



June 2022

CLOUD COMPUTING

DOD Needs to Improve Workforce Planning and Software Application Modernization

GAO Highlights

Highlights of [GAO-22-104070](#), a report to congressional committees

Why GAO Did This Study

In fiscal year 2022, DOD plans to spend approximately \$38.6 billion on unclassified IT investments. To help drive cloud adoption, OMB requires agencies to modernize, retire, or consolidate their portfolios of software applications—a process known as application rationalization. OMB also requires agencies to use TBM to categorize IT and cloud-related spending.

GAO was asked to assess DOD's reported use of cloud services. This report examines the extent to which (1) DOD's planned cloud strategy addresses key requirements in OMB's federal cloud strategy, (2) the department has plans for developing and implementing an enterprise-wide application rationalization process, and (3) DOD is using TBM to track and report spending data for cloud services. To do so, GAO analyzed relevant DOD policies, guidance, and other documentation on cloud services and application rationalization. It also assessed the department's cloud investment data for fiscal years 2021 and 2022 and department-wide guidance and training on implementing TBM. GAO also interviewed DOD officials.

What GAO Recommends

GAO is making nine recommendations to DOD related to addressing gaps in cloud workforce activities, improving application rationalization planning, and updating guidance on TBM implementation. DOD agreed with one recommendation, partially agreed with seven, and did not agree with one. As discussed in the report, GAO continues to believe its recommendations are appropriate.

View [GAO-22-104070](#). For more information, contact Carol C. Harris at (202) 512-4456 or HarrisCC@gao.gov or David B. Hinchman at (214) 777-5719 or HinchmanD@gao.gov.

June 2022

CLOUD COMPUTING

DOD Needs to Improve Workforce Planning and Software Application Modernization

What GAO Found

In 2019, the Office of Management and Budget (OMB) updated its *Federal Cloud Computing Strategy* and established 14 key requirements for agencies to implement within three areas—security, procurement, and workforce. Cloud computing enables on-demand access to shared computing resources. The Department of Defense (DOD) has addressed 11 of the 14 OMB requirements, but gaps exist in its workforce planning (see table). These gaps include identifying the future skills needed for cloud-based services and conducting regular evaluations of customer experiences and user needs. In addition, DOD has not yet developed and executed communication plans to inform employees of changes related to using these services. Addressing these workforce areas is essential to realizing the benefits of cloud computing.

Extent to Which DOD Guidance Has Addressed 14 OMB Key IT Cloud Requirements as of April 2022

Requirement area	Fully addressed	Partially addressed	Not addressed
Security	Four	—	—
Procurement	Five	—	—
Workforce	Two	Two	One

Legend: — = not applicable.

Source: GAO analysis of Department of Defense (DOD) documentation. | GAO-22-104070

In order to meet OMB's application rationalization requirement, DOD has partially implemented the first step noted in leading implementation practices. The department has established a scope for its rationalization efforts and is working to formalize a governance group with the authority to set requirements and issue guidance. However, DOD's lack of established timeframes for completing the remaining activities has impacted its efforts to make progress on subsequent leading practice steps. In addition, DOD has not developed a long-term plan for rationalization implementation with measurable objectives, milestones, and timelines. This is due to significant changes to its approach over the past 2 years; long time frames for implementing enterprise-wide initiatives; and a lack of definition by DOD regarding who is responsible for ensuring rationalization activities are successful. Without measurable objectives, milestones, and time frames for rationalization efforts—and holding department components accountable for these efforts—DOD will be less likely to make consistent measurable progress on rationalization or effectively reduce IT duplication.

In its fiscal year 2019 guidance, OMB began requiring agencies to use Technology Business Management (TBM)—a framework for increasing the granularity in agency-reported IT spending data by grouping related costs together—as part of the annual budget submission. DOD has reported its budget data using TBM cost categories. However, GAO identified weaknesses in the completeness of DOD components' cloud spending data. As a result, DOD's cloud spending is likely underreported. This was due in part to nonspecific department guidance on reporting these data and the control processes needed to ensure reliable data. In addition, the Army and Air Force did not follow leading TBM implementation practices. Until the Army and Air Force address TBM practices, and the DOD Chief Information Officer updates the department's guidance on reporting TBM data and ensuring its reliability, DOD will lack complete information needed to make decisions on its IT investments.

Contents

Letter		1
	Background	5
	DOD's Plans Address Most OMB Cloud Computing Requirements, but Gaps in Workforce Remain	19
	DOD Has Taken Steps to Develop an Enterprise-Wide Application Rationalization Process, but Lacks a Long-Term Implementation Plan	24
	DOD Components Underreported TBM Cloud Spending and Did Not Always Follow Leading Practices	32
	Conclusions	38
	Recommendations for Executive Action	39
	Agency Comments and Our Evaluation	40
Appendix I	Objectives, Scope, and Methodology	45
Appendix II	Prior GAO and OIG Reports From 2014 Through 2016 Reviewing DOD's Adoption of Cloud Services, Portfolio Management, and Rationalization Activities	50
Appendix III	Comments from the Department of Defense	53
Appendix IV	GAO Contact and Staff Acknowledgments	57
Tables		
	Table 1: Key Security, Procurement, and Workforce Cloud Computing Requirements in OMB's <i>Federal Cloud Computing Strategy</i>	7
	Table 2: Extent to Which Department of Defense (DOD) Guidance Has Addressed the 14 OMB Key IT Cloud Requirements	20
	Table 3: Department of Defense (DOD) Implementation of CIO Council Application Rationalization Playbook Step 1: Identify Needs and Set Governance	26
	Table 4: Number of Unclassified DOD IT Cloud Investments Using Commercial Providers but No Reported Spending for Outside Services, as Reported in DOD SNaP-IT for Six	

Components for Fiscal Year 2021 through Fiscal Year 2022	34
Table 5: Number of Unclassified DOD IT Cloud Investments With Reported Spending of \$6,000 or Less, as Reported in DOD SNaP-IT for Six Components for Fiscal Year 2021 through Fiscal Year 2022	35
Table 6: Analysis of Selected DOD Components' Implementation Processes for the Technology Business Management (TBM) Framework	37

Figures

Figure 1: CIO Council's Six-step Application Rationalization Process Outlined in <i>The Application Rationalization Playbook: An Agency Guide to Portfolio Management</i>	10
Figure 2: OMB's Reporting Requirements for Technology Business Management IT Cost Pools and IT Towers for Federal Agencies, Fiscal Years 2019 through 2021	13
Figure 3: Department of Defense (DOD) Timeline of Key Enterprise-Wide Rationalization Governance Activities (December 2018 through December 2022)	31

Abbreviations

CIO	chief information officer
DOD	Department of Defense
IT	information technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OUSD (A&S)	Office of the Under Secretary of Defense for Acquisition & Sustainment
SNaP-IT	Select and Native Programming Data Input Systems for Information Technology
TBM	Technology Business Management

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.



June 29, 2022

The Honorable Carolyn B. Maloney
Chairwoman
The Honorable James Comer
Ranking Member
Committee on Oversight and Reform
House of Representatives

The Honorable Gerald E. Connolly
Chairman
The Honorable Jody Hice
Ranking Member
Subcommittee on Government Operations
Committee on Oversight and Reform
House of Representatives

The Department of Defense (DOD) spends billions of dollars each year on information technology (IT) systems that are fundamental to achieving its mission. In fiscal year 2022, the department plans to spend approximately \$38.6 billion on unclassified IT investments.¹ DOD reported that this included approximately \$1.1 billion in funding for cloud computing services (cloud services) and migration.²

As part of a comprehensive effort to transform IT within the federal government, in 2010, the Office of Management and Budget (OMB) began requiring agencies to shift their IT services to a cloud computing option when feasible.³ According to the National Institute of Standards and Technology, cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned and released. Cloud services offers federal agencies a means to buy services more quickly and possibly at a lower cost than

¹Department Of Defense, *Department of Defense Information Technology and Cyberspace Activities Budget Overview: Fiscal Year 2022 Budget Request* (June 8, 2021).

²Based on our review of the six DOD components' TBM data, there is increased likelihood that the department's spending on cloud services is underreported.

³Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Dec. 9, 2010).

building, operating, and maintaining these computing resources themselves.

In an effort to accelerate agency adoption of cloud services, in June 2019, OMB published its updated *Federal Cloud Computing Strategy*, called Cloud Smart.⁴ As part of Cloud Smart, OMB required all federal agencies to rationalize their application portfolios—streamlining the portfolio with the goal of improving efficiency, reducing complexity and redundancy, and lowering the cost of ownership—in order to drive cloud adoption. In addition, OMB required agencies to take steps in three areas (security, procurement, and workforce) in order to help ensure successful cloud implementation.

In its fiscal year 2019 guidance, OMB began requiring agencies to report spending on IT investments, including IT investments that leverage cloud services, using the Technology Business Management (TBM) framework.⁵ OMB guidance notes that TBM is intended to help agencies manage the cost, quality, and value of their IT services. In addition, TBM is intended to increase the granularity in reporting of agency IT budget and spending data, including spending on cloud services, by grouping related costs together.

We and the DOD Office of Inspector General (OIG) have issued several reports on the department's use of cloud services and application rationalization over the past 10 years, as detailed later in this report. In April 2019, we reported that DOD was in the process of adjusting its January 2018 cloud strategy and had not yet completed an assessment of all of its IT investments for cloud services.⁶ In addition, the department had reported challenges in tracking cloud spending data and could not provide savings data for any of its cloud investments.

Accordingly, we made two recommendations to DOD to complete an assessment of all investment for cloud services and to better track its cloud savings data. DOD concurred with the recommendation on completing assessments, but disagreed with our recommendation to

⁴Office of Management and Budget, *Federal Cloud Computing Strategy* (June 24, 2019).

⁵Office of Management and Budget, *FY 2019 IT Budget–Capital Planning Guidance* (Aug. 1, 2017).

⁶GAO, *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to be Better Tracked*, [GAO-19-58](#) (Washington, D.C.: Apr. 4, 2019).

establish a mechanism to track cost savings. As of April 2022, DOD had not implemented either recommendation.

You asked us to conduct a further review of DOD's reported use of cloud services. Our objectives were to determine the extent to which: (1) DOD's planned cloud strategy addresses the key requirements included in OMB's *Federal Cloud Computing Strategy*, (2) the department has plans for developing and implementing an enterprise-wide process to rationalize its application portfolio, and (3) the department is using the TBM framework to track and report spending data for cloud services.

For our first objective, we analyzed OMB's June 2019 *Federal Cloud Computing Strategy* to identify the requirements that OMB indicated should be undertaken as part of an agency's cloud strategy. Based on our review of the strategy, we identified 14 key requirements across three categories (security, procurement, and workforce); we confirmed the list with staff in OMB's Office of the Federal Chief Information Officer (CIO).

We then analyzed DOD policies, established guidance, and processes related to cloud services, including its digital modernization and software modernization strategies, to determine whether the department had addressed the key cloud computing requirements included in OMB's cloud strategy. We also corroborated our analysis by interviewing officials in DOD's Office of the CIO in the Enterprise Capabilities division and the Office of the Under Secretary of Defense for Acquisition & Sustainment (OUSD [A&S]) regarding department guidance and other documentation related to cloud services in the areas of security, procurement, and workforce planning.

For our second objective, we analyzed DOD policies and other documentation related to enterprise-wide application rationalization to determine whether they were consistent with OMB guidance and the CIO Council's *The Application Rationalization Playbook*.⁷ In addition, we interviewed officials from DOD's Office of the CIO in the Enterprise Services division with responsibility for application rationalization efforts

⁷CIO Council, *The Application Rationalization Playbook: An Agency Guide to Portfolio Management* (June 2019). The CIO Council is the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of federal information resources. Members include CIOs from across the federal government executive branch.

regarding department guidance and other documentation related to the development and implementation of an enterprise-wide process.

To address the third objective, we selected a sample of DOD components based on the size of their IT budget request for cloud services for fiscal year 2021.⁸ Using this criterion, we selected six components with the largest budget requests in the department: the Air Force, Army, Defense Human Resources Activity, Defense Information Systems Agency, Navy, and U.S. Transportation Command.

For each of the six selected components, we obtained and analyzed TBM data including investments leveraging cloud services and their spending for fiscal years 2021 and 2022, from the department's Select and Native Programming Data Input Systems for Information Technology (SNaP-IT).⁹ We chose fiscal year 2021 because according to OMB's capital planning guidance, that was the first year that OMB would begin publicly reporting all of the agencies' TBM data.

To assess the reliability of the SNaP-IT data, we reviewed documentation related to the system (e.g., data dictionaries, instructions for inputting budget data in DOD and the six components' guidance) and reviewed the data for obvious issues, including missing or questionable values. We also interviewed officials in charge of SNaP-IT data within the DOD Office of the CIO regarding the department's guidance, the systems, and how the department ensures the quality and reliability of the data. Further, we interviewed staff from OMB's Office of the Federal CIO regarding their guidance on TBM.

To help ensure the accuracy and completeness of the selected components' number of investments leveraging cloud services and the spending allocated using TBM, we presented the results of our analysis to officials in each of the six components, as well as officials in charge of SNaP-IT data within the DOD Office of the CIO. We asked them to verify the completeness and accuracy of these data and provide any updates as appropriate.

⁸Department of Defense, *DoD FY 2021 Cloud Profile and Budget Estimates* (Feb. 18, 2020).

⁹DOD uses SNaP-IT to report its IT budget data on the federal IT Dashboard. OMB's IT Dashboard is a public website that provides detailed information on IT investments at 26 federal agencies. See <https://itdashboard.gov/>.

Based on the measures we took to ensure the reliability of the data reported by the six components from SNaP-IT, we determined that the data were sufficiently reliable for the purpose of determining whether the department was using TBM to meet OMB's requirement. However, we identified issues with the completeness of the department's cloud spending data, which we discuss later in the report. Further details on our objectives, scope, and methodology are included in appendix I.

We conducted this performance audit from January 2020 to June 2022 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

Cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned. More specifically, purchasing IT services through a cloud service provider enables agencies to avoid paying for all the computing resources that would typically be needed to provide such services. This approach offers federal agencies a means to buy services more quickly and possibly at a lower cost than building, operating, and maintaining these computing resources themselves.

According to the National Institute of Standards and Technology, cloud computing offers federal agencies a number of benefits:

- **On-demand self-service.** Agencies can, as needed, provision computing capabilities, such as server time and network storage, from the service provider automatically and without human interaction.
- **Broad network access.** Agencies can access needed capabilities over the network through workstations, laptops, or other mobile devices.
- **Resource pooling.** Agencies can use pooled resources from the cloud provider, including storage, processing, memory, and network bandwidth.
- **Rapid elasticity.** Agencies can provision the resources that are allocated to match what actual resources are needed according to demand. This is done by scaling resources up or down by adding or

removing processing or memory capacity, or both, according to demand.

