April 2018

DEFENSE BUSINESS SYSTEMS

DOD Needs to Continue Improving Guidance and Plans for Effectively Managing Investments

Accessible Version

April 2018

DEFENSE BUSINESS SYSTEMS

DOD Needs to Continue Improving Guidance and Plans for Effectively Managing Investments

Why GAO Did This Study

DOD spends billions of dollars each year on systems that support its key business areas, such as personnel and logistics. For fiscal year 2018, DOD reported that these business system investments are expected to cost about $8.7 billion. The *NDAA for Fiscal Year 2016* requires DOD to perform activities aimed at ensuring that business system investments are managed efficiently and effectively, to include taking steps to limit their complexity and cost.

The NDAA also includes a provision for GAO to report every 2 years on the extent to which DOD is complying with the act's provisions on business systems. For this report, GAO assessed, among other things, the department's guidance for managing defense business system investments and its business and IT enterprise architectures (i.e., descriptions of DOD's current and future business and IT environments and plans for transitioning to future environments). To do so, GAO compared the department's system certification guidance and architectures to the act's requirements. GAO also interviewed cognizant DOD officials.

What GAO Recommends

GAO is making six recommendations, including that DOD and the military departments establish time frames for, and issue, required guidance; and that DOD develop a complete IT architecture and integrate its business and IT architectures. DOD concurred with three and partially concurred with three recommendations. GAO continues to believe all of the recommendations are warranted as discussed in this report.

View GAO-18-130. For more information, contact Carol Harris at (202) 512-4456 or harriscc@gao.gov.

What GAO Found

The Department of Defense (DOD) has made progress in complying with most legislative provisions for managing its defense business systems, but additional actions are needed. For example, the *National Defense Authorization Act (NDAA) for Fiscal Year 2016* required DOD and the military departments to issue guidance to address five requirements for reviewing and certifying the department's business systems. While DOD has issued guidance addressing all of these requirements, as of February 2018, the military departments had shown mixed progress.

DOD's and Military Departments' Progress in Issuing Guidance that Addressed Fiscal Year 2016 NDAA Business System Management Requirements

Certification Requirement	DOD	Air Force	Navy	Army
Sufficient business process reengineering	Fully addressed	Fully addressed	Fully addressed	Not addressed
Business enterprise architecture compliance	Fully addressed	Fully addressed	Fully addressed	Not addressed
Valid requirements and a viable plan to implement them	Fully addressed	Fully addressed	Partially addressed	Not addressed
Acquisition strategy to eliminate or reduce the need to tailor commercial off-the-shelf systems	Fully addressed	Not addressed	Not addressed	Not addressed
Compliance with the department's auditability requirements	Fully addressed	Not addressed	Not addressed	Not addressed

Source: GAO analysis of Department of Defense documentation. | GAO-18-130

The military departments' officials described plans to address the gaps in their guidance; however, none had defined when planned actions are to be completed. Without guidance that addresses all five requirements, the military departments risk developing systems that, among other things, are overly complex and costly to maintain.

DOD has efforts underway to improve its business enterprise architecture, but its information technology (IT) architecture is not complete. Specifically, DOD's business architecture includes content called for by the act. However, efforts to improve this architecture to enable the department to better achieve outcomes described by the act, such as routinely producing reliable business and financial information for management, continue to be in progress. In addition, DOD is updating its IT enterprise architecture, which describes, among other things, the department's computing infrastructure. However, the architecture lacks a road map for improving the department's IT and computing infrastructure for each of the major business processes. Moreover, the business and IT enterprise architectures have yet to be integrated, and DOD has not established a time frame for when it intends to do so. As a result, DOD lacks assurance that its IT infrastructure will support the department's business priorities and related business strategies.

