint Information Environment, which was DOD's initiative to consolidate information technology infrastructure to improve mission effectiveness, achieve savings, and improve network security. However, the road map did not address improving the department's financial management business and systems environment. According to the CIO's memo transmitting the road map to OMB, future versions are expected to expand the scope to address the broader range of IT from both the enterprise and DOD component perspectives. However, as of June 2020, the department had not developed an updated road map that includes its financial management systems environment.

The department did not explain why it had not updated its enterprise road map. In response to our request for the reason that it had not yet produced an enterprise road map that includes its financial management systems environment, and the status of an updated enterprise road map, the Director, Architecture and Engineering, in the office of the DOD CIO, provided a written response. According to the response, the Office of the CIO was in the process of updating its information enterprise architecture, and planned to provide the first increment of version 3 of the architecture to Congress. However, the official did not provide the status of developing an enterprise road map that includes the department's financial management systems environment. Further, while the DOD CIO's January 2020 report to Congress on its updated information enterprise architecture described, among other things, plans related to integrating the department's information and business architectures, it did not include an enterprise road map that addresses the financial management business and systems environment.

In addition, while an official from the Office of the CFO agreed that it is important that the department take an integrated approach to improving its financial management systems environment, the official said that the department had questioned whether it would be cost effective. Specifically, the official said that integration needs to occur across silos and service providers to achieve an unmodified audit opinion, and DOD needs to find a way to manage this integration. The official added, however, that DOD officials had often discussed whether it was cost effective to create a chart of the department's business systems and determined that the return on investment was questionable. The official

estimated that it would cost \$4 million to \$5 million a year to create and maintain a chart of the department's approximately 1,900 defense business systems.

DOD has also not yet fully addressed the provisions in the NDAA for Fiscal Year 2020 for a Defense Business Systems Audit Remediation Plan. The department stated in its June 2020 report to Congress that it intends to develop a road map for its systems that addresses the provisions in the act. However, the department did not state when it plans to complete its road map.

According to OMB, it is particularly important that large agencies have an enterprise road map that documents the tasks, milestones, and time frames for implementing a new systems environment because such agencies are likely to have many new development, modernization, retirement, and migration projects underway that require coordination to establish the optimal sequencing of activities. Further, the department could prioritize developing such a road map as part of the over \$800 million it already expects to spend annually on audits, audit support, and remediation in fiscal years 2019 through 2022.

Until DOD develops an enterprise road map to implement its financial management systems strategy, the department will not be well-positioned to know about and reuse existing solutions and services, see dependencies between projects department-wide that require sequencing, make consistent decisions, and provide measurable results. In addition, the department risks focusing planned system improvements on short term actions that might not support its longer term goals.

DOD Does Not Have Detailed Plans for Migrating Critical Legacy Accounting Systems to New Systems

According to the Software Engineering Institute (SEI), an organization should develop a plan to migrate legacy system software to a new system, and the plan should be agreed to by affected stakeholders. Migration planning includes analyzing the needs of affected stakeholders to determine migration schedules, training requirements, and operational cutover to the new system; developing quantifiable measures of success for the migration effort; and identifying meaningful and measurable milestones to track progress. In addition, according to SEI, an organization should ensure that the scope of migration planning includes deployment, transition to full operational use, and phase out of affected

legacy systems.⁶⁴ Also, according to the fiscal year 2019 DOD Annual Financial Report, a legacy financial system is expected to have a retirement plan (i.e., a plan for migrating a legacy system to a new system and deactivating the legacy system) for the department's investment review process.⁶⁵

Based upon our review of the documentation provided by the Army, Navy and Air Force on its migration plans, DOD did not demonstrate that it had fully developed detailed plans for migrating some of its critical legacy accounting systems to new systems. Specifically,

- Army officials did not provide a documented detailed retirement plan for its legacy accounting systems, STANFINS and SOMARDS. In response to our request, they provided a brief overall description of their migration approaches for the two legacy accounting systems to GFEBS, the new accounting system. The Army's description did not provide any of the migration elements.
- Navy officials provided a high-level plan description of its approach to the retirement of its legacy accounting system, STARS to SABRS, an existing Marine Corps' system.⁶⁶ The plan identified key stakeholders. An associated project schedule listed milestones and tasks with start and end dates for each task. However, the plan did not describe training requirements or discuss quantifiable measures to track the migration progress.
- Air Force officials stated that they do not have a documented retirement plan for its legacy accounting system, GAFS-R.⁶⁷ They are still working on the transition of business lines from GAFS-R to DEAMS, the new accounting system.

⁶⁴Software Engineering Institute, *DOD Software Migration Planning*, CMU/SEI-2001-TN-012 (Pittsburgh, PA: August 2001). SEI is a nationally recognized, federally funded research and development center established at Carnegie Mellon University in Pittsburgh, Pennsylvania, to address software development issues.

⁶⁵Department of Defense, *Agency Financial Report: Fiscal Year 2019*, November 15, 2019.

⁶⁶Department of the Navy Financial Management Transformation, *STARS-FL System GL Consolidation and System Decommissioning Plan*, April 2020.

⁶⁷GAFS-R is owned by Defense Finance and Accounting Service (DFAS) but utilized by the Air Force.

Without detailed plans for migrating its legacy accounting systems to new financial management systems, the department may fail to address the material weaknesses identified in its financial statement audits. In addition, if the department proceeds to migrate without plans, it may experience cost increases and schedule delays because of deployment and interface issues.

DOD Has a Plan to Address IT Issues, but Lacks Performance Goals to Effectively Monitor the Issues' Remediation

The *Standards for Internal Control in the Federal Government* states that managers should evaluate internal control issues and remediate deficiencies.⁶⁸ Managers should also monitor the status of remediation efforts so that they are completed on a timely basis, with oversight from the oversight body. In addition, OMB guidance states that, in order to effectively monitor progress, performance goals should be established that include a performance indicator, a target, and a time frame.⁶⁹ A performance indicator is a metric that can be used to track progress toward a goal or target within a time frame.

DOD evaluated the issues identified in its IT NFRs and, in June 2019, developed a plan to begin to remediate the deficiencies. Specifically, DOD categorized IT NFRs into four tiers, by reporting entity, and developed a plan to begin to address the IT NFRs for Tier 1.⁷⁰ The department also established a detailed approach to prioritization and prioritized issues in the IT NFRs. The plan includes identifying near- and mid-term mitigation strategies for all Tier 1 enterprise-level IT NFRs. Specifically, the plan includes providing policy direction and guidance for enterprise-level mitigations and tracking to completion. The plan also specified that the DOD CFO and CIO are to receive weekly updates on the status of the efforts in the plan.