- **Measured service.** Agencies can pay for services based on usage. This allows agencies to monitor, control, and generate reports, providing greater transparency into the agency's use of cloud services.

OMB's Mission and Guidance Related to Cloud Computing Services, Application Rationalization, and TBM

By law, OMB is to oversee federal agencies' management of information and information technology.¹⁰ Within OMB, primary responsibility for oversight of federal IT has been given to the Administrator of the Office of Electronic Government and Information Technology, who is also called the Federal CIO.¹¹ As a part of its oversight, OMB develops and ensures the implementation of policies and guidelines that drive enhanced technology performance and budgeting for the federal government.

OMB Guidance Targets Agency Adoption and Reporting of Cloud Computing Services

In December 2010, OMB made cloud computing an integral part of its *25 Point Implementation Plan to Reform Federal Information Technology Management*.¹² The plan called for the development of a government-wide strategy to hasten the adoption of cloud services. To accelerate the shift, OMB required agencies to identify three systems to migrate to cloud services, create a project plan for migration, and migrate all three systems by June 2012.

Subsequently, in February 2011, OMB issued the *Federal Cloud Computing Strategy*, that required each agency's CIO to evaluate safe, secure cloud computing options before making any new investments.¹³ The strategy provided definitions of cloud services; benefits of cloud services, such as accelerating data center consolidations; a decision

¹⁰40 U.S.C. §§ 11302-03 (*Clinger-Cohen Act*); 44 U.S.C. § 3504 (*Paperwork Reduction Act*); 44 U.S.C. § 3602 (*E-Government Act*); 44 U.S.C. § 3553 (*Federal Information Security Modernization Act of 2014*, which largely superseded the *Federal Information Security Management Act of 2002*).

¹¹OMB's Office of Electronic Government works with OMB's Office of Information and Regulatory Affairs in carrying out its IT management responsibilities. 44 U.S.C. § 3602.

¹²Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management*.

¹³Office of Management and Budget, *Federal Cloud Computing Strategy* (Feb. 8, 2011).

framework for migrating services to a cloud environment;¹⁴ case studies to support agencies' migration to cloud services; and roles and responsibilities for federal agencies.

In June 2019, OMB issued an update to its *Federal Cloud Computing Strategy* in an effort to accelerate agency adoption of cloud-based solutions.¹⁵ The strategy focused on equipping agencies with the tools needed to make informed IT decisions according to its mission needs. In addition, the strategy included 14 key requirements for agencies to implement within three areas—security, procurement, and workforce—that were intended to help ensure successful cloud implementation. Table 1 outlines the key requirements in each of the three areas.

Table 1: Key Security, Procurement, and Workforce Cloud Computing Requirements in OMB's *Federal Cloud Computing Strategy*

Area	Key requirement	Description
Security		
	Implement identify, credential, and access management.	Agencies should implement modern identity, credential, and access management as an essential part of continuous data protection and awareness in cloud-based environments.
	Use mature Agile development practices including development, security, and operations.	Agencies should utilize mature Agile development practices, including DevSecOps (an iterative software development approach ^a), in order to realize the security benefits of cloud infrastructure and scalability.
	Perform continuous monitoring.	Agencies should perform continuous monitoring to detect malicious activity and dedicate effort to improving systems governance.
	Update business continuity and disaster recovery plans.	Agencies should update their business continuity and disaster recovery plans to include contingencies involving the sudden interruption or termination of service.
Procurement		
	Ensure the agency's chief information officer oversees modernization.	The agency Chief Information Officer should oversee the modernization processes.
	Have cloud service level agreement in place.	If a vendor deploys a cloud solution, agencies should ensure that a service level agreement is in place that provides the agency with continuous awareness of the confidentiality, integrity, and availability of its information. With commercial cloud service providers, agencies should granularly articulate roles and responsibilities, establish clear performance metrics, and implement remediation plans for non-compliance.

¹⁴The decision framework, among other things, identified several key areas for determining the readiness for moving to a cloud environment, including the ability of the cloud service provider to address government security requirements.

¹⁵Office of Management and Budget, *Federal Cloud Computing Strategy* (2019).

Area	Key requirement	Description
	Standardize cloud contract service level agreements.	Agencies should standardize cloud contract service level agreements that will provide more effective, efficient, and secure cloud procurement outcomes for agencies.
	Iteratively improve agency policies and guidance.	Agencies will need to iteratively improve policies, technical guidance, and business requirements.
	Ensure continuous visibility in high value asset contracts.	Agencies must ensure that contracts impacting their high value assets, including those managed and operated in the cloud, include requirements that provide agencies with continuous visibility of the asset.
Workforce		
	Provide cloud-related training.	Agency IT staff should become familiar with Lean product management, ^b Agile development, continuous delivery, and automated infrastructure. Additionally, non-IT staff supporting privacy, security, and procurement should receive training in the multiple core disciplines outlined above.
	Plan for workforce development and training.	Agencies' cloud strategies and policies should also include a workforce development and planning component that tailors a transformation and training approach to that agency. In the event that an impact to the existing workforce has been identified, this approach should include a crosswalk of new skills and occupational categories with legacy occupational categories to foster clarity and ease of transition. Agencies should plan for ongoing education in this rapidly evolving field.
	Conduct skills gap analysis for future skill and position requirements for cloud-based services, and where appropriate, equip existing staff with the additional skills and knowledge needed.	Agency chief information officers, chief human capital officers and senior agency officials for privacy should collaboratively conduct a skills gap analysis that maps current IT workforce resources to future skill and position requirements. Agencies should identify potential skills gaps that may emerge as a result of a transition to cloud-based services, and, where needed, equip their existing staff with additional skills and knowledge to keep up with the ever-expanding list of technology options available to procure and deploy.
	Conduct regular evaluations of customer experience and user needs.	Agencies should conduct regular evaluations of customer experience and user needs to ensure that their solutions successfully foster efficiency, accessibility, and privacy.
	Execute communication plans regarding changes affecting employees.	Agencies should execute communication plans that help employees understand the changes that will occur.

Source: GAO analysis of the Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-22-104070

^aDevSecOps are not mutually exclusive to Agile, but in this report, this resource is included under the category of Agile development because it supports Agile software development.

^bLean and Agile are related philosophies. Lean can be characterized as related to Agile because the Lean practice and principles can be mapped to Agile methods.

OMB Guidance on Application Rationalization

OMB requires agencies to assess which applications are best suited for the cloud using application rationalization. Application rationalization is the effort to strategically identify business applications across an organization to determine which should be kept, replaced, retired, or consolidated. This includes developing a detailed inventory with attributes and functionality, determining business value and total cost of ownership, and then comparing or rationalizing that inventory of applications as a whole to eliminate redundancies, lower costs, and maximize efficiency. Application rationalization drives improved IT portfolio management

capabilities, empowers leaders to make better decisions, and enhances the delivery of key mission and business services.

In March 2012, OMB launched the PortfolioStat initiative which required agencies to conduct an annual review of their commodity IT portfolio to, among other things, achieve savings by identifying opportunities to consolidate investments or move to shared services.¹⁶ In a subsequent memorandum, OMB advocated for the use of application rationalization in order to optimize agencies' data center consolidation efforts.¹⁷ OMB's guidance stated that application rationalization would become a focus of the PortfolioStat sessions and required agencies to describe their approach to maturing the IT portfolio, including rationalizing applications, in the agency's information resource management plans and enterprise roadmaps (that were required to be updated annually).

Subsequently, in June 2019, OMB required all federal agencies to rationalize their application portfolios to drive cloud adoption. OMB's cloud strategy noted that the CIO Council would develop best practices and other resources to support rationalization efforts.

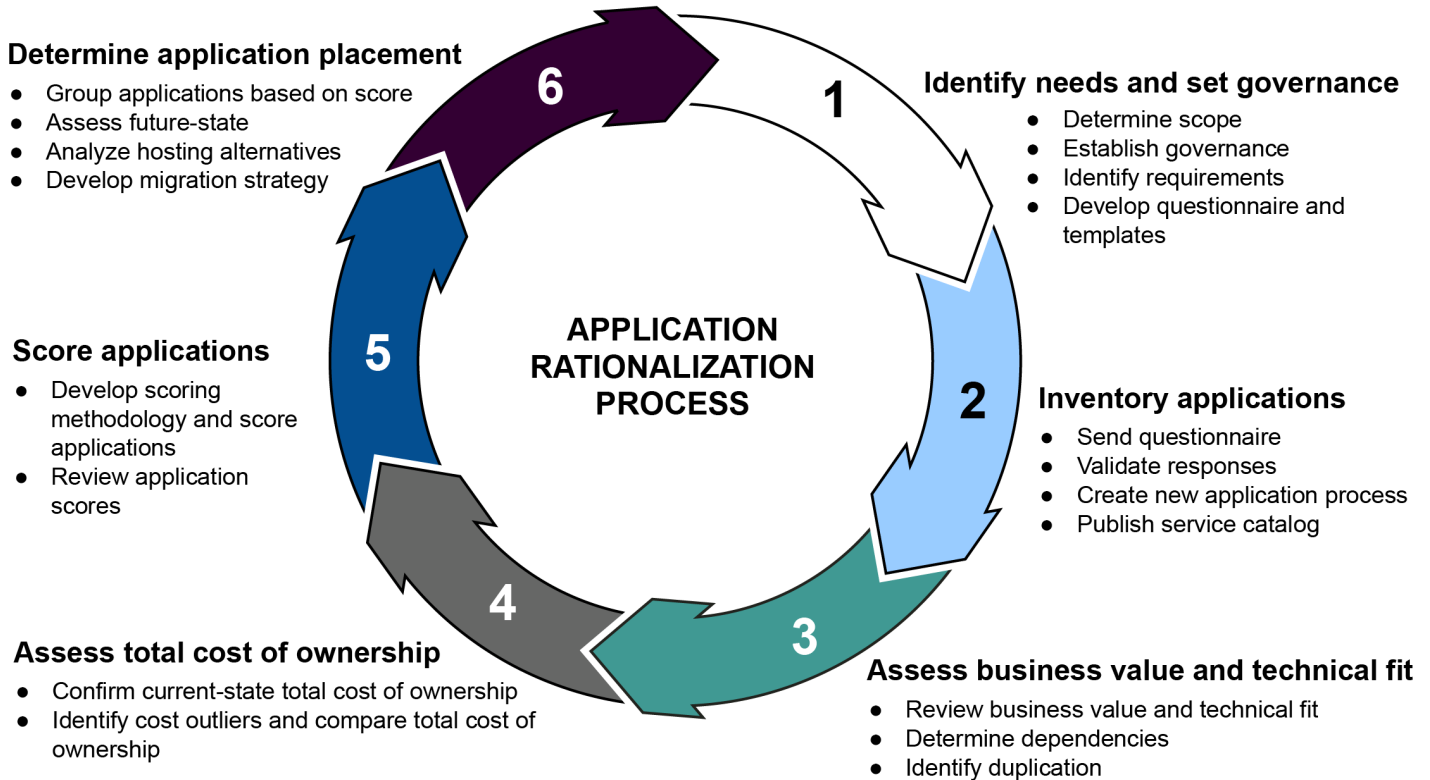
In June 2019, the CIO Council released *The Application Rationalization Playbook* to assist agencies with implementing the application rationalization process to decide which applications belong in the cloud.¹⁸ The playbook included a six-step process with discrete actions for agencies to consider when undergoing application rationalization. Agencies were encouraged to tailor these steps to meet organizational structures, unique requirements, and mission needs. Figure 1 outlines the six-step process noted in the CIO Council's playbook.

¹⁶Office of Management and Budget, *Implementing PortfolioStat*, M-12-10 (Washington, D.C.: Mar. 30, 2012).

¹⁷Office of Management and Budget, *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management*, M-13-09 (Washington, D.C.: Mar. 27, 2013). While OMB advocated for the use of application rationalization in its memorandum, it did not define a process or propose steps for carrying it out.

¹⁸CIO Council, *The Application Rationalization Playbook: An Agency Guide to Portfolio Management* (June 2019).

Figure 1: CIO Council’s Six-step Application Rationalization Process Outlined in *The Application Rationalization Playbook: An Agency Guide to Portfolio Management*



Source: GAO analysis of Chief Information Officer Council *Application Rationalization Playbook*. | GAO-22-104070

OMB Guidance Focuses on TBM Implementation

Starting in fiscal year 2019, OMB began requiring agencies to use TBM cost categories to report spending on agency investments, including cloud investments, as part of the annual budget process.¹⁹ First established by the TBM Council, TBM is a framework focused on providing technology, finance, and business leaders with standards for managing the value that IT brings to their organizations.²⁰ According to the TBM Council’s *TBM Taxonomy, Version 3.0* (referenced in OMB

¹⁹Office of Management and Budget, *FY 2019 IT Budget–Capital Planning Guidance*.

²⁰The TBM Council is a non-profit professional organization established in 2012 with a stated mission to advance the discipline of TBM through education, standards, and collaboration. The council is governed by an independent board of directors comprised of 20 CIO executive directors.

guidance), TBM provides a standard taxonomy to describe cost sources, technologies, IT resources (IT towers), applications, and services.²¹ The TBM Council's taxonomy is comprised of four layers of cost categories, including cost pools; IT towers; products and services; and business units and capabilities.

OMB's guidance noted that, by requiring agencies to report their spending data using the framework's cost categories, agencies would have a cost taxonomy to use to manage the cost, quality, and value of their IT services. In addition, OMB's guidance noted that using these cost categories would increase the granularity in reporting of agency IT budget and spending data.

As part of OMB's implementation of TBM across the federal government, agencies were required to use two of the four layers identified in the TBM Council's taxonomy—cost pools and IT towers—for the annual budget submission.²² As noted in the *TBM Taxonomy, Version 3.0*, this includes:

- **Cost pools.** A classification of IT spending comprised of low level categories that make cost allocations easier by revealing the composition of costs. For example, application total cost of ownership can be broken down into hardware, software, internal and external labor, outside services, facilities, and telecom costs. There are nine available cost pool categories.
- **IT towers.** A classification of IT spending comprised of resources or building blocks of specific IT applications. Examples of IT towers include compute (e.g., servers, mainframes), networks, applications (e.g., application development, application support and operations) and IT management. There are eleven available IT tower categories.