_____ **United States Government Accountability Office**

Contents

Figures

Abbreviations

CIO	Chief Information Officer
CMO	Chief Management Officer
DCMO	Deputy Chief Management Officer
DOD	Department of Defense
IT	information technology
NDAA	National Defense Authorization Act
OMB	Office of Management and Budget

April 16, 2018

Congressional Committees

The Department of Defense (DOD) spends billions of dollars each year to acquire modernized systems that are fundamental to achieving its business transformation goals, including systems that address key areas such as personnel, financial management, health care, and logistics. However, while DOD's capacity for modernizing its business systems has improved over time, significant challenges remain. We have designated the department's business systems modernization program as high risk since 1995.[1]

In addition, we have reported that significant potential exists for identifying and avoiding costs associated with duplicative functionality across the department's portfolio of defense business systems.[2] Since 1995, we have made a series of recommendations aimed at strengthening the department's institutional approach to business systems modernization and reducing the risks associated with its key investments.[3] Congress included provisions consistent with our recommendations in the department's annual authorizing legislation for fiscal year 2005, and in

---

[1]GAO, *High Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: February 2017). GAO's high-risk program focuses attention on government operations with greater vulnerabilities to fraud, waste, abuse, and mismanagement or that are in need of transformation to address economy, efficiency, or effectiveness challenges. Agencies can show progress by addressing our five criteria for removal from the list: leadership commitment, capacity, action plan, monitoring, and demonstrated progress.

[2]GAO, *Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue*, GAO-11-318SP (Washington, D.C.: Mar. 1, 2011) and *Follow-up on 2011 Report: Status of Actions Taken to Reduce Duplication, Overlap, and Fragmentation, Save Tax Dollars, and Enhance Revenue*, GAO-12-453SP (Washington, D.C., Feb. 28, 2012). For GAO's latest assessment of DOD's efforts to address actions GAO identified for DOD to optimize business operations and systems, see http://www.gao.gov/duplication/action_tracker/DOD%27s_Business_Systems/action1

[3]See, for example, GAO, *Business Systems Modernization: Summary of GAO's Assessment of the Department of Defense's Initial Business Enterprise Architecture*, GAO-03-877R (Washington, D.C.: July 7, 2003); *Information Technology: Architecture Needed to Guide Modernization of DOD's Financial Operations*, GAO-01-525 (Washington, D.C.: May 17, 2001); and *High-Risk Series: An Overview*, GAO/HR-95-1 (Washington, D.C.: February 1995).

subsequent amendments.[4] Most recently, the *National Defense Authorization Act for Fiscal Year 2016* (NDAA), which was enacted in November 2015, included provisions that revised U.S. Code Title 10, Section 2222. These provisions required DOD to perform certain activities aimed at ensuring that its business system investments are managed efficiently and effectively.[5]

The NDAA included provisions for GAO to assess, biennially, the department's compliance with the provisions in the act. Accordingly, our objective for this review was to assess the extent to which actions taken by DOD comply with the act's provisions to:

1. establish guidance for effectively managing its defense business system investments;

2. develop and maintain a defense business enterprise architecture and information technology (IT) enterprise architecture, in accordance with relevant laws and Office of Management and Budget (OMB) policies and guidance;[6]

3. use the Defense Business Council to provide advice to the Secretary on developing the business enterprise architecture, reengineering the department's business processes,[7] developing and deploying business systems, and developing requirements for business systems; and

4. ensure that covered business systems are reviewed and certified in accordance with the act.

---

[4]Pub. L. No. 108-375, § 332, 118 Stat. 1811, 1851-1856 (2004), as amended by Pub. L. No. 113-291, § 901, 128 Stat. 3292 (2014), Pub. L. No. 113-66, § 901, 127 Stat. 672, 815 (2013), Pub. L. No. 112-239, § 906, 126 Stat. 1632, 1869 (2012), Pub. L. No. 112-81, § 901, 125 Stat. 1298, 1527 (2011), and Pub. L. No. 111-84, § 1072, 123 Stat. 2190, 2470 (2009).

[5]Pub. L. No. 114-92, § 883, 129 Stat. 726, 942 (2015).

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

[7]Business process reengineering is an approach organizations use to redesign the way work is done to better support the organization's mission and reduce costs.

To assess the extent to which actions taken by DOD comply with the act's provisions to establish guidance for effectively managing its defense business system investments, we obtained and reviewed the department's guidance for managing business system investments. We then compared the guidance with the act's requirements that the guidance include six specific elements related to managing business system investments.[8]

We also assessed DOD's guidance for managing business system investments relative to the act's certification requirements. Specifically, we compared the DOD Deputy Chief Management Officer's (DCMO)[9] April 2017 certification guidance with the act's certification requirements. In addition, we compared the guidance established by the Departments of the Air Force, the Army, and the Navy for certifying their business systems with the act's certification requirements.