⁶⁸GAO-14-704G.

⁶⁹OMB, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11 (June 2018).

⁷⁰For audit purposes, each reporting entity was assigned to one of four tiers based on materiality. Tier 1 includes the military services and the Military Retirement Trust Fund; Tier 2 includes large defense agencies; Tier 3 includes mid-sized defense agencies; and Tier 4 includes the remaining defense agencies and funds.

DOD Issued Guidance to Address Access Control Issues, But Has Not Established Performance Goals to Effectively Monitor Remediation of IT Issues

Addressing access controls is the department's first priority. The DOD CIO, Acting CMO, and CFO issued a memorandum to department components on July 3, 2019, to guide efforts to address access control issues across the department, which the department determined was its first priority. The memorandum provided guidance for taking several short-term actions and stated that the actions for systems with current audit findings must be completed by July 12, 2019. The memorandum also stated that the actions described in it for all other systems subject to audit must be completed by September 30, 2019. The department monitored and reported progress on the actions required by the July 3, 2019, memorandum, which were for 244 systems, to DOD CMO, CFO, and CIO points of contact.

However, as of September 30, 2019, most system reporting entities had not responded to the memo. An official from the office of the CFO sent a reminder on September 30, 2019, to the reporting entities to complete the required actions. However, as of December 2019, the department had not updated its time frames for addressing the actions.

The department also monitored the number of total IT NFRs closed through weekly status updates. These updates include metrics, measures, and the status of IT NFR remediation efforts. For example, the September 20, 2019, status update reported that, as of September 19, 2019, there were a total of 1,307 IT NFRs, of which 1,265 NFRs were covered by corrective action plans. In addition, 162 IT NFRs had been closed by an independent public accountant.

However, the status updates did not report progress relative to targets and time frames. DOD did not establish a performance goal that includes a performance indicator, target, and time frame, to assess progress in addressing its IT NFRs. Specifically, the department's audit remediation plans and status updates did not define targets and time frames, or report progress relative to a target within a time frame to monitor remediation efforts for IT NFRs.

Officials in the Office of the CFO noted that part of the reason that DOD has not established a performance goal is that the NFRs vary widely and it can be challenging to establish targets and time frames for addressing them. However, DOD has already grouped the issues identified in its IT NFRs by priority levels, facilitating the establishment of appropriate performance goals.

Until DOD establishes performance goals for its IT NFR remediation efforts, which include targets, time frames, and performance indicators for tracking, and reports progress relative to targets and time frames, the department will be poorly positioned to monitor achievement of its remediation efforts and, thus, know if changes need to be made to its approach to ensure that the remediation efforts are completed on a timely basis.

DOD Does Not Know How Much It Spends on Financial Management Systems; GAO Calculated at Least \$2.4 Billion Annually, but Data Are Not Fully Reliable

Federal guidance on internal controls calls for management to use and communicate quality information to achieve an entity's objective.⁷¹ The guidance also stipulates that quality information includes data that are accurate and complete, and that management should have accurate and complete information for decision-making. Accurate and complete information on the magnitude of the funds spent on financial management systems is an important aspect of evaluating DOD's efforts and prioritizing resources to improve them and achieve an unmodified audit opinion.

DOD does not track how much it spends on its financial management systems portfolio. However, while the department does not track how much it spends on the financial systems and feeder systems supporting its financial statements, our analysis of IT system databases identified relevant systems and associated expenditures—albeit with some limitations.

Specifically, we calculated that the department spent at least \$2.4 billion, \$2.6 billion, \$2.5 billion, and \$2.7 billion in fiscal years 2016, 2017, 2018, and 2019, respectively, for its financial management systems. Additionally, we calculated that the department expects to spend at least \$2.8 billion in fiscal year 2020 on the systems included in its database of significant financial and feeder systems. Table 5 includes our calculations of the spending estimates and the percentages spent or planned to be spent on developing and modernizing and operating and maintaining the systems, for fiscal years 2016 through 2020.

This spending includes a total of about \$2.2 billion on seven new financial management systems and about \$427 million on 12 legacy accounting

⁷¹[GAO-14-704G](#).

systems in fiscal years 2016 through 2020.⁷² For detailed information on the specific spending by the seven new and 12 legacy accounting systems, see appendix IV.

Table 5: DOD Spending on Development and Modernization and Operations and Maintenance for Systems in DOD’s Financial Improvement and Audit Readiness (FIAR) System Database, Fiscal Years 2016-2020

Fiscal year	Financial management systems budget (in billions of dollars)	Development and modernization spending (percentage)	Operations and Maintenance spending (percentage)
2016	2.4	18	82
2017	2.6	17	83
2018	2.5	14	86
2019	2.7	15	85
2020	2.8	15	85

Source: GAO analysis of Department of Defense data. | GAO-20-252

Note: GAO calculated the reported spending for the significant financial and feeder systems included in DOD’s FIAR Systems Database, as of February 2019. GAO determined that the database did not include all DOD systems the department considers relevant to its financial statement audit.

However, we were not able to develop a complete calculation of the department’s annual spending. DOD uses a tool called the FIAR Systems Database to record information about systems that the department has identified as significant financial and feeder systems. We used the information in this tool to determine which systems to include in our analysis of the department’s annual spending. However, the list of 224 significant financial and feeder systems that the department provided to us from this database in February 2019 did not include all the systems that were relevant to the fiscal year 2018 audit. Specifically, we identified 45 systems that were relevant to the audit, according to IPA contracts, but were not included in the list of significant financial and feeder systems.⁷³

Further, DOD lacks a reliable way to identify a complete inventory of the financial and feeder systems it uses to prepare financial statements in its

⁷²Legacy accounting systems are systems that support the key functions of a military service’s financial management and are integral to the financial reporting process, which are planned to be decommissioned, retired, or replaced.

⁷³DOD’s contracts with the IPAs include a list of systems that the military services consider relevant to the audit.

budget data. While the department maintains multiple IT system databases, none of them identify the systems that are significant to the audit and their associated expenditures. Specifically, the department maintains the DOD Information Technology Portfolio Repository (DITPR) and Select and Native Programming-IT System (SNAP-IT), both of which identify systems that are categorized as financial management systems.⁷⁴ However, the financial management system category does not include systems that the department has placed in other categories, such as human resource and logistics, some of which are also used for financial management and support the development of DOD's financial statements.