Recognizing that each agency had a different level of maturity, capability, and resources, OMB's guidance noted that agencies' implementation of the two layers would occur over a 3-year time period, from fiscal year 2019 through fiscal year 2021. In doing so, OMB reported that the extended time frame would afford agencies the opportunity to understand

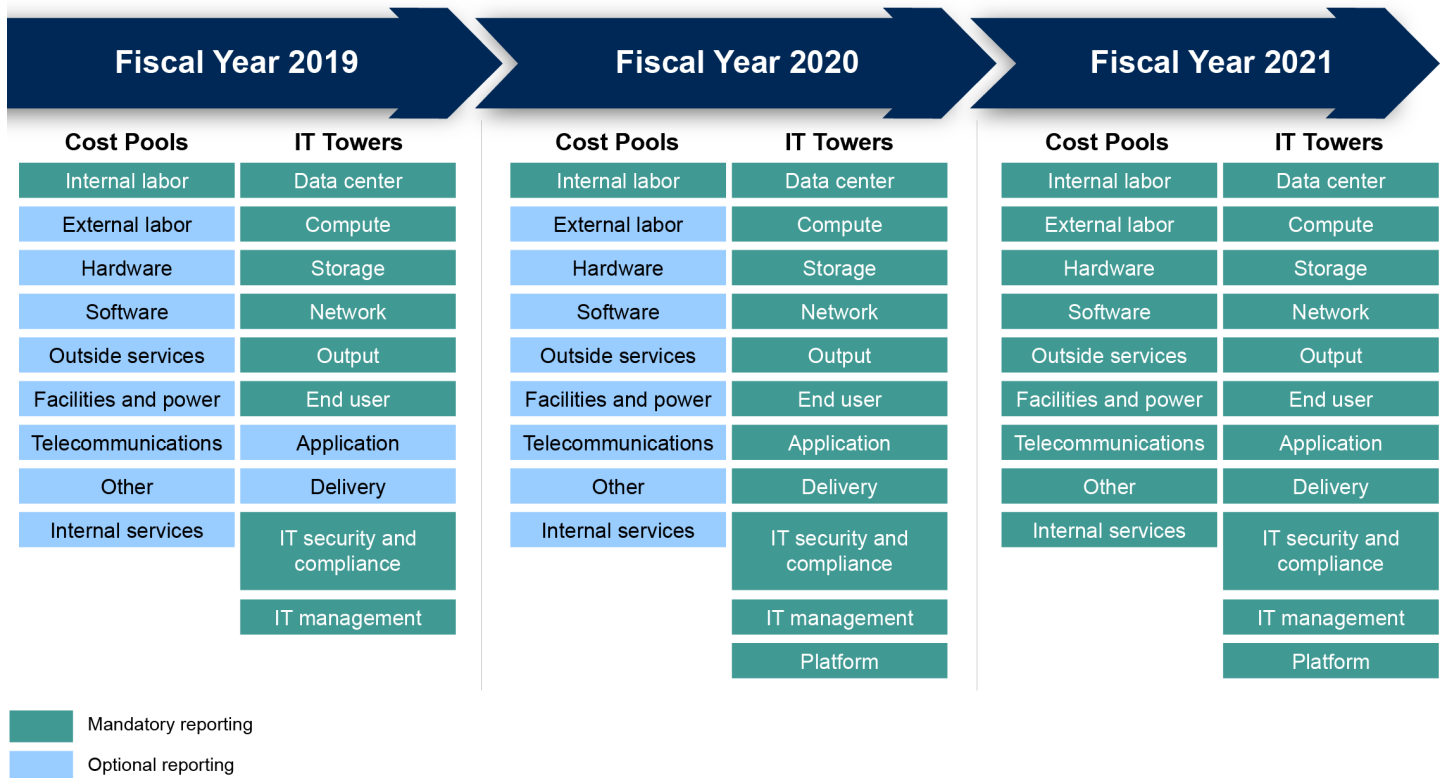
²¹Technology Business Management Council, *TBM Taxonomy, Version 3.0* (Nov. 2, 2018). Copyright © 2020 Technology Business Management Council.

²²OMB's guidance does not currently require agencies to use the TBM Council's cost categories related to reporting spending for: (1) products and services, and (2) business units and capabilities.

the challenges associated with implementation and work directly with OMB before all TBM data were required.

Specifically, during this 3-year period, agencies would be required to begin allocating investment spending to specified cost pools and IT towers and reporting these allocations to OMB. OMB's guidance noted that reporting costs for the specified cost pool and IT tower categories was mandatory in certain fiscal years, while reporting costs for the remaining cost pool and IT tower categories was optional. Subsequently, each fiscal year, OMB would require additional cost pool and IT tower categories for agencies to allocate and report spending on for their investments. However, OMB's guidance encouraged agencies to report spending associated with the optional cost pool and tower categories each fiscal year even though it was not required. Figure 2 outlines OMB's reporting requirements for TBM cost pools and IT towers for fiscal years 2019 through 2021 for federal agencies.

Figure 2: OMB’s Reporting Requirements for Technology Business Management IT Cost Pools and IT Towers for Federal Agencies, Fiscal Years 2019 through 2021



Source: GAO analysis of Office of Management and Budget guidance. | GAO-22-104070

OMB planned to make the agency-provided TBM data publicly available on the IT Dashboard beginning in fiscal year 2021. According to OMB’s guidance, OMB anticipated that agencies’ implementation of the framework would provide significant value for agency CIOs, who would be in a position to leverage existing industry benchmarking data and share identified best practices government-wide. OMB’s guidance noted that it would continue to be a strong partner to agencies in promoting consistent improvements in data quality and effective IT oversight.

In addition, the General Services Administration and the Department of Education released a TBM playbook in February 2019 that was designed to assist federal agencies as they began the framework’s

implementation.²³ In particular, the playbook offered guidance and lessons learned as well as a number of strategies that would improve the chances of successful implementation, including that agencies:

- Have a dedicated implementation team that would drive change through the collection, analysis, reporting, and an informed review of the data.
- Provide educational opportunities, including resources and training, to key players and stakeholders to help everyone understand common TBM terminology and definitions.

The TBM playbook also noted that agencies should tailor their implementation activities to achieve their organization's desired outcomes.

DOD's Cloud and Rationalization Roles, Responsibilities, and Previous Efforts

DOD is a complex organization and the largest U.S. government department. In support of its military operations, DOD manages many IT investments, including investments in business, communications, and command and control systems. The department spends billions of dollars annually to build and maintain these systems. In fiscal year 2022, DOD plans to spend approximately \$38.6 billion on unclassified IT investments.²⁴ DOD reported that this included approximately \$1.1 billion in funding for cloud services and migration, with \$798 million for commercial or in-house cloud services, and \$329 million in costs related to migrating systems to cloud services.²⁵

Over the past decade, DOD has worked on multiple efforts for cloud computing in accordance with the laws, department policies, and strategies that assigned roles and responsibilities for cloud and rationalization efforts throughout the department. The DOD CIO is ultimately responsible for the department's information enterprise, including eliminating duplicative IT within and between department components and identifying opportunities for IT efficiencies. However,

²³General Services Administration and Department of Education, *Technology Business Management Playbook* (Feb. 2019).

²⁴As part of the annual budget submission process, the department uses SNaP-IT to submit its budget to OMB, including spending allocated to TBM cost categories, and to publish the annual IT budget estimate to Congress. The DOD CIO's office also uses the system to submit monthly IT performance reports to the IT Dashboard.

²⁵Based on our review of the six DOD components' TBM data, there is increased likelihood that the department's spending on cloud services is underreported.

federal law and DOD policy has assigned IT responsibilities to other, non-CIO stakeholders as well.²⁶ For example, the OUSD (A&S) is responsible for developing policies for the acquisition and development of new IT systems. As a result, the CIO collaborates and coordinates with stakeholders in various committees and working groups when implementing significant cloud or rationalization efforts.

In 2010, the Secretary of Defense announced the creation of the Joint Information Environment to consolidate the department's disparate networks and systems. In 2013, the department developed the Joint Information Environment Execution Strategy,²⁷ which elaborated on the initiative and identified both cloud computing and application rationalization as key to the department's consolidation and optimization goals. The execution strategy reinforced the CIO's position as the primary official responsible for DOD's IT, but assigned implementation responsibilities to an executive committee chaired by the CIO, the Joint Chiefs of Staff, and U.S. Cyber Command.

Moreover, in July 2012, the DOD CIO issued the *DoD Cloud Computing Strategy*, which aligned the department with federal requirements²⁸ to consider cloud options before making new IT investments.²⁹ The department's strategy noted that the DOD CIO was committed to providing a secure, resilient enterprise cloud environment through an alignment with department-wide IT efficiency initiatives, federal data center consolidation, and cloud computing efforts. The strategy also identified steps necessary for the department's transition to an enterprise wide cloud environment.

Additionally, in December 2018, the strategy was updated to align with the department's implementation of an enterprise cloud environment.³⁰ The enterprise cloud environment included the Joint Enterprise Defense

²⁶See e.g. 10 U.S.C. § 4571 note (2019) (Authority for Continuous Integration and Delivery of Software Applications and Upgrades to Embedded Systems).

²⁷Department of Defense, *The Department of Defense Strategy for Implementing the Joint Information Environment* (Sept. 18, 2013).

²⁸Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management*.

²⁹Department of Defense, *DoD Cloud Computing Strategy* (July 2012).

³⁰Department of Defense, *DoD Cloud Strategy* (Dec. 2018).

Infrastructure, which focused on a commercially available cloud service solution. However, after awarding the contract to cloud service provider, in July 2021, the department cancelled the contract because of DOD's evolving requirements and the department's decision to pursue a multi-vendor approach to meet its needs.³¹ In addition, the updated strategy noted that the DOD CIO would develop written guidance on the implementation plans for rationalization, and accelerating the department's migration toward an enterprise cloud solution.

Further, in July 2019, the department issued its *DoD Digital Modernization Strategy*,³² which outlined the DOD CIO's vision for the department's future digital environment and provided a roadmap for modernizing its cloud infrastructure, among other things. A key objective within the first goal of the strategy was to deliver a department enterprise-wide cloud environment, which would leverage commercial innovation. In addition, the strategy noted that the department would optimize its IT by, in part, rationalizing applications for migration to the cloud. The Digital Modernization Infrastructure Executive Committee leads the strategy's implementation efforts, and is led by the same chairs as the Joint Information Environment Executive Committee.

Subsequently, in May 2021, the department published its *Department of Defense Outside the Continental United States Cloud Strategy*,³³ which established goals and objectives for modernizing the department's infrastructure that supported military missions and humanitarian efforts overseas using innovative cloud solutions. The strategy noted that the DOD CIO and the Joint Chiefs of Staff would co-lead the development of an enterprise cloud architecture for this environment and develop an implementation plan to ensure coordinated execution of the strategy's modernization activities.

³¹The department awarded a contract to a commercial cloud service provider in October 2019. During the contract award process, there were both pre-award and post-award bid protests. Due to these ongoing post-award bid protests, the department had not yet begun implementation of the Joint Enterprise Defense Infrastructure contract at the time of its cancellation.

³²Department of Defense, *DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY19-23* (July 12, 2019).

³³Department of Defense, *Department of Defense Outside the Continental United States Cloud Strategy* (May 26, 2021).

More recently, in February 2022, the department published its *Department of Defense Software Modernization Strategy*,³⁴ which replaced the department's 2018 cloud strategy. One of the key goals was to accelerate the DOD enterprise cloud environment as the foundation for software modernization using a multi-cloud, multi-vendor approach. The Software Modernization Senior Steering Group leads the implementation of the software modernization activities supporting the strategy and is chaired by the DOD Deputy CIO for Information Enterprise, a senior representative from OUSD (A&S), and a senior representative from the Office of the Under Secretary of Defense for Research & Engineering.

The steering group chairs' responsibilities include creating performance measures, and developing and maintaining an annual action plan to implement the goals and objectives of the strategy, among other things. In addition, the strategy noted that the department would: (1) mature an innovative portfolio of cloud contracts, (2) secure data in the cloud, (3) accelerate cloud adoption through automated design patterns, and (4) prepare the department's infrastructure outside the continental United States for cloud.

Prior GAO and OIG Reports Reviewing DOD's Adoption of Cloud Services, Portfolio Management, and Rationalization Activities

From 2014 to 2022, we and the department's OIG issued multiple reports on DOD's efforts to implement cloud services, portfolio management, and rationalization activities. For example, in December 2018, DOD's OIG found that divisions and commands in three of the military services did not consistently rationalize their software applications.³⁵ Officials in the OIG attributed their finding in part to some divisions and commands lacking a process for eliminating duplicative or obsolete software applications and in part to none of the commands or divisions maintaining accurate software inventories.

The OIG recommended that the DOD CIO develop an enterprise-wide application rationalization process, establish guidance requiring components to conduct application rationalization, and conduct periodic reviews to ensure that components regularly validate their software inventories. While DOD did not comment on the recommendations, officials from the OIG reported that the department took action to implement the recommendations related to developing an enterprise-wide

³⁴Department of Defense, *Department of Defense Software Modernization Strategy* (Feb. 2, 2022).

³⁵Department of Defense Office of Inspector General, *DoD Management of Software Applications*, DODIG-2019-037 (Dec. 13, 2018).

application rationalization process and establishing guidance on application rationalization. The recommendation for conducting reviews to validate its software inventories remains open, according to OIG officials.

In April 2019, we reviewed 16 agencies (including DOD), and found that DOD had not completed an assessment of 237 cloud investments.³⁶ Specifically, DOD noted that inconsistent reporting of cloud investments and investment consolidation had impacted its reported percentage. Further, while DOD reported that it had increased its cloud service spending since 2015, the department also identified issues in tracking and reporting cloud spending and savings data, including not having consistent processes in place to do so.

We therefore recommended that DOD complete an assessment of all IT investments for suitability for migration to a cloud computing service, and establish a consistent and repeatable mechanism to track savings and cost avoidances from the migration and deployment of cloud services. DOD concurred with our recommendation to complete an assessment of all IT investments, but disagreed with our recommendation to establish a mechanism to track cost savings. As of April 2022, DOD had not implemented either recommendation.³⁷

In March 2022, the Army Audit Agency found that Army organizations did not consistently rationalize their IT applications before migrating them to the cloud.³⁸ Specifically, the audit agency found that the Army did not rationalize 44 percent of the systems it reviewed (with a combined \$915.9 million in programmed costs) before migrating them to the cloud.

The Army Audit Agency cited a lack of detailed rationalization processes and procedures, as well as a lack of a cloud-specific workforce, and noted that the lack of consistent rationalization hinders DOD's ability to achieve its Digital Modernization Strategy goals. The Army Audit Agency recommended that the Army CIO develop rationalization guidance, require organizations to periodically reassess their systems, and establish

³⁶[GAO-19-58](#).