To assess the extent to which actions taken by DOD comply with the act's provisions to develop and maintain a defense business enterprise architecture in accordance with relevant laws and OMB policies and guidance, we reviewed the department's business enterprise architecture, version 10, which was released in February 2013. We also reviewed data in the department's Integrated Business Framework—Data Alignment Portal system and DOD IT Portfolio Repository—which the department defined as part of its business enterprise architecture. We compared the architecture with the act's requirements and OMB policy and guidance[10] for the architecture's content. We also reviewed the department's January 2017 plan for improving the architecture and changes in the plan since it was issued.

To assess the extent to which actions taken by DOD comply with the act's provisions regarding DOD's IT enterprise architecture, we first determined the extent to which the IT architecture addressed relevant laws and OMB

---

[8]The guidance is to include policies and processes related to the coordination of, and decision making for, the planning, programming, and control of investments in covered defense business systems. For example, the guidance is to include a process for establishing requirements for covered defense business systems.

[9]On February 1, 2018, the Secretary of Defense eliminated the DCMO position and expanded the role of the Chief Management Officer, in accordance with the *National Defense Authorization Act for Fiscal Year 2018*.

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

policies and guidance. In particular, we reviewed the department's information enterprise architecture, which the department considers its IT enterprise architecture. The information enterprise architecture was released in August 2012. We compared its content with the act's requirements and OMB policy and guidance[11] for enterprise architectures to determine if it includes a plan for improving the IT and computing infrastructure for each of the department's major business processes, as required by the act.

We also assessed the extent to which the department has integrated its business and IT enterprise architectures. To do this, we obtained and reviewed documentation about the architectures, including the department's business enterprise architecture compliance guide and *DOD Directive 8000.01: Management of the Department of Defense Information Enterprise.*[12] Further, we reviewed business and IT architecture working group meeting documentation that discussed plans to update each architecture.

To assess the extent to which actions taken by DOD comply with the act's provisions to use the Defense Business Council to provide advice to the Secretary on developing the business enterprise architecture, reengineering the department's business processes, developing and deploying business systems, and developing requirements for business systems, we reviewed Defense Business Council meeting documentation, including meeting summaries and presentations, to identify instances in which the Council discussed the topics. We also discussed with officials in the Office of the DCMO how the Council provides advice on these topics to the Secretary of Defense.

To assess the extent to which actions taken by DOD comply with the act's provisions to ensure that covered business systems are reviewed and certified in accordance with the act, we reviewed a nongeneralizable sample of business systems from DOD's two categories of covered defense business systems that require certification.[13] To select the

---

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

[12]Department of Defense*, Directive 8000.01: Management of the Department of Defense Information Enterprise* (March 17, 2016, and incorporating change 1, July 27, 2017).

[13]DOD defines business systems categories in *DOD Instruction 5000.75*: *Business Systems Requirements and Acquisition* (Feb. 2, 2017).

sample, we considered Category I systems, which were systems that were expected to have a total amount of budget authority of more than $250 million over the period of the current future-years defense program,[14] and Category II systems, which were systems that were expected to have a total amount of budget authority of between $50 million and $250 million over the period of the future-years defense program.

We further categorized the Category II systems into four groups—those owned by the Air Force, the Army, Navy, and the remaining DOD components. We selected one system with the highest expected cost over the course of the department's future-years defense program from each group. This resulted in our selection of five systems: one Category I system, one Category II system from each military department, and one Category II system from the remaining DOD components.

We reviewed, respectively, DOD's Healthcare Management System Modernization Program; Air Force's Maintenance, Repair and Overhaul initiative; Army's Reserve Component Automation System; Navy's Electronic Procurement System; and the Defense Logistics Agency's Defense Agencies Initiative Increment 2. We compared documentation of the certifications for fiscal year 2017 of the five systems with the requirements in the act.

We supplemented our analyses with interviews of cognizant DOD officials. Specifically, we interviewed officials in the department's Office of the DCMO, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, and Office of the Chief Information Officer (CIO). We also interviewed officials in the Offices of the Chief Management Officers of the Departments of the Air Force, Army, and Navy, as well as other cognizant military department officials. Additional details on our objectives, scope, and methodology are contained in appendix I.