DOD CFO officials agreed that it is not possible to reliably estimate the cost of the financial systems and feeder systems necessary to support the preparation of financial statements and achieve an unmodified audit opinion. Specifically, the officials stated that there is no code or indicator in DITPR or SNAP-IT that can be used to reliably identify these systems.

In the department's June 2020 report to Congress on its Defense Business Systems Audit Remediation Plan, the department stated that it plans to implement changes to DITPR, which is its authoritative repository for the department's IT systems. Specifically, it plans to transition data from the FIAR Systems Database to DITPR and designate which business systems are audit-relevant. However, the department did not state when it plans to implement these changes. In addition, as described in this report, the FIAR Systems Database does not provide a complete list of systems that support the development of DOD's financial statements.

Until the department establishes a reliable way to identify which of its systems are needed to support the preparation of financial statements, DOD is not able to accurately determine how much money it spends on these systems. This impedes the department's ability to effectively manage the portfolio of systems that supports managing its financial and asset information and achieving an unmodified audit opinion.

⁷⁴The DOD IT Portfolio Repository includes defense business system attributes such as DITPR ID, system name and acronym, unique investment identifier, and mission area domain, among other attributes. The Select and Native Programming-IT system is a database application used to collect and assemble information required in support of the IT budget request submitted to Congress. For example, it is used to generate DOD's *IT-1 Report*.

Without a complete and accurate systems inventory, the department risks not knowing whether expenditures on the many accounting and feeder systems contribute to the department's goals. This, in turn, means the department risks making potentially significant expenditures on systems that do not support the department's financial management goals.

Conclusions

The DOD OIG and independent auditors issued a disclaimer of opinion on DOD's fiscal year 2018 and 2019 agency-wide financial statements, largely based on long-standing issues related to the department's financial management systems and data. Because of these long-standing issues, the department faces challenges in ensuring accountability over its extensive resources and in efficiently and economically managing its assets and budgets.

To help improve its financial management systems environment, the department has developed a financial management systems strategy that addresses elements of a comprehensive and effective IT strategic plan. However, the department has not established measures to determine if it is succeeding in achieving its goals to improve its financial management systems. Without fully documented performance measures, the department cannot adequately measure its progress in achieving the planned business outcomes associated with its financial management systems goals.

The department also lacks an enterprise road map to implement its financial management systems strategy. Having an enterprise road map as called for by OMB and recently enacted legislation would allow the department to be better positioned to know of and reuse existing solutions and services, see dependencies between projects department-wide that require sequencing, make consistent decisions, and provide measurable results.

DOD also does not have sufficiently detailed plans for migrating certain critical legacy accounting systems to new systems. Without these plans, the department may fail to address the material weaknesses identified in its financial statement audits. In addition, if the department proceeds to migrate without plans, it may experience cost increases and schedule delays because of deployment and interface issues.

DOD has developed a plan to begin to address the IT and cybersecurity issues, but it lacks performance goals (including performance indicators, targets, and time frames) to effectively monitor the status of remediating the issues. By establishing performance goals for its remediation efforts,

which include targets, time frames, and performance indicators for tracking and reporting progress, the department will be better positioned to monitor achievement of its remediation efforts and know if changes need to be made to its approach.

Further, DOD does not track which of its systems are for financial management. This, in turn, impedes the department's ability to effectively manage the portfolio of systems that supports managing its financial and asset information and achieving an unmodified audit opinion.

We determined that the department spends billions of dollars annually on its financial management systems, including hundreds of millions of dollars aimed at developing and modernizing them. However, the department is making these expenditures without plans that are well-developed to help ensure that the systems will support DOD financial management activities and achieve an unmodified audit opinion. Some spending on system development and modernization is essential to maintain functioning systems and help ensure system security. However, without plans that effectively describe its target financial systems environment and how to get there, the department risks wasting funds on short-term fixes that might not effectively and efficiently support longer term department goals. Specifically, it risks developing systems that do not cost effectively help it collect and report accurate, reliable, and timely financial and performance information; ensure accountability over its resources; manage its assets and budgets efficiently and economically; and achieve an unmodified audit.

Recommendations for Executive Action

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

The Secretary of Defense should direct the Chief Management Officer and other entities, as appropriate, to establish measures to determine if the department is succeeding in achieving its goal to improve its financial management systems. Specifically, it should document targets and time frames to define the level of performance to be achieved. It should also document how DOD plans to measure expected outcomes by identifying data sources, how it plans to measure values, and how DOD plans to verify and validate measured values. (Recommendation 1)

The Secretary of Defense should direct the Chief Management Officer and other entities, as appropriate, to establish a specific time frame for developing an enterprise road map to implement its financial management systems strategy, and ensure that it is developed. The road

map should document the current and future states at a high level, from an architecture perspective, and present a transition plan for moving from the current to the future in an efficient, effective manner. The road map should discuss performance gaps, resource requirements, and planned solutions, and it should map DOD's financial management systems strategy to projects and budget. The plan should also document the tasks, time frames, and milestones for implementing new solutions, and include an inventory of systems. (Recommendation 2)

The Secretary of Defense should direct the Chief Management Officer and other entities, as appropriate, to develop detailed migration plans for the Air Force's General Accounting and Finance System-Reengineered, Navy's Standard Accounting and Reporting System, and Army's Standard Finance System and the Standard Operation and Maintenance Army Research and Development System. (Recommendation 3)

The Secretary of Defense should direct the Chief Management Officer and other entities, as appropriate, to establish performance goals that include performance indicators, targets and time frames, to monitor the status of efforts to address IT-related audit findings. (Recommendation 4)

The Secretary of Defense should direct the Chief Management Officer and other entities, as appropriate, to implement a mechanism for identifying financial management systems that support the preparation of the department's financial statements in the department's systems inventory and budget data, and identify a complete list of financial management systems. (Recommendation 5)

The Secretary of Defense should direct the Chief Management Officer and other entities, as appropriate, to ensure that the department limits investments in financial management systems to only what is essential to maintain functioning systems and help ensure system security until it implements the other recommendations in this report. (Recommendation 6)

Agency Comments and Our Evaluation

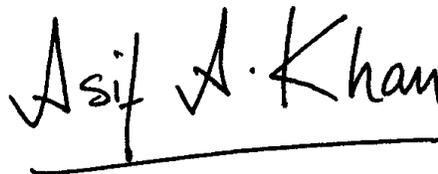
We received comments on a draft of this report from DOD. In its comments, the department stated that it concurred with our recommendations. Further, the department stated that it planned to work on improving its financial management systems environment by focusing on priority capability areas and taking various actions to reform business operations required to deliver these capabilities. The department's comments are reproduced in appendix V. DOD also provided technical comments, which we incorporated in the report, as appropriate.