³⁷Starting in fiscal year 2023, OMB will no longer require agencies to report information related to completing assessments of investments for cloud services. As a result, we have closed the recommendation to the department in this area.

³⁸U.S. Army Audit Agency, *Cloud Migration*, Report A-2022-0033-IIZ (Mar. 14, 2022).

rationalization training. The Army CIO concurred with the recommendations.

For more details on prior GAO and OIG reports issued from 2014 through 2016 related to DOD's cloud services, portfolio management, and rationalization activities, see appendix II.

DOD's Plans Address Most OMB Cloud Computing Requirements, but Gaps in Workforce Remain

OMB's *Federal Cloud Computing Strategy*, issued in June 2019, identified 14 key requirements for agencies to implement to help ensure successful cloud adoption and implementation.³⁹ The requirements were intended to bolster federal IT modernization efforts by improving the return on investment, providing enhanced security, and producing higher quality services for users. The requirements were grouped into three primary areas:

- **Security.** Agencies should modernize their security policies to focus on risk-based decision making, automation, and moving protections closer to the data layer in addition to the network and physical infrastructure layers.
- **Procurement.** Agencies should improve their ability to purchase cloud solutions through repeatable practices and shared knowledge of acquisition principles and risk management practices.
- **Workforce.** Agencies should identify skill gaps, retrain current staff, and recruit key talent external and internal to the department for cybersecurity, acquisition, and cloud engineering.

DOD has fully addressed 11 of the 14 requirements. Specifically, DOD fully addressed all four requirements in the area of security, all five in procurement, and two of the five in workforce.⁴⁰ In particular, officials in the DOD's Office of the CIO reported that the department used a combination of policies, directives, and other guidance to meet the requirements outlined in OMB's guidance. This included strategies related to digital modernization and software modernization, both of which, DOD officials noted, detailed the department's planned enterprise-wide cloud

³⁹Office of Management and Budget, *Federal Cloud Computing Strategy* (2019).

⁴⁰While OMB's guidance is not specific regarding how agencies should address these requirements, our assessment focused on whether DOD had developed policies and other guidance that addressed these requirements because OMB Circular A-130 requires agency CIOs to define policies and processes in sufficient detail for all information resources. See Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (July 28, 2016).

strategy.⁴¹ In addition, there were also strategies related to identity, credential, and access management and DevSecOps,⁴² as well as directives and a cloud acquisition guidebook.⁴³

The results of our assessment of DOD’s guidance and other documentation for OMB’s cloud requirements within the primary areas are summarized in table 2.

Table 2: Extent to Which Department of Defense (DOD) Guidance Has Addressed the 14 OMB Key IT Cloud Requirements

Area	Key requirement	Assessment	Summary of assessment
Security			
	Implement identity, credential, and access management.	Fully addressed	DOD’s digital modernization strategy identified goals for implementing identity, credential, and access management to support rapid access to mission information, strengthen responsible information sharing, and support greater effectiveness and efficiency through migration to the cloud. In addition, the department’s March 2020 strategy on identity, credential, and access management identified an objective that stated that these capabilities must be deployed to support cloud services. This included acquiring, testing, and deploying these capabilities to accelerate a rapid and secure adoption of cloud capabilities.
	Use mature Agile development practices including development, security, and operations.	Fully addressed	DOD’s digital modernization strategy identified elements related to Agile including DevSecOps (an iterative software development approach ^a), for delivering a department enterprise cloud environment. The elements included developing policies and guidance for modernizing, as well as effective application, of DevSecOps principles. In addition, the department’s guidance on enterprise DevSecOps noted that cloud migration required the adoption of new architectural design patterns and would build upon existing enterprise services to prevent the creation of duplicative capabilities.
	Perform continuous monitoring.	Fully addressed	DOD’s guidance on cloud acquisition stated contractor service level agreements were to include requirements for contractors to continuously monitor cloud services. The department’s software modernization strategy emphasized that continuous monitoring was necessary to address evolving cybersecurity issues and to keep up with successful software modernization.

⁴¹Department of Defense, *DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY19-23*; and *Department of Defense Software Modernization Strategy*.

⁴²Department of Defense, *Identity, Credential, And Access Management (ICAM) Strategy* (Mar. 30, 2020); *DoD Enterprise DevSecOps Strategy Guide Version 2.1* (Oct. 19, 2021); and Defense Acquisition University, *DoD Cloud Computing Acquisition Guidebook Version 1.2* (Nov. 5, 2019).

⁴³Department of Defense, *Cybersecurity*, DOD Instruction 8500.01 (Oct. 7, 2019); *Cybersecurity Activities Support to DoD Information Network Operations*, DOD Instruction 8530.01 (July 25, 2017); *DoD Continuity Policy*, DOD Directive 3020.26 (Feb. 14, 2018); and *DoD Chief Information Officer (DoD CIO)*, DOD Directive 5144.02 (Sept. 19, 2017).

Area	Key requirement	Assessment	Summary of assessment
	Update business continuity and disaster recovery plans.	Fully addressed	DOD's guidance included a requirement for developing and updating business continuity and disaster recovery plans related to its IT systems for the continuation of service. Specifically, the department's continuity policy required each component within the department to certify that it was meeting the requirements of the continuity plan as appropriate. In addition, the department's cybersecurity directive required each component head to develop contingency plans and conduct exercises for an emergency interruption of service.
Procurement			
	Ensure the agency's chief information officer oversees modernization.	Fully addressed	DOD's directive on the CIO identified the CIO with the responsibility for the department's information enterprise. In addition, the department's digital modernization strategy stated that the DOD CIO was responsible for the department's information enterprise.
	Have cloud service-level agreement in place.	Fully addressed	DOD's guidance on cloud acquisition identified that service level agreements should require continuous monitoring to maintain the security and performance of applications. The guidance also specified that these agreements were to include roles and responsibilities of all parties and clear definition of performance measures conducted by contractors, such as level of service and response time. In addition, contractors were to provide for disaster recovery and continuity of operations planning and testing, including how and when the cloud service provider was to report such failures and outages to the agency.
	Standardize cloud contract service level agreements.	Fully addressed	DOD's guidance on cloud acquisition identified standardized language and specific contract clauses that were to be used in service level agreements in order to provide effective, efficient, and secure cloud procurement.
	Iteratively improve agency policies and guidance.	Fully addressed	DOD's guidance designates the department's CIO as the entity responsible for improving policies to increase program efficiency and effectiveness and managing and overseeing its information enterprise. Based on our review of the department's documentation related to its cloud strategy, the department does take an iterative approach to improving its policies and guidance. For example, the DOD's new guidance on software modernization builds upon existing department strategies and themes related to software, among other things.
	Ensure continuous visibility in high value asset contracts.	Fully addressed	DOD's guidance on IT risk management required the categorization of department systems identified as high value assets, including those managed and operated in the cloud. In addition, the guidance assigned component heads with the responsibility of ensuring contracts include specific requirements that would provide continuous visibility of the identified high value asset.
Workforce			
	Provide cloud-related training.	Fully addressed	DOD's Software Workforce Working Group, in response to the <i>National Defense Authorization Act of Fiscal Year 2020</i> , provided an initial catalogue of software acquisition and software development education and training. The training included Agile development and Lean software development, ^b as well as continuous delivery.
	Plan for workforce development and training.	Fully addressed	DOD's digital modernization strategy focused on a workforce and development component that included training, new skills, and occupational categories. In addition, the software modernization strategy stated that a fundamental activity that was required for maintaining a cloud environment was to identify, train, and engage resources to create a robust and sustainable cloud workforce.

Area	Key requirement	Assessment	Summary of assessment
	Conduct skills gap analysis for future skill and position requirements for cloud-based services, and where appropriate, equip existing staff with the additional skills and knowledge needed.	Partially addressed	DOD guidance identified the need for conducting skills gap analysis for transitioning to the cloud but the department had not conducted this analysis as of April 2022. Specifically, the department's January 2021 report to Congress identified skills specific to IT areas including two software roles that referenced cloud skills. A DOD official in the Office of the Under Secretary of Defense for Acquisition & Sustainment stated in January 2021 that the department had begun conducting gap analyses for two new occupational series related to software engineering and software development, which would address cloud computing architecture roles. The official stated that the goal would be to have a role for a chief software engineer, who would be required to have knowledge of cloud architecture. In addition, officials in DOD's Office of the CIO reported in January 2021 that the department intended to update its cloud IT workforce planning document, the <i>Defense Cyber Workforce Framework</i> , to include a new software occupational series. While a copy of the framework was provided in March 2022, the role of the software developer did not include any language related to cloud services and the framework did not include a role for a software engineer. In addition, DOD officials did not provide a time frame for including cloud related positions or skills in its workforce framework.
	Conduct regular evaluations of customer experience and user needs.	Partially addressed	Although DOD officials in the Office of the CIO and the Office of the Under Secretary of Defense for Acquisition & Sustainment identified examples of collection efforts on internal and external customer experiences and satisfaction that had been conducted across the department as of April 2022, these officials said that these activities were not happening consistently throughout the department. For example, a department official in the Office of the CIO stated that data collection efforts were underway to collect customer feedback, suggestions, and website performance, among other things. The official noted that the department's efforts included surveys performed by other agencies on behalf of DOD, including the Defense Finance and Accounting Service's annual customer experience and satisfaction survey, which was used to improve processes, products, and services provided to its users. In addition, DOD's Deputy Director for Enterprise Capabilities in the CIO's office stated that surveys or evaluations of customer experience would generally be performed by the military service branches and other department components. However, the official was not aware whether all of these components had implemented practices to gather customer feedback related to their experiences and needs. Further, according to a DOD official in the Office of the Under Secretary of Defense for Acquisition & Sustainment, the office did not conduct surveys of its workforce and the officials were not aware of any working groups that were performing surveys.
	Execute communication plans regarding changes affecting employees.	Not addressed	As of April 2022, DOD had not executed communication plans to provide information to employees regarding changes related to moving to an enterprise-wide cloud environment. According to DOD's Deputy Director for Enterprise Capabilities, although a formal communication structure had not been developed, several established groups shared information about cloud related changes. For example, the department's digital modernization strategy and the Digital Modernization executive committee communicated cloud-related information to aid the department's alignment with its cloud computing strategy. The official also stated that the Software Modernization Senior Steering Group's communication strategy included a standing weekly meeting to discuss cloud updates with the defense community, as well as the dissemination of various guidance and policy memos published by the department. However, department officials did not provide any documentation such as meeting minutes or other materials to support that changes were shared during meetings.

Legend: Fully addressed: DOD provided evidence that addressed the requirement; Partially addressed: DOD provided evidence that it had addressed some, but not all of the requirement; Not addressed: DOD did not provide evidence that it had addressed any of the requirement.

Source: GAO analysis of Department of Defense documentation and Office of Management and Budget's June 2019 *Federal Cloud Computing Strategy*. | GAO-22-104070.

^aDevSecOps are not mutually exclusive to Agile, but in this report, this resource is included under the category of Agile development because it supports Agile software development.

^bLean and Agile are related philosophies. Lean can be characterized as related to Agile because the Lean practice and principles can be mapped to Agile methods.

DOD officials in the Office of the CIO and OUSD (A&S) provided a number of reasons for the shortfalls in the three workforce requirements. Specifically, an official in the DOD CIO's office reported that a gap analysis for skills related to cloud computing was not conducted because that office was not directed to do so. The official also stated that such an assessment would be difficult to complete because the department had not yet identified a work role for the cloud related skills. Further, the official from the Office of the CIO stated that before they could identify additional skills or training necessary for cloud computing, they would need to complete their required review of the cybersecurity workforce, complete a gap analysis, and compare the results to industry standards.

In addition, DOD's Deputy Director for Enterprise Capabilities in the CIO's office stated in April 2022 that the department's current approach was based on maximizing the use of existing authorities and workforce flexibilities to tailor recruitment, reskilling, and retention mechanisms to better support the department's emerging workforce needs. The department official stated that it was impractical and suboptimal to attempt to establish a new cloud specific occupational series because of the rapid changes to cloud technology.

Regarding the evaluations of customer experience and user needs, DOD's Deputy Director for Enterprise Capabilities noted that in April 2022 that individual programs, program executive offices, and portfolio leads were responsible for evaluating user needs and customer experience as part of software modernization efforts. The official noted that, while surveys or other mechanisms are commonly used, that information was not universally consolidated and reported at the enterprise level.

Regarding the execution of communication plans, according to DOD's Deputy Director for Enterprise Capabilities, the department does not have a centralized plan for communicating how cloud related changes would affect its employees across all of its systems and components. This is, in part, because there are different aspects of cloud adoption such as cloud hosting and end-user application modernization. In addition, the official stated that application and system program managers are responsible for following DOD guidance related to change management and end user

communication, including following requirements related to end user knowledge and abilities with new systems.

Officials in the DOD CIO's office have indicated that undertaking these workforce activities is generally the responsibility of lower level offices within the department. However, OMB directed agencies to implement these requirements at the enterprise level to ensure that IT modernization efforts related to cloud adoption would be strengthened across the federal government. In addition, if the department intends to use existing mechanisms to support its future workforce needs, it is unclear how they will determine what those needs are without performing a skills gap analysis.

Until DOD conducts a skill gap analysis to identify future staffing needs for cloud-based services, conducts evaluations of customer experience and user needs, and develops a communication plan that helps employees understand changes, the department will have difficulty anticipating and responding to changing IT staffing needs. This will increase the likelihood that DOD will face challenges in controlling human capital risks while developing, implementing, and operating its IT systems within the cloud environment.

DOD Has Taken Steps to Develop an Enterprise-Wide Application Rationalization Process, but Lacks a Long-Term Implementation Plan

Since OMB began requiring agencies to rationalize their application portfolios in June 2019, DOD has reported making progress in implementing an enterprise-wide application rationalization effort. DOD has done so by establishing a scope for its rationalization efforts and working to formalize a governance group with the authority to set rationalization requirements and issue related guidance. However, these efforts do not address all of the activities that comprise the first step of the CIO Council's six-step process on leading practices for implementation of application rationalization. As of April 2022, the department had not finalized a charter formalizing the governance group, identified what requirements will be put in place for DOD components, or determined what department data will be needed for the rationalization process. According to the CIO Council's playbook, those are key activities that should be completed in Step 1 in order for the rest of the steps to be successful.

In addition, as of April 2022, DOD had not yet established a plan to develop and implement an enterprise-wide rationalization process with measurable objectives, milestones, and timelines. The department's efforts have been impacted by significant changes in DOD's approach for rationalization over the past 2 years, and by long time frames for

implementing new department initiatives. DOD also lacks a definition of who is responsible within the department for ensuring application rationalization is successful and for setting goals and performance metrics to measure that success.