We conducted this performance audit from January 2017 to March 2018, in accordance with generally accepted government auditing standards.

---

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

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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Background

DOD is the largest U.S. federal department and one of the most complex organizations in the world. In support of its military operations, the department manages many interdependent business functions, including logistics management, procurement, health care management, and financial management. DOD relies extensively on IT to support its business functions.

According to its IT investment data, the department has 2,097 business system investments.[15] The department's fiscal year 2018 IT budget request states that DOD plans to spend about $8.7 billion in fiscal year 2018 on its defense business systems.[16]

The IT budget organizes investments by mission areas. The four mission areas are enterprise information environment, business, warfighting, and defense intelligence. Figure 1 shows the amount of DOD's requested fiscal year 2018 IT budget that the department plans to spend on each mission area.

---

[15]DOD's *IT-1 Report* is generated by the department's Select & Native Programming-IT system, which is a database application used to collect and assemble information required in support of the IT budget request submitted to Congress.

[16]Department of Defense, *IT Budget Exhibit Overview: Fiscal Year 2018 President's Budget Request* (May 2017).

Figure 1: Department of Defense (DOD) Fiscal Year 2018 Information Technology Budget by Mission Area (projected)

Dollars in billions
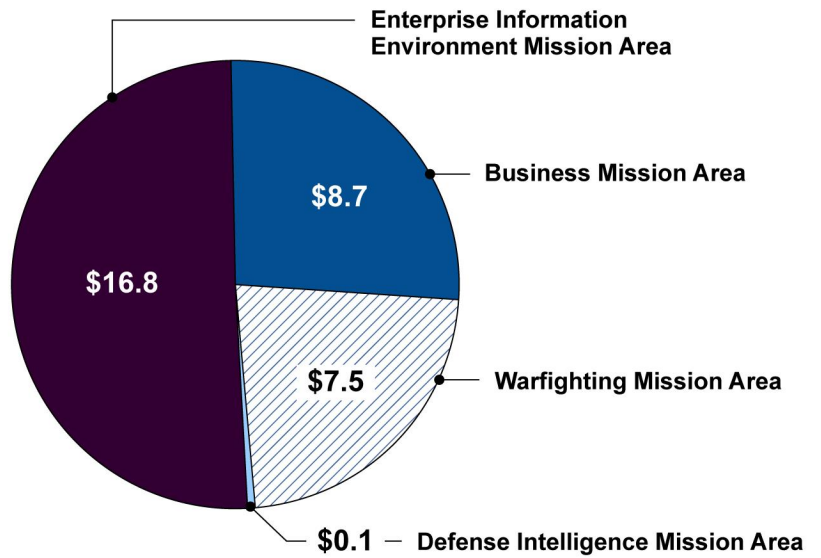
Source: GAO analysis of DOD information technology budget documentation. | GAO-18-130

The department further organizes its IT budget by segments.[17] For example, the business mission area includes segments such as financial management, health, and human resource management.[18] Figure 2 shows the department's projected fiscal year 2018 spending for each segment in the business mission area.

---

[17]According to the department, segments are part of a portfolio management concept required by the Office of Management and Budget. Segments are to serve as the basis for organizing IT investments for both budget management and performance management.

[18]The enterprise information environment mission area segments are IT infrastructure and IT management. The warfighting mission area segments include, among others, command and control, battlespace networks, force training, and force application.

Figure 2: Department of Defense (DOD) Information Technology Business Mission Area Fiscal Year 2018 Budget, by Segment (projected)