We are sending copies of this report to the appropriate congressional committees; the Director, Office of Management and Budget; the Secretary of Defense; and other interested parties. This report also is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff members have any questions on matters discussed in this report, please contact Kevin Walsh at 202-512-6151 or walshk@gao.gov, or Asif Khan at 202-512-9869 or khana@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix VI.



Kevin Walsh
Director
Information Technology and Cybersecurity



Asif A. Khan
Director
Financial Management and Assurance

List of Requesters

The Honorable Michael B. Enzi
Chairman
The Honorable Bernard Sanders
Ranking Member
Committee on the Budget
United States Senate

The Honorable Jim Langevin
Chairman
The Honorable Elise M. Stefanik
Ranking Member
Subcommittee on Intelligence and Emerging Threats and Capabilities
Committee on Armed Services
House of Representatives

The Honorable Charles E. Grassley
United States Senate

The Honorable Ron Wyden
United States Senate

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine (1) to what extent the data produced by DOD's financial management systems are reported to be reliable for presenting financial statements in accordance with generally accepted accounting principles; (2) to what extent DOD and the military services have strategies and plans to address key information technology (IT) controls for their financial management systems; and (3) how much money DOD reports spending on developing and maintaining its financial management systems.

To determine to what extent the data produced by DOD's financial management systems are reported to be reliable for presenting financial statements in accordance with generally accepted accounting principles, we obtained and reviewed the notices of findings and recommendations (NFR) issued by the independent public accountants (IPA) as part of their fiscal year 2019 audit of DOD financial statements. In assessing the financial findings, we used the condition statements within each financial NFR to categorize the NFRs as (1) internal control; (2) accounting policies and procedures; (3) reconciliation and integration of financial systems; and (4) financial statement preparation. In assessing the information technology findings, we used the *Federal Information System Controls Audit Manual* (FISCAM).¹ We reviewed and summarized the NFRs by FISCAM category to identify the key issues limiting data reliability and financial management system security. We also reviewed the DOD OIG reports transmitting the results of the Army, Navy, Marine Corps, and Air Force audits.

To determine to what extent DOD and the military services have strategies and plans to address key information technology controls, we evaluated the department's documents describing its strategy for improving its financial management systems. We also determined whether the department had an enterprise road map to implement its strategy and whether the department had detailed plans for migrating critical legacy accounting systems to new financial systems. In addition, we evaluated the department's plans for addressing IT and cybersecurity issues identified in the department's financial statement audit.

To evaluate the department's strategy for improving its financial management systems, we obtained and reviewed DOD's February 2019 financial management functional strategy and the military services' fiscal

¹GAO, *Federal Information System Controls Audit Manual* (FISCAM), [GAO-09-232G](#) (Washington, D.C.: February 2009).

year 2019 organization execution plans, which the department said comprise its financial management systems strategy. We compared the strategy with elements of a comprehensive and effective IT strategic plan, which we derived from OMB guidance and our prior research and experience reviewing federal agencies IT strategic plans.² The elements of a comprehensive and effective IT strategic plan and how we evaluated DOD's strategy and plans relative to each of the elements follow:

- **Alignment with the agency's overall strategy.** We examined the extent to which DOD's strategy demonstrates how IT goals map to the department's relevant strategic objective identified in its National Defense Business Operations Plan, and Fiscal Year 2020 Annual Performance Plan.³ Specifically, we determined if the strategy mapped to the department's strategic objective to undergo an audit and improve the quality of budgetary and financial information, and the department's related priority goal, which is to complete yearly audits, gain actionable feedback, and remediate findings towards achieving a positive audit opinion.
- **Results-oriented goals and performance measures that permit the agency to determine whether implementation of the plan is succeeding.** We examined the plans to determine if they included results-oriented goals (i.e., expected outcomes) and performance measures that permit the department to determine whether it is succeeding. To determine if the department had performance measures that permit it to determine whether it is succeeding in achieving its goals, we examined the strategy to determine if it

²OMB, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11 (June 2018); *Managing Information as a Strategic Resource*, Circular No. A-130 (July 28, 2016); *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management*, Memorandum M-13-09 (Mar. 27, 2013); *Federal Enterprise Architecture Framework Version 2*, Jan. 29, 2013; and *The Common Approach to Federal Enterprise Architecture*, May 2, 2012; and GAO, *Social Security Administration: Improved Planning and Performance Measures are Needed to Help Ensure Successful Technology Modernization*, [GAO-12-495](#) (Washington, D.C., April. 26, 2012); *Defense Business Transformation: Status of Department of Defense Efforts to Develop a Management Approach to Guide Business Transformation*, [GAO-09-272R](#) (Washington, D.C.: Jan. 9, 2009); *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses*, [GAO-15-315](#) (Washington, D.C., Mar. 31, 2015); and *NASA Information Technology: Urgent Action Needed to Address Significant Management and Cybersecurity Weaknesses*, [GAO-18-337](#) (Washington, D.C.: May 22, 2018).

³Department of Defense, *FY 2018-FY 2022 National Defense Business Operations Plan*, April 9, 2018, *FY 2018-FY 2022 National Defense Business Operations Plan Appendices*, and *Fiscal Year (FY) 2020 Annual Performance Plan & FY 2018 Annual Performance Report*, Feb. 22, 2019.

documented targets and time frames and how the department will measure progress towards its goals.

- **Strategies the agency will use to achieve desired results.** We evaluated the strategy to determine if it provided a clear narrative of how IT is enabling agency goals.
- **Descriptions of dependencies within and between projects.** We evaluated the strategy to determine if it provided descriptions of interdependencies within and across projects.