DOD Has Partially Implemented the First Step of an Enterprise-Wide Application Rationalization Process

OMB's *Federal Cloud Computing Strategy* directs all federal agencies to rationalize their application portfolios to drive cloud adoption by assessing the need for and usage of applications; and discarding obsolete, redundant, or overly resource-intensive applications.⁴⁴ Further, the CIO Council's *The Application Rationalization Playbook* recommends a six-step rationalization process. Step 1 of this process (identify needs and set governance) is comprised of four activities: 1) establish rationalization scope, 2) set transparent and inclusive governance structures, 3) identify rationalization requirements, and 4) develop questionnaire and templates.⁴⁵

In laying out leading practices for application rationalization in its six-step process, the CIO Council's Playbook notes that the success of the overall rationalization process and the implementation of subsequent process steps depend on the successful completion of the activities in the first step. These activities are codifying governance with clear ownership, objectives, and procedures, as well as determining the information to be collected from applications. In addition, the CIO Council's Playbook states that rationalization efforts should prioritize mission support applications, such as human resource applications, over mission-specific applications. Further, the playbook states that agencies should tailor the steps to meet an organization's structure, requirements, and mission needs.

Of the four activities in Step 1 (identify needs and set governance), DOD has addressed one, partially addressed another, and not addressed the remaining two. DOD's implementation of the four activities included in step 1 are summarized in table 3.

⁴⁴Office of Management and Budget, *Federal Cloud Computing Strategy* (2019).

⁴⁵CIO Council, *The Application Rationalization Playbook: An Agency Guide to Portfolio Management*.

Table 3: Department of Defense (DOD) Implementation of CIO Council Application Rationalization Playbook Step 1: Identify Needs and Set Governance

Application rationalization playbook activity	GAO rating	GAO assessment
Establish rationalization scope by determining and prioritizing applications to rationalize.	Fully addressed	DOD's <i>System and Application Rationalization Execution Guidance</i> memo established the scope of the department's rationalization efforts to two of its four IT mission areas (Enterprise Information Environment and Business mission areas). ^a These mission areas consist of the support applications the CIO Council recommends prioritizing in the scope of the rationalization process.
Set transparent and inclusive governance structures by obtaining leadership buy-in and input from a diverse array of agency perspectives.	Partially addressed	DOD has enterprise-wide governance bodies in place to make application investment—including rationalization—decisions, such as the Digital Modernization Infrastructure Executive Committee and Defense Business Council. However, it does not have a governance body dedicated to setting rationalization requirements. DOD officials stated in March 2022 that they were working to charter an IT Portfolio Management Working Group that would have these authorities, but that the charter would not be formalized until April or May 2022. Subsequently, in April 2022, the same officials stated that these estimated time frames could be extended based on comments received from department stakeholders. As such, it is uncertain when a charter will be formalized.
Identify rationalization requirements by ensuring that the rationalization effort aligns to law, agency policies, and agency leadership priorities.	Not addressed	DOD officials stated that they are updating DOD's IT portfolio management policies and processes and plan to complete these efforts by December 2022. While DOD officials reported certain high-level requirements they plan to include in their new policy, the officials reported in March 2022 that the specific requirements would not be formalized until the new policy was completed in December 2022. Subsequently, in April 2022, the same officials stated that these estimated time frames could be extended based on comments received from department stakeholders. As such, it is uncertain when the new policy will be finalized.
Develop questionnaire and templates to collect information that will be required from each application.	Not addressed	DOD officials reported that the department planned to capture the relevant application data needed for the rationalization process by updating its existing IT system repository rather than developing a separate questionnaire and templates to collect the needed information. However, DOD officials reported in March 2022 that the department had not yet determined what additional information it would need from its applications or implemented a means to capture that information. In addition, they had not yet established a time frame for doing so.

Legend: Fully addressed: DOD provided evidence that addressed the requirement; Partially addressed: DOD provided evidence that it had addressed some, but not all of the requirement; Not addressed: DOD did not provide evidence that it had addressed any of the requirement.

Source: GAO analysis of DOD documentation. | GAO-22-104070

^aDepartment of Defense, *DOD System and Application Rationalization Execution Guidance* (Jan. 8, 2021).

Officials in the DOD's Office of CIO stated that the reason why they had not yet fully implemented the activities in first step of the rationalization process was because of changes to the department CIO's roles and responsibilities. Specifically, DOD officials stated that they had planned to determine enterprise-wide rationalization requirements and establish what information should be collected on each application by December 2021. However, Congress eliminated the Chief Management Officer position in

January 2021,⁴⁶ which led to the CIO gaining primary responsibility for the Business Mission Area in October 2021.⁴⁷ As a result, DOD officials reported that the time frames for completing all of these activities would be extended by a year or more.

However, as of May 2022, the department had not established firm timelines for when it would complete the activities noted in Step 1. In addition, since DOD has not completed the first step in the CIO Council's rationalization playbook, it is unable to implement the remaining steps and rationalize its application portfolio, as OMB required. Until DOD establishes enterprise-wide rationalization governance structure, identifies and documents all rationalization requirements in department policy, and determines the relevant information required on each application and the means to collect it, the department will lack the foundation needed for a successful rationalization effort. As a result, DOD will be less likely to effectively uncover duplicative applications and advance cloud adoption as OMB intended.

DOD Lacks a Long-Term Approach to Planning and Implementing Enterprise-Wide Application Rationalization

The CIO Council's *Playbook* on leading practices for application rationalization states that codified governance with clear objectives, procedures, ownership responsibilities, and leadership buy-in supports the overall success of application rationalization efforts.⁴⁸ In addition, our leading practices for federal agency reform efforts highlights the importance of having clear goals and performance measures, implementation timelines, and the means to hold leaders accountable for successful reform implementation.⁴⁹ Further, our *Standards for Internal*

⁴⁶William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 901, 134 Stat. 3388, 3794-95 (2021).

⁴⁷Deputy Secretary of Defense, *Disestablishment of the Chief Management Officer, Realignment of Functions and Responsibilities, and Related Issues* (Sept. 1, 2021). In addition to the CIO, the Chief Financial Officer (Comptroller) and the Under Secretary of Defense for Acquisition & Sustainment also gained additional responsibilities related to the business mission area.

⁴⁸CIO Council, *The Application Rationalization Playbook: An Agency Guide to Portfolio Management*.

⁴⁹GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, [GAO-18-427](#) (Washington, D.C.: June 13, 2018).

Control in the Federal Government recommends agency management clearly define objectives in specific and measurable terms.⁵⁰

DOD has taken some isolated actions to reduce duplication and improve efficiencies as part of application rationalization over the past few years. For example, the department has:

- Begun rationalizing enterprise-wide email and productivity tools across the department through the cloud-based Enterprise Collaboration and Productivity Suite,⁵¹ and is currently deploying the first of three capability sets.
- Begun rationalizing the networks of Defense Agencies and Field Activities through the Fourth Estate Network Optimization initiative.⁵²
- Issued a voluntary rationalization guide for components to use in their rationalization processes.⁵³

However, DOD has not yet established a plan to develop and implement an enterprise-wide rationalization process with measurable objectives, milestones, and timelines. Specifically, the department's efforts to develop this process have been impacted by the following factors:

- **DOD senior leadership has significantly changed its application rationalization approach over the past 2 years.** After the DOD OIG made a recommendation to develop an enterprise-wide process for conducting application rationalization in December 2018,⁵⁴ the Office of the CIO began working on developing a process, which was finalized in April 2020 (the *DoD System & Application Rationalization*

⁵⁰GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 9, 2014).

⁵¹The Enterprise Collaboration and Productivity Suite is an effort to consolidate components' individual collaboration and productivity systems, such as email, file sharing, and voice and video calls, into a single enterprise-wide cloud-hosted system. The first capability set, known as the Defense Enterprise Office Solution, is transitioning DOD components' email and collaboration tools to a cloud solution, and capability sets focus on voice and video collaboration.

⁵²The Fourth Estate Network Optimization initiative is an attempt to consolidate common IT network services, such as device asset management, wireless services, network architecture, and operations support, across DOD's non-military components (e.g. Defense Health Agency, Missile Defense Agency).

⁵³Department of Defense, *DoD System & Application Rationalization Guide* (Apr. 8, 2020).

⁵⁴DODIG-2019-037.

Guide). Subsequently, the department formed an informal Application and System Rationalization Working Group in summer 2020 to assist with implementing the rationalization activities noted in the guide.

The CIO formalized the working group's charter in January 2021, and charged it with establishing objectives and metrics for enterprise-wide rationalization. However, after Congress eliminated the department's Chief Management Officer position in January 2021, the DOD CIO and other senior leadership decided to change their approach from rationalization to focus on a broader enterprise-wide IT portfolio management effort, which would include application rationalization as a component. In March 2021, an IT Portfolio Management Working Group began meeting to work on IT portfolio management efforts and the application rationalization working group was disbanded (2 months after its formalization). Although officials in the DOD CIO's office stated the IT Portfolio Management Working Group would complete the rationalization working group's efforts and establish objectives and milestones for the department, they had not done so as of April 2022.

- **DOD's efforts to implement change and manage enterprise-wide initiatives involve long time frames.** For example, following the OIG's recommendation in December 2018, it took the DOD CIO approximately 16 months to address the recommendation by issuing guidance on an enterprise-wide rationalization process. In addition, although the department's rationalization group began meeting in summer 2020, it took 6 months for the group to be formally established by charter. Likewise, although the IT Portfolio Management Working group began meeting in March 2021, the group had still not been formally chartered more than a year later and no deliverables have been finalized as of April 2022.

In addition, when DOD made changes to its rationalization effort in March 2021, it pushed back the timelines for completing initial activities, including modifying the department's system repository to collect information necessary for rationalization, and has still not updated those timelines more than a year later. Further, in March 2022, officials in DOD's Office of the CIO reported that the department would not update its policy to govern IT portfolio management and application rationalization until December 2022. Subsequently, in April 2022, the official stated that the estimated time frames provided to us for the finalization of the working group charter and the new IT portfolio management policy could be extended based on comments received from department stakeholders.

-
- **DOD leadership has not clearly defined who is responsible for ensuring application rationalization is successful or identified goals and performance metrics to measure success.** Although federal law and DOD policy assign the department CIO responsibility for reducing IT duplication and identifying IT efficiencies,⁵⁵ it is unclear who within the department has responsibility for implementing application rationalization. For example, in July 2020, 3 months after the department CIO released enterprise-wide guidance, officials in the Office of the CIO reported to us that it was optional for DOD components whether they chose to follow the guidance.

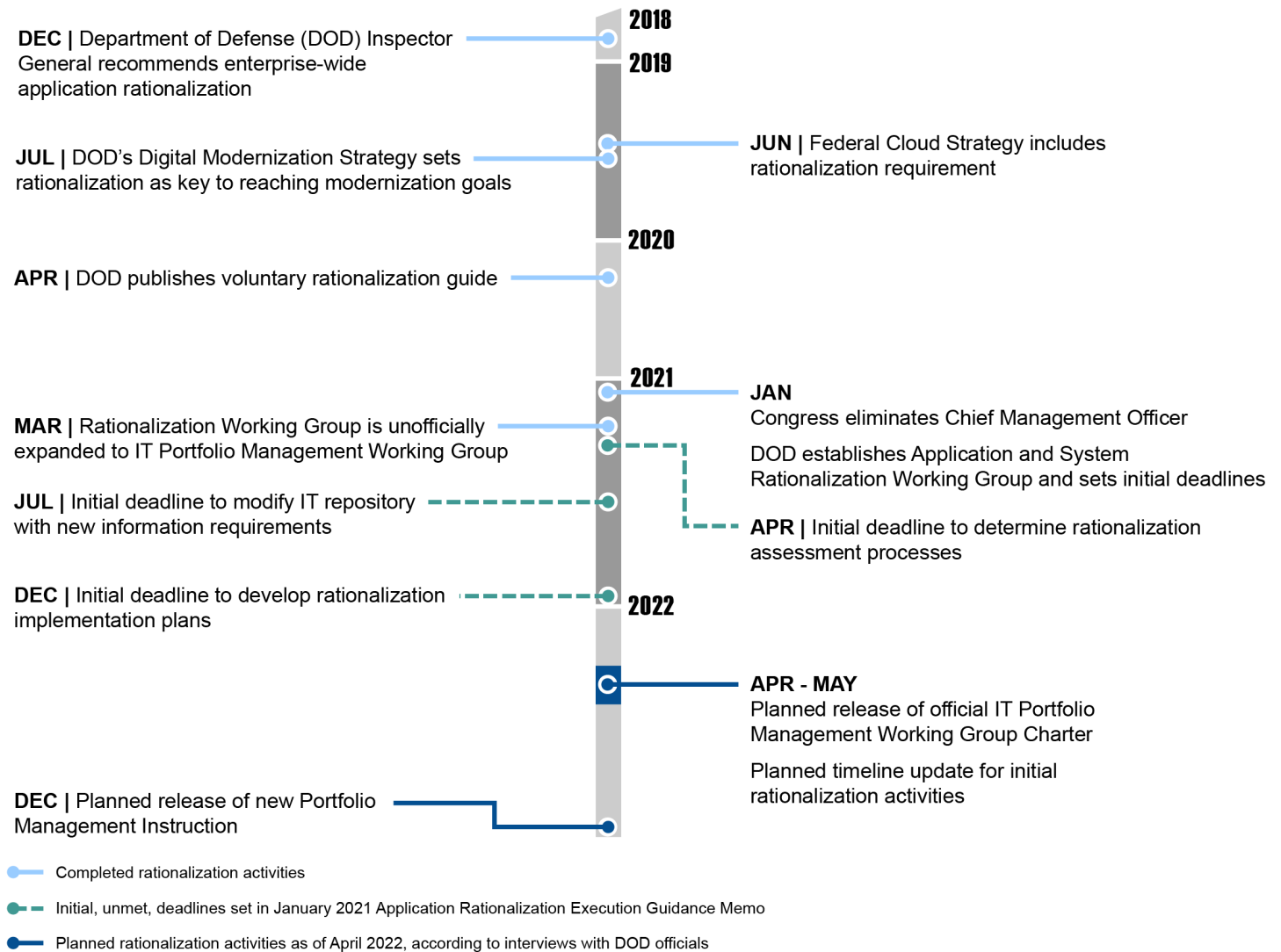
Officials in the Office of the CIO told us at the time that rationalization was primarily the components' responsibility and, to some extent, the portfolio leads' responsibility, and that the DOD CIO would focus on understanding component's needs. In January 2021, the department CIO later released a rationalization execution memo that charged the Rationalization Working Group with establishing metrics to ensure enterprise-wide rationalization objectives were being met. The memo noted that the working group would oversee DOD-wide execution of rationalization but that mission leads would continue to be responsible for the management and rationalization of their portfolios.