Dollars in millions
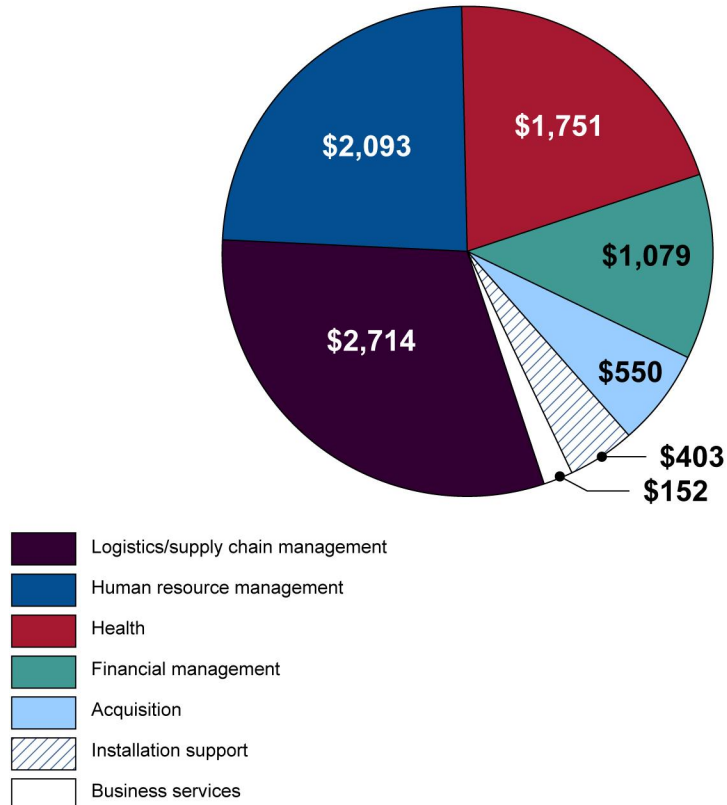
Source: DOD Information technology budget documentation. | GAO-18-130

GAO designated the department's business systems modernization efforts as high risk in1995 and has continued to do so in the years since. DOD currently bears responsibility, in whole or in part, for half of the programs (17 of 34 programs) across the federal government that we have designated as high risk.[19] Seven of these areas are specific to the department, and 10 other high-risk areas are shared with other federal agencies.

Collectively, these high-risk areas are linked to the department's ability to perform its overall mission and affect the readiness and capabilities of

---

[19]GAO-17-317.

U.S. military forces. DOD's business systems modernization is one of the department's specific high-risk areas and is essential for addressing many of the department's other high-risk areas. For example, modernized business systems are integral to the department's efforts to address its financial and supply chain high-risk areas.

Since 2005, we have issued 11 reports in response to mandates directing GAO to assess DOD's actions to respond to business system modernization provisions contained in Section 2222 of Title 10, United States Code. These reports contained 23 recommendations to help strengthen the department's management of its business systems. As of September 2017, the department had implemented 13 of the recommendations and 2 had been closed as not implemented. The other 8 recommendations remain open. The 11 reports are listed in appendix II.

The NDAA for Fiscal Year 2016 Included Provisions for Managing Defense Business Systems

The *NDAA for Fiscal Year 2016* included provisions requiring DOD to perform certain activities aimed at ensuring that its business system investments are managed efficiently and effectively. Specifically, the act established requirements for the department related to issuing policy and guidance for managing defense business systems; developing and maintaining a defense business enterprise architecture; establishing a Defense Business Council to provide advice to the Secretary on managing defense business systems; and obtaining approvals before systems proceed into development (or if no development is required, into production or fielding) and related annual reviews.

According to the *Joint Explanatory Statement accompanying the NDAA for Fiscal Year 2016,* the act revised Section 2222 of Title 10, United States Code, to streamline requirements and clarify the responsibilities of senior officials related to acquiring and managing business systems.[20] Key revisions pertain to:

- Covered defense business systems. The code previously defined a covered defense business system as a system having a total cost of

---

[20]*Joint Explanatory Statement to Accompany S. 1356, The National Defense Authorization Act for Fiscal Year 2016.* H. Committee Print 114-2 (Nov. 2015).

over $1 million over the period of the future-years defense program.[21] As revised, the code now defines a covered defense business system as a system that is expected to have a total amount of budget authority over the period of the current future-years defense program of over $50 million.

- Priority defense business systems. The act established a new category of system, called a priority defense business system. This is a system that is (1) expected to have a total amount of budget authority of over $250 million over the period of the current future-years defense program, or (2) designated by the DCMO[22] as a priority defense business system based on specific program analyses of factors including complexity, scope, and technical risk, and after notification to Congress of such designation.

- Thresholds and officials responsible for review and certification of defense business systems. The code previously stated that the DCMO had responsibility for reviewing and certifying all defense business system investments over $1 million over the future-years defense program. The revised code states that, unless otherwise assigned by the Secretary of Defense, military department Chief Management Officers (CMO) are to have approval authority for their covered defense business system investments below $250 million over the future-years defense program. The DCMO is to have approval authority for defense business systems owned by DOD components other than the military departments, systems that will support the business process of more than one military department or other component, and priority defense business systems.