To determine if the department had an enterprise road map to implement its financial management systems strategy, we requested the department's enterprise road map, which the Office of Management and Budget (OMB) requires federal agencies to develop annually. According to OMB guidance, federal agencies should have an enterprise road map to implement their IT strategic plans. The road map should be an integrated plan that documents the current and future states of a business and systems environment at a high level, from an architecture perspective, and presents a transition plan for moving from the current to the future in an efficient, effective manner.⁴ The road map should discuss performance gaps, resource requirements, and planned solutions, and it should map the IT strategy to projects and budget. The road map should document the tasks, time frames, and milestones for implementing new solutions, and it should contain an inventory of systems.⁵

We also compared the department's June 2020 report on its efforts to develop a Defense Business Systems Audit Remediation Plan with provisions in the National Defense Authorization Act for Fiscal Year 2020.⁶ The act requires DOD to develop and maintain a plan, which is to include a current accounting of defense business systems that will be introduced, replaced, updated, modified, or retired in connection with the

⁴Enterprise architecture is intended to provide a clear and comprehensive picture of a functional or mission area that cuts across more than one organization. It describes the enterprise in logical terms (such as interrelated business processes and business rules, information needs and flows, and work locations and users), as well as in technical terms (such as hardware, software, data, communications, security attributes, and performance standards).

⁵OMB, *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management*, Memorandum M-13-09 (Washington, D.C.: Mar. 27, 2013); *Federal Enterprise Architecture Framework* Version 2, Jan. 29, 2013; and *The Common Approach to Federal Enterprise Architecture*, May 2, 2012; and *FY 2019 IT Budget – Capital Planning Guidance*, August 1, 2017.

⁶Pub. L. No. 116-92, § 1002, 133 Stat. 1198, 1570 (Dec. 20, 2019).

full financial statement audit. The plan is also to include a comprehensive road map that displays

- in-service, retirement, and other pertinent dates for affected systems
- cost estimates for each affected system;
- dependencies between the various systems; and
- dependencies between the introduction, replacement, update, modification, and retirement of such systems.

To determine if the department had detailed plans for migrating legacy accounting systems to new systems, we requested documented plans for the Air Force's, Navy's and Army's systems.⁷ These included the Air Force's General Accounting and Finance System Reengineered (GAFS-R),⁸ Navy's Standard Accounting and Reporting System (STARS), Army's Standard Finance System (STANFINS) and Standard Operation and Maintenance Army Research and Development System (SOMARDS).⁹ We identified these systems based on our past and ongoing oversight of DOD financial audits. According to the Software Engineering Institute (SEI), an organization should develop a plan to migrate legacy system software to a new system.¹⁰ In addition, according to the fiscal year 2019 DOD Annual Financial Report, a legacy accounting system is expected to have a retirement plan for the department's investment review process.¹¹

To determine to what extent DOD is effectively monitoring the status of IT NFR remediation efforts, we obtained and reviewed the department's June 2019 Financial Management Audit Support Plan, and July 3, 2019, memorandum signed by the Chief Information Officer (CIO), the Deputy

⁷The Marine Corps systems are included in the Department of Navy's plan.

⁸GAFS-R is owned by Defense Finance and Accounting Service (DFAS) but utilized by the Air Force.

⁹These legacy accounting systems are systems that support the key functions of a military service's financial management and are integral to the financial reporting process, which are planned to be decommissioned, retired, or replaced.

¹⁰Software Engineering Institute, *DOD Software Migration Planning*, CMU/SEI-2001-TN-012 (Pittsburgh, PA: August 2001). SEI is a nationally recognized, federally funded research and development center established at Carnegie Mellon University in Pittsburgh, Pennsylvania, to address software development issues.

¹¹Department of Defense, *Agency Financial Report: Fiscal Year 2019*, November 15, 2019.

Under Secretary of Defense (Comptroller) (hereinafter, referred to as the Chief Financial Officer or CFO), and the Acting Chief Management Officer (CMO), on addressing deficiencies in system access controls identified in IT NFRs.¹² In addition, we reviewed the 25 CIO financial management audit updates issued between February 2019 and September 2019, the minutes of 13 CFO-CIO synchronization meetings held between April 2019 and July 2019, and the minutes of 6 CMO-CFO-CIO meetings held in August 2019 and September 2019. We compared the content of these documents with OMB guidance on establishing performance goals and using them to measure progress.¹³ Specifically, we assessed the extent to which DOD plans included performance goals with performance indicators, targets, and time frames, and the extent to which the status updates report progress.

We also conducted interviews with relevant officials in the Offices of the CIO, CFO, and CMO to discuss the development of strategies and plans to guide financial management systems improvement efforts. These included plans to address key information technology controls for their financial management systems. In addition, we discussed system migration plans with officials from the Departments of the Air Force, Army, and Navy.

To determine how much money DOD reports spending on developing and maintaining its financial management systems, we analyzed the department's IT system databases to identify the systems the department considers necessary for preparing financial statements and associated expenditures. We calculated how much the department reports spending annually on these systems. We also determined how much the department spent in fiscal years 2016 through 2018 and the amount it planned to spend in fiscal years 2019 and 2020 on new financial management systems and on legacy accounting systems. We discussed our approach and analysis with DOD CIO and CFO officials, and they provided comments, which we incorporated in our report.

To determine how much money DOD reports spending on developing and maintaining the financial management systems the department considers necessary for preparing financial statements, we obtained DOD's list of

¹²The Acting Chief Management Officer was confirmed by the Senate on December 19, 2019, to be Chief Management Officer.

¹³OMB, Circular No. A-11: *Preparation, Submission, and Execution of the Budget*, June 2018.

significant financial and feeder systems from its Financial Improvement and Audit Readiness (FIAR) systems database, as of February 2019. We matched the system identification numbers in the list with the identification number in the DOD IT Portfolio Repository (DITPR). We then identified the unique investment identifier in the repository associated with each system in the list of significant financial and feeder systems. Using these unique investment identifiers, we identified in the budget data reported on the federal IT Dashboard the amount spent on developing and modernizing and operating and maintaining the systems in fiscal years 2016 through 2018, and the amount planned to be spent in fiscal years 2019 and 2020.¹⁴

To determine how much money DOD spent in fiscal years 2016 through 2018 and the amount it planned to spend in fiscal years 2019 and 2020 on developing new financial management systems, we requested this information from DOD and military service officials. Specifically, we requested that DOD and military service officials identify any new financial management system investments being developed. We then identified in the budget data reported on the federal IT Dashboard the amount spent in fiscal years 2016 through 2018 and the amount planned to be spent in fiscal years 2019 and 2020 on these systems.