However, after the working group was dissolved and the department changed focus to IT portfolio management, officials in the Office of the CIO told us that they were working to develop a new IT portfolio management policy that would be issued in December 2022. According to officials, the new policy and process would allow the department to assess IT investments for duplication and optimization opportunities, implement and enforce optimization recommendations, and conduct department-wide portfolio analysis. As of April 2022, the officials reported that the Office of the CIO and the working group had not yet defined timelines or milestones to decide how they would conduct these analyses and assessments.

Figure 3 shows key rationalization governance activities the department has taken, unmet deadlines for activities the department planned to take, activities the department currently plans to implement, and external events that contributed to the department's actions.

⁵⁵10 U.S.C. § 2223; DOD Directive 5144.02, *DoD Chief Information Officer (DoD CIO)*, (Nov. 21, 2014), (updated Sept. 19, 2017).

Figure 3: Department of Defense (DOD) Timeline of Key Enterprise-Wide Rationalization Governance Activities (December 2018 through December 2022)



Source: GAO analysis of DOD documentation. | GAO-22-104070

Officials in the DOD CIO's office with responsibility for application rationalization acknowledged these factors had affected their rationalization efforts. The officials noted that the change to their rationalization approach was caused by a realignment of responsibilities following the Chief Management Officer's disestablishment. This required the CIO's office to begin reviewing and updating their IT portfolio

management policies and processes. In addition, these officials said that the department can take a long time to implement changes to IT policies and processes because of the size of the department and the large number of stakeholders that need to approve any changes. Finally, DOD officials stated that they have chosen not to require components to follow the department's rationalization guide because they do not want to interfere with individual components and sub-portfolios that already have robust rationalization processes in place.

While making changes to department policies and processes in order to respond to changes in federal law is necessary, the department has spent the past nine years identifying application rationalization as a key element in multiple reform strategies,⁵⁶ but does not yet have an enterprise-wide application rationalization process in place. Further, even if the department does update its new IT portfolio management policy by December 2022, it remains unclear what the rationalization implementation time frames will be after the policy is finalized, who will be responsible for implementation, who will oversee implementation, and how the department will determine success.

Until the department establishes measurable objectives, milestones, and time frames for the development and implementation of its application rationalization process, and ensures components are held accountable for these activities, it is unlikely that DOD will make consistent, measurable progress toward meeting its rationalization goals.

DOD Components Underreported TBM Cloud Spending and Did Not Always Follow Leading Practices

In its fiscal year 2019 guidance, OMB began requiring agencies to use TBM as part of the annual budget submission process for IT investments.⁵⁷ Agencies are required to use a standard set of cost

⁵⁶DOD has prioritized application rationalization as a key IT modernization goal since the Joint Information Environment Execution Strategy in 2013 and re-emphasized its importance in its 2019 Digital Modernization Strategy.

⁵⁷Office of Management and Budget, *FY19 IT Budget-Capital Planning Guidance*.

categories—called cost pools⁵⁸ and IT towers⁵⁹—to allocate spending on each investment, including cloud-related spending. According to the TBM Council's *TBM Taxonomy, Version 3.0* (referenced in OMB's guidance),⁶⁰ IT services purchased from cloud service providers (including infrastructure as a service, platform as a service, and software as a service) should be categorized under the IT cost pool outside services.

Although DOD reported its budget data to OMB using TBM cost categories, the cloud spending data are likely underreported. The six department components' investments we reviewed that used a commercial cloud provider did not always have spending allocated to the outside services cost pool. In addition, DOD investments using cloud services sometimes had a small total reported spending amount of \$6,000 or less for a given fiscal year.

Specifically, the six department components in our review did not always allocate spending to the outside services cost pool for their cloud investments that used a commercial cloud provider (as required by OMB guidance).⁶¹ In fiscal year 2021, DOD components reported that 97 out of their 111 cloud investments used commercial cloud services. However, 34 out of these 97 investments (35 percent) did not have any reported spending to the outside services cost pool. In addition, for fiscal year 2022, while 121 out of 136 investments used commercial cloud services, 50 of these investments (41 percent) had no reported spending for outside services. Table 4 lists the number of DOD's unclassified IT cloud investments using a commercial cloud provider that reported no spending

⁵⁸The *TBM Taxonomy, Version 3.0* states that cost pools are low-level categories that make cost allocations easier by revealing the composition of costs. For example, application total cost of ownership can be broken down into hardware, software, internal and external labor, outside services, facilities, and telecom costs. Copyright © 2020 Technology Business Management Council.

⁵⁹According to the TBM Council's *TBM Taxonomy, Version 3.0*, IT towers are the resources or building blocks of specific IT applications. Examples of IT towers include compute (e.g., servers, mainframe), network, application (e.g., application development, application support and operations) and IT management. Copyright © 2020 Technology Business Management Council.

⁶⁰Technology Business Management Council, *TBM Taxonomy, Version 3.0*. Copyright © 2020 Technology Business Management Council.

⁶¹The six components within the department were selected based on the largest budget requests for cloud services for fiscal year 2021.

for the outside services cost pool for the six selected components for fiscal years 2021 through 2022.

Table 4: Number of Unclassified DOD IT Cloud Investments Using Commercial Providers but No Reported Spending for Outside Services, as Reported in DOD SNaP-IT for Six Components for Fiscal Year 2021 through Fiscal Year 2022

DOD component	Investments using cloud services ^a		Investments using commercial cloud provider		Investments that reported no spending for outside services cost pool ^b	
	Fiscal year 2021	Fiscal year 2022	Fiscal year 2021	Fiscal year 2022	Fiscal year 2021	Fiscal year 2022
Air Force	37	55	37	52	20	29
Army	24	15	23	14	10	12
Defense Human Resources Activity	4	3	4	3	0	1
Defense Information Systems Agency	6	4	4	2	2	2
Navy	37	54	28	47	2	4
U.S. Transportation Command	3	5	1	3	0	2
Total	111	136	97	121	34	50

Source: GAO analysis of Select and Native Programming Data Input Systems for Information Technology System (SNaP-IT) data as of February 18, 2020 (fiscal year 2021) and June 8, 2021 (fiscal year 2022). | GAO-22-104070.

^aAn investment was considered to use cloud services if there was spending on cloud services, either direct spending for a cloud contract or spending on hosting the investment in a cloud environment.

^bThe TBM Council's *TBM Taxonomy, Version 3.0* (noted in OMB's capital planning guidance) states that IT services purchased from cloud service providers should be categorized under the outside services cost pool. (TBM = Technology Business Management).

In addition, two or more department components in our review reported a small spending total of \$6,000 or less for an investment for fiscal years 2021 and 2022. Specifically, 14 out of 111 investments (13 percent) had total reported spending of \$6,000 or less for the investment in fiscal year 2021. In fiscal year 2022, 13 out of 136 investments (10 percent) had total reported spending of \$6,000 or less for the investment. Table 5 lists the number of DOD's unclassified IT cloud investments that had total reported spending of \$6,000 or less for fiscal years 2021 and 2022 for the six selected components.

Table 5: Number of Unclassified DOD IT Cloud Investments With Reported Spending of \$6,000 or Less, as Reported in DOD SNaP-IT for Six Components for Fiscal Year 2021 through Fiscal Year 2022

DOD component	Investments using cloud services ^a		Investments reporting total spending of \$6,000 or less	
	Fiscal year 2021	Fiscal year 2022	Fiscal year 2021	Fiscal year 2022
Air Force	37	55	4	4
Army	24	15	9	9
Defense Human Resources Activity	4	3	0	0
Defense Information Systems Agency	6	4	1	0
Navy	37	54	0	0
U.S. Transportation Command	3	5	0	0
Total	111	136	14	13

Source: GAO analysis of Department of Defense (DOD) Select and Native Programming Data Input Systems for Information Technology System (SNaP-IT) data as of February 18, 2020 (fiscal year 2021) and June 8, 2021 (fiscal year 2022). | GAO-22-104070.

^aAn investment was considered to use cloud services if there was spending on cloud services, either direct spending for a cloud contract or spending on hosting the investment in a cloud environment.

Based on our review of the six DOD components' TBM data, the two issues identified with the completeness of the data increase the likelihood that all costs associated with the department's spending on cloud services may have been incorrectly allocated to the wrong TBM cost category or incompletely captured. As a result, the six DOD components' use of TBM to track and report spending on investments using cloud services is likely allocated by cost category incorrectly or underreported.

DOD officials in the Office of the CIO in charge of TBM provided a number of reasons for the issues identified with the data. Specifically, DOD officials reported in April 2020 that TBM was used solely for the annual budget submission in order to comply with OMB's requirement. The officials noted that the department had provided annual training to components on the framework and oversaw a data quality working group that met weekly regarding DOD's IT investments. However, the officials stated that it was up to the components to review and ensure the quality of reported data. They stated that the DOD CIO's guidance required all component CIOs to submit an annual statement that the submission was complete and accurately aligned with their primary budget, program, and acquisition materials. Further, the DOD officials reported that the

department's CIO relied on the components' quality control processes to ensure the quality of the data.

Regarding the small reported spending amounts, a DOD official in the Office of the CIO with responsibility for SNaP-IT data noted that components might put in \$1,000 as a placeholder so the investment would not be eliminated. In addition, DOD officials reiterated that it was up to the components to ensure the quality of reported data. They also stated that the DOD CIO's guidance noted that investments must have a minimum of at least \$1,000 or else the investment would be noted as terminated.

Our review of the DOD CIO's budget guidance for fiscal years 2021 and 2022⁶² did not find any information regarding what quality control processes the components should have in place to ensure the quality of the reported TBM data—except the statement requiring component CIOs to confirm their submission was complete and accurate. In addition, the documentation did not include any specific guidance on the allocation of spending to TBM cost pools and IT towers, and merely referred components to the TBM Council's *TBM Taxonomy, Version 3.0* documentation. Further, while the DOD CIO's budget guidance regarding reporting a minimum of at least \$1,000 may have helped components to ensure their investments were not terminated, it has not aided the department's efforts to ensure that spending amounts for these investments were reported completely and accurately by the components.

Ensuring components understand how they are supposed to allocate spending to cost pools and IT towers, and the control processes they should have in place to confirm the quality of the data is critical to assuring the department's TBM investment data is reliable. Absent detailed guidance from the DOD CIO's office on how to allocate spending to specific cost pools and towers for cloud services and what control processes should be in place to ensure the TBM data is reliable, the department and the CIO are at risk of having incomplete data to make fully informed decisions on its IT investments. Further, until the department CIO's office updates its annual budget guidance to provide clarification on the use of minimum reported spending of at least \$1,000,

⁶²Department of Defense, *FY 2021 Information Technology/Cyberspace Activities Budget Guidance* (Washington, D.C.: Aug. 8, 2019); *FY 2022 Information Technology/Cyberspace Activities Budget Guidance* (Sept. 25, 2020).

Two DOD Components Did Not Follow Leading Practices for TBM Implementation

the department will likely not be able to ensure that planned investment spending is reported completely and accurately.

While OMB’s guidance is not specific regarding what activities agencies should undertake in order to implement TBM, the General Services Administration’s *Technology Business Management Playbook* recommends that agencies have a dedicated implementation team for the collection, analysis, reporting, and informed review of the data. The playbook also recommends that the implementation team provide resources and training to key players and stakeholders to help everyone understand common TBM terminology and definitions.⁶³ *Standards for Internal Control in the Federal Government* emphasizes that management should track the actual performance of key initiatives in order to ensure that these activities are meeting plans, goals, and objectives, and in doing so, management should use quality information.⁶⁴

While four of the six components implemented the activities noted in the General Services Administration’s TBM playbook, the other two components did not. In particular, the Army and Air Force did not provide additional guidance on how to allocate spending by TBM cost category and did not have a process for assessing and improving the quality of TBM data. In addition, the Air Force did not have a unit designated with responsibility for TBM implementation. The results of our analysis of DOD components’ processes for implementing TBM are shown in table 6.

Table 6: Analysis of Selected DOD Components’ Implementation Processes for the Technology Business Management (TBM) Framework

DOD component	Uses department guidance on TBM allocation by cost category	Has a designated unit responsible for TBM implementation	Provided guidance on TBM allocation by cost category	Has a process for assessing and improving the quality of TBM data
Air Force	●	○	○	○
Army	●	●	○	○
Defense Human Resources Activity	●	●	●	●
Defense Information Systems Agency	●	●	●	●

⁶³General Services Administration and the Department of Education, *Technology Business Management Playbook*. The playbook is designed to assist agencies in TBM implementation by offering guidance and lessons learned.

⁶⁴[GAO-14-704G](#).

DOD component	Uses department guidance on TBM allocation by cost category	Has a designated unit responsible for TBM implementation	Provided guidance on TBM allocation by cost category	Has a process for assessing and improving the quality of TBM data
Navy	●	●	●	●
U.S. Transportation Command	●	●	●	●

Legend: ● = used, ○ = not used

Source: GAO analysis of Department of Defense (DOD) component documentation. | GAO-22-104070.

Regarding its TBM implementation activities, Air Force officials reported that their efforts had been fragmented and, as a result, no single organizational unit was responsible for implementation within the component. In addition, due to the fragmentation, the officials noted that the organization had not reached a level of maturity where the data could be assessed for improvement. Army officials reported that the component was examining how to efficiently align its internal data reporting structures with the cost pools and IT towers. In addition, Army officials reported that they were also currently identifying opportunities to improve the quality of data.

Therefore, until the Air Force CIO designates a unit within the component with responsibility for TBM implementation, the Air Force will have less assurance that the component has collected, analyzed, and reported its TBM data correctly. In addition, until the Air Force CIO and Army CIO provide TBM allocation guidance and develop a TBM data quality assessment process, the department components will likely not have sufficiently reliable data to make IT investment decisions.

Conclusions

DOD's budget for cloud services and migration for fiscal year 2022 emphasizes the importance of cloud services in achieving the department's mission. While DOD has taken steps to address OMB's key cloud requirements related to securing its cloud environments and improving the procurement of these services, there has not been a corresponding effort to ensure that the department has the current and future workforce that it needs to support its planned enterprise-wide cloud environment. These gaps in workforce planning include identifying the future skills needed for cloud-based services and conducting regular evaluations of customer experience and user needs. An important aspect to the success of DOD's implementation efforts will be the ability of the department to address these workforce planning areas to ensure the department's cloud solutions meet its needs.