- Certification requirements. The code previously required that a defense business system program be reviewed and certified, at least annually, on the basis of its compliance with the business enterprise architecture and appropriate business process reengineering. In addition to these requirements, the revised code requires that the

---

[21]In this report, both the "act" and the "code" can refer to the requirements of 10 U.S.C. § 2222. The *NDAA for Fiscal Year 2016,* the "act," amended the requirements of Sec. 2222. In this section of the report that discusses the prior and revised versions of Sec. 2222, we use the "code" to refer to the prior version of Sec. 2222, before it was amended by the "act" and "revised code" to refer to Sec. 2222 after it was amended by the "act."

[22]References to the Deputy Chief Management Officer in this report reflect requirements in the *NDAA for Fiscal Year 2016*. The *NDAA for Fiscal Year 2015* amended section 2222 to refer to the position as "Under Secretary of Defense for Business Management and Information." However, the *NDAA for Fiscal Year 2017* repealed the pending authority to establish that position.

business system program be reviewed and certified on the basis of having valid, achievable requirements and a viable plan for implementing the requirements; having an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems; and being in compliance with the department's auditability requirements.[23]

Key Roles and Responsibilities for Managing Defense Business Systems

DOD Instruction 5000.75: Business Systems Requirements and Acquisition assigns roles and responsibilities for managing defense business system investments.[24] Table 1 identifies the key entities and their responsibilities for managing defense business system investments.

Table 1: Key Department of Defense Entities and Their Responsibilities for Managing Defense Business System Investments

Entity	Responsibilities
DOD Deputy Chief Management Officer (DCMO)[a]	Establish policy and provide oversight for certification of business system investments.
	Maintain the business enterprise architecture.
	Establish policy and processes for business system capability management and its appropriate linkage to the business enterprise architecture.
	Establish policy and processes for validating business needs and identifying capability requirements for business systems.
	Validate requirements for priority defense business systems, which are systems that are expected to have a total amount of budget authority over the period of the current future-years defense program greater than $250 million or designated as priority by the DCMO based on complexity, scope, and technical risk.
	Certify priority defense business systems.
	Validate requirements for defense business systems of DOD components, other than the military departments, that are expected to have a total amount of budget authority between $50 million and $250 million over the period of the current future-years defense program.
	Co-Chair the Defense Business Council/Investment Review Board with the DOD Chief Information Officer (CIO).

[23]The department's auditability requirements are outlined in DOD's *Financial Improvement and Audit Readiness Guidance*, which is to provide a standard, multi-phased methodology for DOD components to follow to assess their financial management processes and controls and develop and implement financial improvement plans.

[24]Department of Defense, *DOD Instruction 5000.75: Business Systems Requirements and Acquisition* (Feb. 2, 2017). The instruction supersedes *DOD Instruction 5000.02: Operation of the Defense Acquisition System*, for all business system acquisition programs that are not designated as major defense acquisition programs.

Entity	Responsibilities
Military department Chief Management Officers (CMO)	Validate requirements and certify military department defense business systems that are expected to have a total amount of budget authority of between $50 million and $250 million during the period of the current future-years defense program.
Defense Business Council	Provide advice to the Secretary on developing the business enterprise architecture, reengineering the department's business processes, developing and deploying business systems, and developing requirements for business systems.
	Serve as Investment Review Board for Defense Business Systems.
	Oversee business enterprise architecture implementation for all business systems.
	Co-chaired by the DCMO and the DOD CIO. Members are the CMOs of the military departments; the Under Secretary of Defense (Acquisition, Technology, and Logistics); the Under Secretary of Defense (Comptroller); and the Under Secretary of Defense for Personnel and Readiness; or their designees.

Source: GAO analysis of Department of Defense documentation. | GAO-18-130

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

[a]On February 1, 2018, the Secretary of Defense eliminated the DCMO position and expanded the role of the Chief Management Officer, in accordance with the *National Defense Authorization Act for Fiscal Year 2018*.