To determine how much money DOD spent in fiscal years 2016 through 2018 and the amount it planned to spend in fiscal years 2019 and 2020 on legacy accounting systems, we obtained information from DOD and military service officials, which identifies legacy accounting systems. We also reviewed legacy systems identified in the financial management portfolio provided by the DOD CFO. We then identified in the budget data reported on the federal IT dashboard the amount spent in fiscal years 2016 through 2018 and the amounts planned to be spent in fiscal years 2019 and 2020 on these systems.

To determine the reliability of the data we used to calculate how much money DOD spends on financial management systems, we reviewed documentation of the data systems and discussed these data systems with DOD officials. Specifically, we reviewed the FIAR Systems Database, DITPR, and the Select and Native Programming-Information Technology System (SNAP-IT). DOD uses SNAP-IT to report its IT budget data on the IT Dashboard. We requested and reviewed

¹⁴The federal IT Dashboard is a website that enables federal agencies, industry, the general public, and other stakeholders to view details regarding the performance of federal IT investments.

department responses to questions about the systems and how the department ensures the quality and reliability of the data. In addition, we reviewed documentation related to the systems (e.g., data dictionaries, system instructions, and user training manuals) and reviewed the data for obvious issues, including missing or questionable values. We determined that the data in DITPR and the data reported on the IT Dashboard were sufficiently reliable for calculating the annual costs of the systems in the FIAR Systems Database. However, we determined that many systems and their associated costs were not included in this database. Accordingly, the total amount of costs we determined is understated.

We conducted this audit from March 2018 to August 2020, 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: Summary of the Department of Defense's Financial Management Functional Strategy

The Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer developed the *Department of Defense Financial Management Functional Strategy for Fiscal Years 2019 to 2023* to provide direction and guidance to DOD organizational entities for making financial management investment decisions that support strategic outcomes. According to the strategy, it addresses specific material weaknesses and critical issues that adversely affect the way the department conducts business, and describes DOD's vision as achieving a target financial management environment that is data driven, standards-based, technology enabled, affordable, auditable, and secure.

The strategy is composed of four goals and associated objectives, expected business outcomes, and initiatives:

Goal 1 is to enhance and implement financial policies and processes to improve, simplify, and standardize the financial management business and systems environment, and includes two objectives:

- Objective 1.1: Improve and standardize business processes and data for decision-making
- Objective 1.2: Simplify the financial management systems and interface environment

The expected outcomes of Goal 1 are

- reduced reconciliation work,
- supportable transactions,
- stronger internal controls,
- timely, accurate, and reliable financial data,
- improved interoperability between systems,
- end to end funds traceability between budget and expenditures, and
- cost effective business environment.

Goal 2 is to develop and strengthen a well-trained financial workforce that has the knowledge, skills, and abilities to support business reform and auditability in DOD. It includes one objective:

- Objective 2.1: Provide course-based financial management training and developmental opportunities in required financial management.

The expected outcomes of Goal 2 are

- requisite knowledge, skills, and abilities to perform effectively in all financial management career series;
- closure of identified competency gaps;
- improved analytic capability across the workforce; and
- improved audit and remediation capabilities.

Goal 3 is to develop a standardized planning, programming, budget and execution process that enables end-to-end funds traceability and data linkage between planning, budgeting, and execution. It includes one objective:

- Objective 3.1: Establish clearer and closer links between prioritized requirements and program execution.

The expected outcomes of Goal 3 are

- timely, accurate, and reliable financial data for decision-makers;
- supportable transactions;
- end-to-end funds traceability between budget and expenditures; and
- a cost effective business environment.

Goal 4 is to achieve a sustainable unmodified audit opinion by improving financial processes, controls, and information via audit remediation. It includes two objectives:

- Objective 4.1: Achieve an unmodified financial statement audit opinion.
- Objective 4.2: Continually strengthen compliance with financial management laws, regulations, policies, and internal controls.

The expected outcomes of Goal 4 are

- an auditable business environment;
- timely, accurate, and reliable property, inventory, and financial data for decision-makers;
- supportable transactions (eliminations);
- reduced reconciliation work;
- improved interoperability between systems;

- stronger internal controls;
- strengthened mission capabilities;
- enhanced stewardship and public trust; and
- an unmodified audit opinion.

Related to these goals and objectives, DOD established, among others, a Financial Management IT Systems Environment initiative and a Digital Accountability and Transparency Act of 2014 (DATA Act) initiative. The Financial Management IT Systems Environment initiative is intended to reduce legacy financial management systems by investing in current enterprise resource planning systems and target financial management systems.¹

According to the strategy, the target financial management systems environment will include

- standardized, enterprise-wide data, processes, and systems as a result of the full adoption of data standards;
- standardized, non-customized, and fully leveraged enterprise resource planning system implementations;
- a small number of enterprise resource planning systems in each military service and other DOD organizational entity, which support all core financial management functions;
- integrated financial management and non-financial management functions within the enterprise resource planning systems and direct integration with the Treasury, eliminating the need for separate entitlement systems and reconciliations;
- fewer interfaces where non-financial management functions are tightly integrated with core accounting functions;
- financial statements that are traceable to source transactions through the enterprise resource planning systems and to any remaining critical feeders; and
- a standardized set of business analytics.

¹An enterprise resource planning system is an automated system using commercial off-the-shelf software consisting of multiple, integrated functional modules that perform a variety of business-related tasks such as general ledger accounting, payroll, and supply chain management.

**Appendix II: Summary of the Department of
Defense's Financial Management Functional
Strategy**

The DATA Act initiative is intended to assist DOD in complying with the act's reporting requirements. The act was enacted, in part, to increase accountability and transparency of government spending to the public.² According to the strategy, DOD will leverage a pilot it is conducting to, for example, identify the amount of any federal funds reprogrammed or transferred, and report the amount of expired and unexpired unobligated balances. In addition, according to the strategy, the pilot results will be used as the basis for developing a department-wide solution for complying with DATA Act reporting requirements.

² Pub. L. No. 113-101, 128 Stat. 1146 (May 9, 2014). The DATA Act amended the Federal Funding Accountability and Transparency Act of 2006 (FFATA). Pub. L. No. 109-282, 120 Stat. 1186 (Sept. 26, 2006), codified at 31 U.S.C. § 6101 note.

Appendix III: Key Roles and Responsibilities of the DOD CFO, CIO, and CMO for Financial Management Systems

Under Secretary of Defense (Comptroller)/Chief Financial Officer (CFO)

The CFO has authority and responsibility related to financial management, an integrated accounting and financial management system, and reporting.