Although DOD has partially implemented the first step noted in leading practices on application rationalization implementation, the department's lack of established time frames for completing the remaining activities has impacted its efforts to make progress on subsequent steps. In addition, DOD's lack of a long-term plan for rationalization implementation—including clear objectives, milestones, and timelines—hinders the department in ensuring consistent progress is made toward its stated goals. Consistent measurable progress on enterprise application rationalization would also help the department's CIO to fulfill the statutory responsibility to provide for the elimination of IT duplication.

OMB intended agencies to use TBM data, including data on cloud-related costs, to make informed decisions regarding the performance of their investments. Although DOD has reported its budget data to OMB using TBM cost categories, the issues we identified with the completeness of the department's cloud spending data increase the likelihood that cloud spending is underreported. In addition, the Army and Air Force did not following leading practices for TBM implementation. Until the department updates its TBM guidance to include more specific information on how spending on services provided by commercial cloud providers should be allocated and the control processes that components should have in place to ensure the TBM data is reliable, DOD will likely not be able to take advantage of TBM's stated benefits.

Recommendations for Executive Action

We are making nine recommendations: seven to DOD, one to the Air Force, and one to the Army. Specifically:

The Secretary of Defense should direct the CIO and OUSD (A&S) to work with department components, to conduct skills gap analyses that maps current IT workforce resources to future skill and position requirements needed for an enterprise-wide cloud environment. (Recommendation 1)

The Secretary of Defense should direct the CIO to ensure that the department's components and OUSD (A&S) conduct regular evaluations of customer experience and user needs to ensure that the solutions for the enterprise-wide cloud environment foster efficiency, accessibility, and privacy. (Recommendation 2)

The Secretary of Defense should direct the CIO and department components to develop and execute a communication plan that will help employees understand the planned changes that will occur for the implementation of the department's enterprise-wide cloud environment. (Recommendation 3)

The Secretary of Defense should direct the CIO to establish an enterprise-wide rationalization governance structure, identify and document all rationalization requirements in department policy, and determine the relevant information required on each application for rationalization and the means to collect it. (Recommendation 4)

The Secretary of Defense should direct the CIO to establish measurable objectives, milestones, and time frames for the development and implementation of the department's enterprise-wide application rationalization process. (Recommendation 5)

The Secretary of Defense should direct the CIO to ensure that all department components are held accountable for meeting the objectives, milestones, and time frames included in for the department's enterprise-wide application rationalization process. (Recommendation 6)

The Secretary of Defense should direct the CIO to update department-wide guidance to components regarding TBM implementation to include more specific information: how components should allocate spending for cloud services to specific cost pools and towers; identify what control process should be in place to ensure the TBM data is reliable; and provide clarification on the use of minimum reported spending of at least \$1,000 for IT investments. (Recommendation 7)

The Secretary of the Air Force should direct the Air Force CIO to designate a unit within the component with responsibility for TBM implementation, provide additional guidance on TBM allocation of spending for cloud services to specific cost pools and towers, and to develop a process for assessing and improving the quality of TBM data. (Recommendation 8)

The Secretary of the Army should direct the Army CIO to provide additional guidance on TBM allocation of spending for cloud services to specific cost pools and towers, and to develop a process for assessing and improving the quality of TBM data. (Recommendation 9)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD and OMB for review and comment. We received written comments from DOD that are reprinted in appendix III and summarized below. OMB did not provide comments.

In its comments, DOD concurred with one of our nine recommendations, partially concurred with seven, and did not concur with one recommendation. Specifically, DOD concurred with our recommendation

for the CIO and OUSD (A&S) to work with department components to conduct a skills gap analysis that maps current IT workforce resources to future skill and position requirements needed for an enterprise-wide cloud environment. DOD stated that it intended to complete a zero-based review of cyber and IT personnel and submit the results to Congress in June 2022. The department also noted that the process was designed to be repeatable at the service level for continued implementation and assessment of additional workforce categories in the future.

In addition, DOD partially concurred with seven of our nine recommendations (recommendations 2, 3, 4, 5, 6, 8, and 9). These recommendations were to address gaps in cloud workforce planning, improve application rationalization planning, and ensure the Air Force and Army addressed TBM leading practices. While DOD did not state any specific disagreements with elements of these seven recommendations, department officials did identify ongoing or planned actions to address them.

- For recommendations 2 and 3, DOD stated that it would update or issue workforce planning guidance by September 2024. Specifically, for recommendation 2, DOD stated it would include responsibilities for ongoing evaluation of customer experience in future guidance. In addition, for recommendation 3, DOD stated that it would include requirements in future guidance for communication planning to increase awareness of capabilities available to department users for the enterprise-wide cloud environment.
- For recommendations 4, 5, and 6, DOD stated that it would update or issue application rationalization guidance by September 2024. For recommendation 4, DOD stated that it would make improvements to its current department portfolio management processes to include governance, requirements, and roles and responsibilities to enable enterprise-wide rationalization. In addition, for recommendation 5, DOD stated that it would include measurable objectives, milestones, and time frames for implementation of the department's enterprise-wide rationalization priorities in future guidance. Further, for recommendation 6, DOD stated that it would include defined responsibilities in future guidance to ensure that application rationalization objectives, milestones, and timeframes would be met.

The actions that DOD described for recommendations 2, 3, 4, 5, and 6, if implemented effectively and in accordance with OMB and other federal guidance in these areas, would address the intent of our recommendations.

Regarding recommendations 8 and 9, DOD also described actions it planned to take. However, as discussed below, it is not evident that these actions would fully address our recommendations.

- For recommendation 8, DOD stated that the Air Force's budget reporting aligned with department guidance from the CIO's office and that the Air Force had taken actions to upgrade its portfolio suite in accordance with the TBM framework. However, the department did not provide any supporting documentation regarding the Air Force's actions related to upgrading the portfolio suite; therefore, we were not able to confirm these activities prior to the issuance of this report.

As stated previously, having a dedicated implementation team for the collection, analysis, reporting, and informed review of TBM data, and providing TBM allocation guidance are important practices for TBM implementation. In addition, developing a TBM data quality assessment process is critical for ensuring the reliability of TBM data that will be used to make investment decisions. Consequently, we believe our recommendation to the Air Force to implement these practices is still warranted.

- For recommendation 9, DOD stated that it concurred that a definitive assessment process should be codified into Army policy (in accordance with the portion of our recommendation to develop a process for assessing and improving the quality of TBM data). In addition, DOD stated that the Army currently uses TBM towers and cost pools for all cloud contracts and requires all investments to align to these towers and cost pools. Further, DOD stated that the Army would initiate an Army-wide review of how IT requirements were documented as part of its planning, programming, budgeting, and execution process. DOD noted that the Army's review of this process would entail a review of its processes, systems, and the data required to standardize IT resourcing and related information to create an enterprise view of IT and its impact on Army operations.

However, DOD did not provide any time frames for when the Army's review would begin or be completed. In addition, it was not clear how Army's planned review would address the portion of our recommendation to provide additional guidance on TBM allocation of spending for cloud services to specific cost pools and towers. As stated previously, providing resources and training to key players and stakeholders to help everyone understand common TBM terminology and definitions is an important practice to help ensure the reliability of TBM data that will be used to make investment decisions.

Consequently, we believe our recommendation to the Army to implement this practice is still warranted.

Finally, DOD did not concur with our recommendation to update department-wide guidance to components regarding TBM implementation. While DOD did not state why it disagreed with our recommendation, the department noted that the CIO issues guidance based on and in compliance with OMB policy, including TBM implementation. The department stated that components are responsible for data quality and the DOD CIO relies on their quality control to ensure data quality. Further, DOD stated that component CIOs and chief financial officers are required to submit a memorandum to the DOD CIO stating that their electronic budget submission is complete and accurate.

However, based on the issues that we identified with the completeness of DOD's cloud spending data, the DOD CIO's reliance on components' quality control processes is not sufficient to ensure quality TBM data. These issues were identified in multiple components within the department—specifically, the components with the largest budgets for cloud services in DOD. Accordingly, ensuring that components understand how they are supposed to allocate TBM spending, and the control processes necessary for quality data, is critical to assuring that the department's TBM investment data is reliable. Consequently, we believe our recommendation to the department to update its guidance in these areas is still warranted.

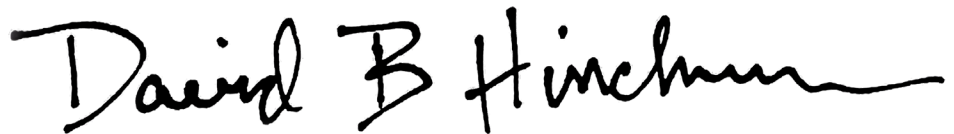
As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Director of the Office of Management and Budget; the Secretary of Defense; and other interested parties. This report will also be available at no charge on our website at <http://www.gao.gov>.

If you or your staffs have any questions on matters discussed in this report, please contact Carol Harris at (202) 512-4456 or HarrisCc@gao.gov and David Hinchman at (214) 777-5719 or HinchmanD@gao.gov. Contact points for our Offices of Congressional

Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.



Carol C. Harris
Director, Information Technology
Acquisition Management Issues



David B. Hinchman
Acting Director, Information Technology
and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our objectives for this engagement were to determine the extent to which: (1) the Department of Defense's (DOD) planned cloud strategy addresses the key requirements included in the Office of Management and Budget's (OMB) *Federal Cloud Computing Strategy*, (2) the department has plans for developing and implementing an enterprise-wide process to rationalize its application portfolio, and (3) the department is using Technology Business Management (TBM) to track and report spending data for cloud services.

For the first objective, we analyzed OMB's June 2019 *Federal Cloud Computing Strategy* to identify the requirements that OMB indicated should be undertaken as part of an agency's cloud strategy.¹ Based on our review of the strategy, we identified 14 key requirements across three categories (security, procurement, and workforce); we confirmed the list with staff in OMB's Office of Federal Chief Information Officer (CIO). We then analyzed DOD policies, directives, and other guidance related to cloud computing services (cloud services) to determine whether the department's planned cloud strategy aligned with the key requirements selected from OMB's *Federal Cloud Computing Strategy*.

We chose to focus on whether DOD had developed department-wide policies and other guidance that addressed OMB's requirements because OMB Circular A-130 requires agency CIOs to define policies and processes in sufficient detail for all information resources.² This included strategies related to digital modernization, software modernization, identity, credential, and access management and DevSecOps, as well as related directives and a cloud acquisition guidebook.³ In performing our analysis, we determined the extent to which each requirement was either

¹Office of Management and Budget, *Federal Cloud Computing Strategy* (June 24, 2019).

²Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (July 28, 2016).

³Department of Defense, *DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY19-FY23* (July 12, 2019); *Department of Defense Software Modernization Strategy* (Feb. 2, 2022); *Identity, Credential, and Access Management (ICAM) Strategy* (Mar. 30, 2020); *DoD Enterprise DevSecOps Strategy Guide Version 2.1* (Oct. 19, 2021); *Cybersecurity*, DOD Instruction 8500.01 (Oct. 7, 2019); *Cybersecurity Activities Support to DoD Information Network Operations*, DOD Instruction 8530.01 (July 25, 2017); *DoD Continuity Policy*, DOD Directive 3020.26 (Feb. 14, 2018); *DoD Chief Information Officer (DoD CIO) DOD Directive 5144.02* (Sept. 19, 2017); and Defense Acquisition University, *DoD Cloud Computing Acquisition Guidebook Version 1.2* (Nov. 5, 2019).

fully addressed, partially addressed, or not addressed.⁴ In addition, we corroborated our analysis by interviewing officials from DOD's Office of the CIO and the Office of the Under Secretary of Defense for Acquisition & Sustainment (OUSD [A&S]) regarding department guidance and other documentation related to cloud services in the areas of security, procurement, and workforce planning.

For the second objective, we analyzed the department's policies and other documentation related to developing and implementing an enterprise-wide application rationalization process to determine whether those policies and guidance were consistent with OMB guidance, which required agencies to rationalize their application portfolios. We chose to focus on enterprise-level rationalization efforts because the DOD's Office of the Inspector General and U.S. Army Audit Agency had recently completed or had ongoing work reviewing military services' rationalization efforts. To assess this, we reviewed leading practices included in the CIO Council's *The Application Rationalization Playbook*⁵ and reform management leading practices included in GAO's Key Questions to Assess Agency Reform Efforts.⁶

In analyzing whether the department's policies and documentation met CIO Council criteria, we assessed whether the department's application rationalization documentation addressed the four actions included in the first step in the CIO Council's playbook. We chose the first step in the CIO Council's six-step process because the department had begun planning its process for enterprise-wide application rationalization and had not yet begun implementation. In performing our analysis, we determined the extent to which each requirement was addressed, using the same rating criteria as in the first objective.

In analyzing whether the department's plans for developing its enterprise-wide application rationalization process met reform management leading practices, we reviewed the department's rationalization planning documentation to determine whether it included goals, objectives,

⁴Fully addressed: DOD provided evidence that addressed the requirement; Partially addressed: DOD provided evidence that it had addressed some, but not all of the requirement; Not addressed: DOD did not provide evidence that it had addressed any of the requirement.

⁵CIO Council, *The Application Rationalization Playbook: An Agency Guide to Portfolio Management* (June 2019).

⁶GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, [GAO-18-427](#) (Washington, D.C.: June 13, 2018).

performance measures, and implementation timelines. We also reviewed the documentation to identify whether there was language included in the requirements that would hold leaders accountable for successful reform implementation. In addition, we corroborated our analysis by interviewing officials in the DOD CIO's office regarding the extent to which the provided documentation reflected the department's current plans for enterprise-wide application rationalization.

We also determined that the control activities component of internal control was significant to this objective, along with the underlying principles that management should design control activities to achieve objectives and respond to risk, and implement control activities through policies. We analyzed the department's policies and documentation for an enterprise-wide process to determine whether the department had defined objectives in specific and measurable terms to allow for the assessment of performance toward achieving these objectives, as noted in the *Standards for Internal Control in the Federal Government*.⁷

To address the third objective, we selected a sample of DOD components based on the size of their IT budget request for cloud services for fiscal year 2021.⁸ Using this criterion, we selected six components with the largest budget requests in the department the Air Force, Army, Defense Human Resources Activity, Defense Information Systems Agency, Navy, and U.S. Transportation Command.

For the third objective, we obtained and analyzed TBM data from the department's Select and Native Programming Data Input Systems for Information Technology (SNaP-IT) system⁹ related to the six components' reported number of investments leveraging cloud services and the spending allocated to TBM cost categories for these services for fiscal years 2021 through 2022. We chose fiscal year 2021 because OMB's capital planning guidance noted that this was the first year that OMB would begin publicly reporting all of agencies' TBM data on the IT Dashboard.