Financial Management

According to the DOD financial management regulation, the CFO is responsible for overseeing financial management activities related to the CFO programs and operations of the department.¹ Among other things, the CFO is to

- establish financial management policies for DOD, including its components;
- ensure compliance throughout DOD with applicable accounting policies, standards and principles, as well as financial information and systems functional standards;
- establish, review, and enforce internal control policies, standards, and compliance guidelines involving financial management;
- ensure complete, reliable, consistent, timely and accurate information on disbursements is available in financial management systems;
- prepare and annually revise a DOD plan to implement the 5-year financial management plan prepared by the Director of the Office of Management and Budget (OMB) and to comply with the audited financial statements provisions of the CFO Act;
- approve and manage DOD financial management systems design or enhancement projects;
- implement DOD asset management systems, including for cash management, credit management, debt collection, and property inventory management and control; and
- manage directly, and/or monitor, evaluate and approve the design, budget, development, implementation, operation and enhancement of DOD-wide accounting, financial, and asset management systems.

¹Department of Defense, Under Secretary of Defense (Comptroller), *DOD 7000.14-R: Financial Management Regulation, Volume 1: "General Financial Management Information, Systems and Requirements"*.

Integrated Accounting and Financial Management System

According to section 902 of Title 31 of the U.S. Code and the DOD Financial Management Regulation, the DOD CFO is to develop and maintain an integrated agency accounting and financial management system, including financial reporting and internal controls.² This financial management system must comply with applicable accounting principles, standards and requirements, and internal control standards; policies and requirements prescribed by OMB; and any other requirements applicable to such systems. In addition, the DOD CFO should ensure that the financial management system provides for complete, reliable, consistent, and timely information which is prepared on a uniform basis and which is responsive to the financial information needs of DOD management.

Annual Reporting

The DOD CFO is required by law to prepare and transmit an annual report to the Secretary of Defense and the Director of OMB, which includes

- a description and analysis of the status of financial management within the department;
- annual financial statements;
- audit reports submitted to the Secretary of Defense addressing financial statements;
- a summary of reports on the internal accounting and administrative control systems submitted under the Federal Managers' Financial Integrity Act of 1982;³
- other information the Secretary of Defense considers appropriate to fully inform the President and the Congress concerning DOD financial management.⁴

²31 U.S.C. § 902(a)(3). DOD 7000.14-R: *Financial Management Regulation, Volume 1: General Financial Management Information, Systems and Requirements*

³31 U.S.C. § 3512(c), (d).

⁴31 U.S.C. § 902(a)(6).

**Appendix III: Key Roles and Responsibilities of
the DOD CFO, CIO, and CMO for Financial
Management Systems**

**DOD Chief Information Officer
(CIO)**

Under Section 142 of Title 10 of the United States Code, the DOD CIO is responsible for

- policy, oversight, and guidance for the architecture and programs related to the information technology, networking, information assurance, cybersecurity, and cyber capability architectures;
- implementing and enforcing a process for developing, adopting, or publishing standards for information technology, networking, or cyber capabilities to which a military service or defense agency would need to adhere in order to run such capabilities on defense networks; and certifying on a regular and ongoing basis that any capabilities being developed or procured meets such standards as have been published by DOD at the time of certification; and
- identifying gaps in standards and mitigation plans for operating in the absence of acceptable standards.

Under Section 2222 of Title 10, the DOD CIO is to develop an information technology enterprise architecture, which will describe a plan for improving the information technology and computing infrastructure of the department, including for each of the major business processes conducted by DOD.

Under Section 2223(a) of Title 10, the DOD CIO is to

- review and provide recommendations to the Secretary of Defense on DOD budget requests for information technology;
- ensure the interoperability of information technology throughout DOD; and
- ensure that information technology standards that will apply throughout the department are prescribed.

**DOD Chief Management
Officer (CMO)**

CMO responsibilities include

- Management of the enterprise business operations and shared services of the department.
- Advising the Secretary and Deputy Secretary on establishing policies for, and directing, all enterprise business operations of the department, including planning and processes, business transformation, and performance measurement and management activities and programs.

**Appendix III: Key Roles and Responsibilities of
the DOD CFO, CIO, and CMO for Financial
Management Systems**

-
- Exercising authority, direction, and control over the defense agencies and field activities providing shared business services for the department that are designated by the Secretary or Deputy Secretary.

According to DOD's Fiscal Year 2020 Annual Performance Plan, the CMO has authority to direct the principal staff assistants, military services, combatant commands, and the defense agencies and DOD field activities with regard to business operations.

Appendix IV: DOD Spending On New and Legacy Accounting Systems, Fiscal Years 2016 through 2020

DOD spends billions of dollars annually on its financial management systems, including hundreds of millions of dollars aimed at developing and modernizing them. This spending includes a total of about \$2.2 billion for seven new financial management systems.¹ In addition, it includes about \$427 million on 12 legacy accounting systems in fiscal years 2016 through 2020.²

According to the military services, they are in the process of developing seven new financial management systems, for which DOD estimates spending a total of about \$2.2 billion in fiscal years 2016 through 2020. Specifically, the Department of the Army is developing three new systems and the Department of the Air Force is developing four new systems.³ According to DOD's budget data, the military services spent about \$174 million in fiscal year 2016, \$261 million in fiscal year 2017, and \$407 million in fiscal year 2018. In addition, the military services planned to spend about \$724 million in fiscal year 2019 and about \$592 million in fiscal year 2020 on the systems. Table 6 provides details on the amount spent in fiscal years 2016 through 2018 and planned to be spent in fiscal years 2019 and 2020.

¹New financial management system investments identified by DOD or the military services.

²These legacy accounting systems are systems that support the key functions of a military service's financial management and are integral to the financial reporting process, which are planned to be decommissioned, retired, or replaced.

³The Department of the Navy did not identify any new financial management systems.