⁷GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 9, 2014).

⁸Department of Defense, *DoD FY 2021 Cloud Profile and Budget Estimates* (Feb. 18, 2020).

⁹DOD uses SNaP-IT to report its IT budget data on the federal IT Dashboard.

We also determined that the control activities component and information and communications component of internal control were significant to this objective, along with the underlying principles that management should design the entity's information system and related control activities to achieve objectives and respond to risks; implement control activities through policies; and use quality information (information that is appropriate, current, complete, and accurate) to make informed decisions and achieve its objectives. We analyzed department-wide and component-level documentation (policies, guidance, and training) related to reporting TBM data in SNaP-IT to determine whether the department had ensured its information processing objectives (accuracy and completeness) were met and that the sources of data were evaluated for reliability to ensure the data was reasonably free from error, as noted in the *Standards for Internal Control in the Federal Government*.

To assess the reliability of the SNaP-IT data, we reviewed documentation of the data system and discussed the data system with DOD officials in the Office of the CIO. We requested and reviewed department responses to questions about the system and how the department ensures the quality and reliability of the data. In addition, we reviewed documentation related to the system (e.g., data dictionaries, instructions for inputting budget data in DOD and the six components' guidance) and reviewed the data for obvious issues, including missing or questionable values. We also interviewed officials in charge of SNaP-IT data within the DOD Office of the CIO regarding its guidance, the systems, and how the department ensures the quality and reliability of the data. Further, we interviewed staff from OMB's Office of the Federal CIO regarding their guidance on TBM.

To ensure the accuracy and completeness of the selected components' number of investments leveraging cloud services and the spending allocated using TBM, we presented the results of our initial analysis to the six components and asked each component to verify the information presented and provide any updates or additional documentation as appropriate. Each of the components provided updated information, which we incorporated into this analysis, as appropriate. We also presented the results of our final analysis to these officials, as well as officials in charge of SNaP-IT data within the DOD Office of the CIO. We asked them to verify the completeness and accuracy of these data and provide any updates as appropriate.

Based on the measures we took to ensure the reliability of the data reported by the six components from SNaP-IT, we determined that the data were sufficiently reliable for the purpose of determining whether the

department was using TBM to meet OMB's requirement. However, we identified issues with the completeness of the department's cloud spending data, which we discuss in the report.

We conducted this performance audit from January 2020 to June 2022 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: Prior GAO and OIG Reports From 2014 Through 2016 Reviewing DOD's Adoption of Cloud Services, Portfolio Management, and Rationalization Activities

The following five reports were issued by GAO and the Department of Defense's (DOD) Office of Inspector General (OIG) from 2014 through 2016 related to the department's efforts to implement cloud adoption, portfolio management, and rationalization.

Department of Defense Office of Inspector General, *DoD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process*, DODIG-2015-045.

In December 2014, DOD's OIG found that the department had not fully executed elements of its cloud strategy issued in July 2012.¹ Specifically, the department had not fully developed skills training for the acquisition and contract specialists who would procure cloud services or who would fully develop cloud service broker management capabilities. In addition, the office found that the DOD CIO had not developed an implementation plan for the strategy that included assignment of roles and responsibilities and associated tasks, resources, and milestones. The OIG recommended that the DOD CIO develop a plan to implement the department's cloud strategy that assigned roles and responsibilities and associated tasks, resources, and milestones for all unexecuted elements of the strategy. DOD partially agreed with the recommendation and officials from the OIG reported that the department took action to implement it.

Department of Defense Office of Inspector General, *DoD Needs an Effective Process to Identify Cloud Computing Service Contracts*, DODIG-2016-038.

In December 2015, DOD's OIG found that the department did not maintain a comprehensive list of cloud computing service contracts.² In particular, the DOD CIO had not established a standard, department-wide definition for cloud computing and had not developed an integrated repository that could provide detailed information to identify cloud computing service contracts. The OIG recommended that the DOD CIO issue guidance related to a cloud computing definition and establish an integrated repository that provided detailed information to identify department cloud computing contracts. While DOD neither agreed nor

¹Department of Defense Office of Inspector General, *DoD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process*, DODIG-2015-045 (Dec. 4, 2014).

²Department of Defense Office of Inspector General, *DoD Needs an Effective Process to Identify Cloud Computing Service Contracts*, DODIG-2016-038 (Dec. 28, 2015).

disagreed with the recommendations, officials from the OIG reported that the department took action to implement both of them.

GAO, *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance*, [GAO-16-325](#).

In April 2016, we identified 10 key practices that federal and private sector guidance noted should be included in service-level agreements in a contract when acquiring IT services through a cloud services provider.³ However, our review of five agencies' (including DOD) cloud service contracts found that not all 10 key practices were included in these contracts. We therefore made recommendations to DOD and the other four agencies to incorporate these key practices as their contract and service level agreements expire. The agencies generally agreed with our recommendations and, to date, DOD and three other agencies have taken action to implement the recommendations.

GAO, *Joint Information Environment: DOD Needs to Strengthen Governance and Management*, [GAO-16-593](#).

In July 2016, we identified issues in DOD's approach to implementing the Joint Information Environment.⁴ Specifically, we found that DOD had not consistently defined the Joint Information Environment's scope, inconsistently including application, and server rationalization as part of the environment; had not defined an end date or key milestones associated with the effort; and had not performed a gap analysis to identify the number of staff and the specific skills and abilities needed.

Accordingly, we made several recommendations to the department, including developing a scope statement and plan for managing the scope of the effort, developing a schedule management plan, and completing an assessment to determine the number of staff and the specific skills and abilities needed. DOD generally agreed with our recommendations and took action to address the two recommendations related to developing documentation for the effort's scope. However, as of April 2020, the department had not taken sufficient action to address the other recommendations. In April 2020, the department reported that it was in

³GAO, *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance*, [GAO-16-325](#) (Washington, D.C.: Apr. 7, 2016).

⁴GAO, *Joint Information Environment: DOD Needs to Strengthen Governance and Management*, [GAO-16-593](#) (Washington, D.C.: July 14, 2016, revised Oct. 25, 2016).

the process of retiring the Joint Information Environment, and therefore, did not plan to implement the recommendations. Accordingly, we closed them as not implemented.

GAO, *Information Technology: Agencies Need to Improve Their Application Inventories to Achieve Additional Savings*, [GAO-16-511](#).

In September 2016, we reviewed 24 agencies (including DOD), and found that while DOD was implementing four key practices for establishing an application inventory, its rationalization process did not allow for collecting or reviewing the information needed to effectively rationalize all their applications.⁵ Specifically, we found that DOD used its investment management process to review systems in the business mission area, but was not reviewing the approximately 1,200 enterprise IT and business systems under the enterprise information environment mission area. We recommended that the department expand its rationalization process to include enterprise information environment mission area systems; while the department disagreed with our recommendation, it took action to address it.

⁵GAO, *Information Technology: Agencies Need to Improve Their Application Inventories to Achieve Additional Savings*, [GAO-16-511](#) (Washington, D.C.: Sept. 29, 2016).

Appendix III: Comments from the Department of Defense



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

JUN 14 2022

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-22-104070, 'CLOUD COMPUTING: DOD Needs to Improve Workforce Planning and Software Application Modernization,' dated May 16, 2022 (GAO Code 104070).

The Department appreciates GAO's extensive review and acknowledgement of the DoD Chief Information Officer's efforts to address key cloud computing requirements in the areas of security, procurement, and workforce. As noted within the report, the Department has taken action to address cloud computing requirements and develop an enterprise-wide application rationalization process.

The Department appreciates the opportunity to review this report. Enclosed is the DoD's response to the recommendations made in the draft report. My point of contact for this matter is Mr. Robert Vietmeyer at robert.w.vietmeyer.civ@mail.mil or phone (571) 372-4461. We look forward to working with you in the future.

Sincerely,

A handwritten signature in blue ink, appearing to read "John B. Sherman".

John B. Sherman

Enclosure:
As stated

GAO DRAFT REPORT DATED MAY 16, 2022

GAO-22-104070 (GAO CODE 104070)

**“CLOUD COMPUTING: DOD Needs to Improve Workforce Planning and Software
Application Modernization”**

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

Recommendation 1: The Secretary of Defense should direct the CIO and OUSD (A&S) to work with department components, to conduct skills gap analyses that maps current IT workforce resources to future skill and position requirements needed for an enterprise-wide cloud environment

DoD Response: Concur. In response to FY2020 National Defense Authorization Act, Section 1652, “Zero-based review (ZBR) of Department of Defense cyber and information technology personnel,” the Department will complete a zero-based review of cybersecurity and information technology (IT) personnel and submit the results to congress in June of 2022. The ZBR process was intentionally designed to be repeatable at the Service level for continued implementation and assessment of additional workforce categories across the Department in the future.

Recommendation 2: The Secretary of Defense should direct the CIO to ensure that the department’s components and OUSD (A&S) conduct regular evaluation of customer experience and user needs to ensure that the solutions for enterprise-wide cloud environment foster efficiency, accessibility, and privacy

DoD Response: Partially Concur. The DoD CIO Software Modernization Strategy and Software Acquisition Pathway include a focus on Customer Experience when migrating IT services to the cloud. A significant part of this migration strategy includes ensuring operational requirements are met, including maximizing the user experience. Responsibilities for the on-going evaluation of customer experience in line with Circular A-11 section 280.10 will be included in the updated Department guidance. The estimated guidance publication is 4th Quarter 2024.

Recommendation 3: The Secretary of Defense should direct the CIO and its department components to develop and execute communication plan that will help employees understand the planned changes that will occur for the implementation of the department’s enterprise-wide cloud environment

DoD Response: Partially Concur. The DoD CIO will update existing guidance to address the requirements for communication planning to increase awareness of current and future capabilities available to authorized DoD users in the department’s enterprise-wide cloud environment. The estimated completion date is 4th Quarter 2024.

Appendix III: Comments from the Department of Defense

Recommendation 4: The Secretary of Defense should direct the CIO to establish an enterprise-wide rationalization governance structure, identify and document all rationalization requirements in DoD policy, and determine relevant information required for each application and means to collect it

DoD Response: Partially Concur. The DoD CIO published the Application Rationalization Guidebook on June 11, 2020, to outline an application rationalization process for DoD-wide use. Additionally, the DoD CIO is working to implement improvements to the current DoD IT portfolio management processes that will include governance, requirements, roles, and responsibilities, to enable enterprise-wide rationalization. The estimated completion date is 4th Quarter 2024.

Recommendation 5: The Secretary of Defense should direct the CIO to establish measurable objectives, milestones, and timeframes for development and implementation of the department's enterprise-wide application rationalization process.

DoD Response: Partially Concur. DoD policy governing information technology (IT) development, acquisition, and budgeting address the requirements to ensure an efficient and rationalized IT environment. DoD CIO will provide additional guidance to include measurable objectives, milestones, and timeframes for implementation of the Department's enterprise-wide application rationalizations priorities. The estimated guidance publication is 4th Quarter 2024.

Recommendation 6: The Secretary of Defense should direct the CIO to ensure that all department components are held accountable for meeting objectives, milestones, and timeframes included in the department's enterprise-wide application rationalization process.

DoD Response: Partially Concur. DoD Planning, Programming, Budgeting & Execution Process (PPBE) address the requirements for effective and efficient information technology investments while ensuring that desired outcomes are being achieved. DoD CIO will define responsibilities to ensure that application rationalization objectives, milestones, and timeframes are met (see response to Recommendation 5).

Recommendation 7: The Secretary of Defense should direct the CIO to update its department-wide guidance to components regarding TBM implementation to include more specific information on how components should: allocate spending for cloud services to specific cloud pools and towers; identify what control process should be in place to ensure TBM data is reliable; and provide clarification on the use of minimum reported spending of at least \$1,000.

DoD Response: Non-Concur. DoD CIO issues guidance based on and in compliance with OMB policy (A-11 and Capital Planning Guidance), including TBM implementation. Components are responsible for data quality and the DoD CIO relies on their quality control to ensure data quality. Following collection of the President's Budget data collection cycle, component chief information officers and chief financial officers are required to submit a memorandum to the DoD CIO, stating that their electronic budget submission is complete and accurate.

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

Recommendation 8: The Secretary of the Air Force should direct the Air Force CIO to designate a unit within the component with responsibility for TBM implementation, provide additional guidance on TBM allocation of spending for cloud services to specific cost pools and towers, and to develop a process for assessing and improving the quality of TBM data.

DoD Response: Partially concur. Currently the DAF performs IT Budget reporting using the Information Technology Investment Portfolio Suite (ITIPS) for its annual budget submission. Although we have not fully implemented the TBM framework yet, DAF has taken actions to upgrade ITIPS to provide IT investment data categorized in accordance with the TBM framework. For example, the Capability and Category of Expense data elements in ITIPS are aligned with the TBM Towers and Sub-Towers using the definitions provided by DoD CIO. The DAF IT Budget reporting is accomplished in compliance with the direction and guidance of DoD CIO, which complies with TBM framework.

Recommendation 9: The Secretary of the Army should direct the Army CIO to provide additional guidance on TBM allocation of spending for cloud services to specific cost pools and towers, and to develop a process for assessing and improving the quality of TBM data.

DoD Response: Partially concur. Army currently utilizes TBM towers and cost pools for all cloud contracts. In FY21, Army modified the Army's annex to the Federal Acquisition Regulations (AFARS) that established standardized Cost Towers and Cost Pools, contract CLIN structures and Product Service Codes for all cloud contracts. Additionally, Army requires all IT investments to be registered in the Army Portfolio Management System (APMS) which aligns those investments to TBM cost pools and towers.

Army has also initiated an Army-wide review of how IT requirements are documented across the Planning, Programming, Budgeting, and Execution (PPBE) process which will look at the processes, systems, and data required to standardize IT resourcing and related information to create an enterprise view of IT and its impact on Army operations.

Continual assessment and process improvement is a necessary function within all Army organizations. The Department concurs that a definitive assessment process should be codified into Army policy.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Carol C. Harris, (202) 512-4456, or harriscc@gao.gov
David B. Hinchman, (214) 777-5719, or hinchmand@gao.gov

Staff Acknowledgments

In addition to the individual named above, the following staff made key contributions to this report: Eric Winter (Assistant Director), Valerie Hopkins (Analyst in Charge), Logan Arkema, Melina Asencio, Lauri Barnes, Chris Businsky, Sandra Kerr, Priscilla Smith, and Teresa Smith.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (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

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



Please Print on Recycled Paper.