Appendix IV: DOD Spending On New and Legacy Accounting Systems, Fiscal Years 2016 through 2020

Table 6: Military Services Spending on New Financial Management Systems, Fiscal Years (FY) 2016 through 2020

Millions of dollars

Military Service	System	FY 2016	FY 2017	FY 2018	FY 2019	FY 2020	Total
Army	GFEBs-SA	6.415	11.044	37.974	42.016	47.374	144.823
Army	IPPS-A	120.661	165.802	243.100	444.498	360.560	1334.621
Army	ACWS	0	20.657	23.913	49.395	37.914	131.879
Air Force	AFIPPS	30.334	29.825	27.347	51.109	68.058	206.673
Air Force	CON-IT	4.326	8.327	20.408	30.209	33.116	96.386
Air Force	MROi	11.393	23.703	43.119	78.592	28.095	184.902
Air Force	PBES	0.900	1.991	11.261	27.762	17.355	59.269
Total		174.029	261.349	407.122	723.581	592.472	2,158.553

Legend:

GFEBs-SA: General Fund Enterprise Business System – Sensitive Activities

IPPS-A: Integrated Personnel and Payroll System – Army

ACWS: Army Contract Writing System

AFIPPS: Air Force Integrated Personnel and Pay System

CON-IT: Contracting Information Technology

MROi: Maintenance, Repair, and Overhaul Initiative

PBES: Program Budget Enterprise System

Source: GAO analysis of Department of Defense information. | GAO-20-252

According to DOD and the military services, they are currently maintaining 12 legacy accounting systems, for which DOD estimates spending about \$427 million in fiscal years 2016 through 2020. Specifically, the Department of the Army is maintaining three legacy accounting systems, the Department of the Air Force is maintaining four legacy accounting systems, the Department of the Navy is maintaining three legacy accounting systems, and DOD is maintaining two legacy accounting systems.

According to DOD’s budget data, the department spent about \$60 million in fiscal year 2016, \$98 million in fiscal year 2017, and \$103 million in fiscal year 2018. In addition, the department planned to spend about \$85 million in fiscal year 2019 and about \$81 million in fiscal year 2020 on maintaining these systems. Table 7 provides details, by system, on the amount spent in fiscal years 2016 through 2018 and planned to be spent in fiscal years 2019 and 2020.

Appendix IV: DOD Spending On New and Legacy Accounting Systems, Fiscal Years 2016 through 2020

Table 7: Department of Defense and the Military Services Spending on Legacy Accounting Systems, Fiscal Years (FY) 2016 through 2020

Millions of dollars

DOD and Military Service	System	FY 2016	FY 2017	FY 2018	FY 2019	FY 2020	Total
Army	STANFINS	2.824	2.575	2.602	2.738	2.672	13.411
Army	SOMARDS	6.084	6.812	6.543	7.287	6.971	35.697
Army	NIFMS IMCOM	0	0	.001	.001	.001	.003
Air Force	GAFS-R ^a	12.094	12.229	14.826	16.883	15.575	71.607
Air Force	AFTOC	4.729	2.504	8.751	5.184	5.216	26.384
Air Force	CRIS	1.047	33.038	28.489	7.681	6.564	76.819
Air Force	JOCAS II	1.119	1.128	1.150	3.306	3.533	10.236
Navy	STARS	18.64	20.006	19.885	20.321	14.841	93.693
Navy	IMPS	3.664	6.371	3.984	4.590	4.679	23.288
Navy	MSC-FMS	1.470	5.311	7.278	8.388	8.594	31.041
DFAS	DIFMS	3.548	3.525	4.331	4.327	7.213	22.944
DFAS	DWAS	4.660	4.691	4.910	4.915	5.096	24.272
Total		59.879	98.190	102.750	85.621	80.955	427.395

Legend:

- STANFINS: Standard Finance System
- SOMARDS: Standard Operations and Maintenance, Army Research & Development System
- NIFMS IMCOM: IMCOM Non Appropriated Fund Integrated Financial and Management System Installation Management Command
- GAFS-R: General Accounting and Finance System – Reengineered
- AFTOC: Air Force Total Ownership Cost
- CRIS: Commander’s Resource Integration System
- JOCAS II: Job Order Cost Accounting System II
- STARS: Standard Accounting and Reporting System
- IMPS: Integrated Management Processing System
- MSC FMS: Military Sealift Command Financial Management System
- DFAS: Defense Finance and Accounting Service
- DIFMS: Defense Industrial Financial Management System
- DWAS: Defense Working Capital Fund Accounting System

Source: GAO analysis of Department of Defense information. | GAO-20-252.

^aGAFS-R is owned by DFAS, but utilized by the Air Force.

Appendix V: Comments from the Department of Defense



CHIEF MANAGEMENT OFFICER
9010 DEFENSE PENTAGON
WASHINGTON, DC 20301-9010

10 SEP 2020

Ms. Carol C. Harris
Director, Information Technology Acquisition Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Harris,

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-20-252, 'FINANCIAL MANAGEMENT: DOD Needs to Implement Comprehensive Plans to Improve its Systems Environment,' dated August 14, 2020 (GAO Code 102651).

The Department appreciates the opportunity to review this draft report and concurs with the recommendations provided. While progress has been made to address audit findings related to IT, improving the financial management systems environment is a critical element to achieve a clean audit. The Department will drive this by focusing on priority capability areas and reforming business operations required to deliver these capabilities. The Department will develop a consolidated enterprise roadmap to document the transition plans and establish more specific performance measures to monitor progress towards achieving the end state. Additionally, the Department will continue to leverage its existing governance processes to manage the implementation of the enterprise roadmap to ensure the most efficient use of resources and investments.

Attached are the Department's proposed technical comments to the subject report. My point of contact is Ms. Lora Muchmore who can be reached at lora.h.muchmore.civ@mail.mil and phone (703) 692-0725.

Sincerely,

A handwritten signature in blue ink, which appears to read "Lisa W. Hershman", is positioned above the printed name.

Lisa W. Hershman

Enclosure:
Response to GAO Draft Report GAO-20-252 (Code 102651) Consolidated.pdf

Appendix VI: GAO Contacts and Staff Acknowledgments

GAO Contacts

Kevin Walsh, 202-512-6151 or walshk@gao.gov

Asif Khan, 202-512-9869 or khana@gao.gov

Staff Acknowledgments

In addition to the individuals named above, individuals who made key contributions to this report include Michael Holland (Assistant Director), Chanetta Reed (Assistant Director), Beatrice Alff, Michelle Chan, Cheryl Dottermusch, Linda Erickson, Nadine Ferreira, Camille Garcia, Carol Harris, Maxine Hattery, James Kernen, Tyler Mountjoy, Ashley Paw, Monica Perez-Nelson, Kevin Smith, Priscilla Smith, and Althea Sprosta.

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/fraudnet/fraudnet.htm>

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

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548