DOD Has Made Progress in Complying with Legislative Provisions for Managing Defense Business Systems, but More Remains to Be Done

DOD has taken steps to address provisions of the *NDAA for Fiscal Year 2016* related to defense business system investments. Specifically, as called for in the act, the department has established guidance that addresses most legislative requirements for managing its defense business systems; however, the military departments are still developing guidance to fully address certification requirements for their systems.[25]

---

[25]Subsequent to sending a draft of this report to DOD for comment in December 2017, the Department of the Navy issued guidance that addresses all of the certification requirements. In addition, the Department of the Army issued its *Implementation Guidance for the DoDI 5000.75, Defense Business System Requirements and Acquisition Process* on March 23, 2018, and provided it to us on March 27, 2018. Due to the date on which we received the Army's guidance, we did not include an assessment of the guidance in this report.

Further, DOD has developed a business enterprise architecture and is in the process of updating the architecture to improve its content. The department also has a plan to improve the usefulness of the business enterprise architecture; however, the department has not delivered the plan's intended capabilities. In addition, the department is in the process of updating its IT enterprise architecture; however, it does not have a plan for improving the department's IT and computing infrastructure for each of the major business processes. Further, the department has not yet demonstrated that the business enterprise architecture and the IT enterprise architecture are integrated.

The department fully addressed the act's requirement related to defense business system oversight. Specifically, the department's governance board, called the Defense Business Council, addressed legislative provisions to provide advice to the Secretary of Defense.

Lastly, DOD and the military departments did not apply new legislative requirements when certifying business systems for fiscal year 2017. Instead, the DOD DCMO certified the systems in our sample in accordance with the previous fiscal year's (fiscal year 2016) certification requirements.[26]

DOD Issued Guidance Addressing Most Legislative Requirements for Managing Business Systems

The *NDAA for Fiscal Year 2016* required the Secretary of Defense to issue guidance by December 31, 2016 to provide for the coordination of, and decision making for, the planning, programming, and control of investments in covered defense business systems. The act required this guidance to address six elements:

- Policy to ensure DOD business processes are continuously reviewed and revised to implement the most streamlined and efficient business

---

[26]The act required the Secretary of Defense to issue guidance by December 31, 2016. The department stated in its technical comments on a draft of our report that the deadline was 3 months after fiscal year 2017 began. Accordingly, DOD stated that it did not apply the new legislative requirements when certifying business systems for fiscal year 2017 or any portion thereof. The department also stated that DOD certified many systems to the fiscal year 2016 NDAA requirements during the fiscal year 2018 certification cycle. However, we did not evaluate certifications that occurred during the fiscal year 2018 certification cycle as part of our assessment.

processes practicable and eliminate or reduce the need to tailor
commercial off-the-shelf systems to meet or incorporate requirements
or interfaces that are unique to the department.

- A process to establish requirements for covered defense business
systems.

- Mechanisms for planning and controlling investments in covered
defense business systems, including a process for the collection and
review of programming and budgeting information for covered
defense business systems.

- Policy requiring the periodic review of covered defense business
systems that have been fully deployed, by portfolio, to ensure that
investments in such portfolios are appropriate.

- Policy to ensure full consideration of sustainability and technological
refreshment requirements, and the appropriate use of open
architectures.

- Policy to ensure that best acquisition and systems engineering
practices are used in the procurement and deployment of commercial
systems, modified commercial systems, and defense-unique systems
to meet DOD missions.

Of these six elements called for by the act, the department has issued
guidance that fully addresses four elements and partially addresses two
elements. Table 2 summarizes our assessment of DOD's guidance
relative to the act's requirements.

Table 2: Assessment of the Department of Defense's Guidance for Covered Defense Business Systems

Legislative requirement	Rating
Policy to ensure that DOD business processes are continuously reviewed and revised to implement the most streamlined and efficient business processes practicable and eliminate or reduce the need to tailor commercial off-the-shelf systems to meet or incorporate requirements or interfaces that are unique to the department.	Fully addressed
Process to establish requirements for covered defense business systems.[a]	Fully addressed
Mechanisms for planning and controlling investments in covered defense business systems, including a process for the collection and review of programming and budgeting information for covered defense business systems.	Fully addressed
Policy requiring the periodic review of covered defense business systems that have been fully deployed, by portfolio, to ensure that investments in such portfolios are appropriate.	Fully addressed
Policy to ensure full consideration of sustainability and technological refreshment requirements, and the appropriate use of open architectures.	Partially addressed:
Policy to ensure that best acquisition and systems engineering practices are used in the procurement and deployment of commercial systems, modified commercial systems, and defense-unique systems, to meet DOD missions.	Partially addressed:

Source: GAO analysis of Department of Defense documentation. | GAO-18-130

^aA covered defense business system is a system that is expected to have a total amount of budget authority of over $50 million over the period of the current future-years defense program. The future-years defense program is to be submitted to Congress by the Secretary of Defense each year, at or about the time that the President's budget is submitted to Congress. It is to reflect the estimated expenditures and proposed appropriations included in the DOD budget, and cover the budget-submission fiscal year and at least the four succeeding fiscal years.

DOD fully addressed the element requiring policy to ensure that the business processes of the department are continuously reviewed and revised. For example, *DOD Instruction 5000.75* requires the functional sponsor of a defense business system to engage in continuous process improvement throughout all phases of the business capability acquisition cycle. The department also fully addressed the element to provide a process for establishing requirements for covered defense business systems with *DOD Instruction 5000.75,* which introduces the business capability acquisition cycle for business system requirements and acquisition.

In addition, DOD fully addressed the element to provide mechanisms for planning and controlling investments in covered defense business systems. Specifically, the department's *Financial Management Regulation;*[27] *Directive 7045.14* on its planning, programming, budgeting, and execution process;[28] and the *April 2017 Defense Business System Investment Management Guidance*[29] provide such mechanisms. For example, the April 2017 investment management guidance includes a process, called the integrated business framework, which the department is to follow for selecting, managing, and evaluating the results of investments in defense business systems. In addition, the directive assigns the DOD CIO responsibility for participating in the department's annual resource allocation process and for advising the Secretary and Deputy Secretary of the Defense on IT resource allocations and investment decisions.

Further, DOD fully addressed the requirement for a policy requiring the periodic review of covered business systems that have been fully

[27]Department of Defense, Under Secretary of Defense (Comptroller), *DOD 7000.14-R: Financial Management Regulation, Volume 2B: "Budget Formulation and Presentation (Chapters 4-19)."*

[28]Department of Defense, *Directive Number 7045.14, The Planning, Programming, Budgeting, and Execution Process* (Jan. 25, 2013).

[29]Department of Defense, Office of the Deputy Chief Management Officer, *Defense Business Systems Investment Management Guidance, Version 4.0* (April 2017).

deployed, by portfolio, to ensure that investments in such portfolios are appropriate. Specifically, the department's *April 2017 Defense Business System Investment Management Guidance* requires the department to annually review an organization's plan for managing its portfolio of defense business systems over the period of the current future-years defense program (e.g., Army's plan for its financial management systems) to ensure, among other things, that the portfolio is aligned with applicable functional strategies (e.g., DOD's strategy for its financial management functional area).

DOD partially addressed the element requiring policy to ensure full consideration of sustainability and technological refreshment requirements, and the appropriate use of open architectures. Specifically, the department established policy requiring consideration of open architectures, but it has not established policy requiring consideration of sustainability and technological refreshment requirements. The Office of the DCMO stated that future guidance is expected to provide a policy to ensure full consideration of sustainability and technological refreshment requirements. However, the department could not provide a time frame for when the guidance will be developed and issued. Without a policy requiring full consideration of sustainability and technological refreshment requirements for its defense business system investments, the department may not be able to ensure that it has a full understanding of the costs associated with these requirements. As a result, the department may not be able to effectively manage spending on these systems.

DOD has also partially addressed the element requiring policy to ensure that best acquisition and systems engineering practices are used in the procurement and deployment of commercial, modified-commercial, and defense-unique systems. Specifically, the department has established policy requiring the acquisition of business systems to be aligned with commercial best practices and to minimize the need for customization of commercial products to the maximum extent possible. On the other hand, the department has not established policy to ensure the use of best systems engineering practices.

With regard to this finding, officials in the Office of the DCMO asserted that *DOD Instruction 5000.75* addresses the requirement. However, while the instruction requires the system acquisition strategy to include a description of how the program plans to leverage systems engineering, it does not require the use of best systems engineering practices. Without a policy requiring the use of best systems engineering practices in the procurement and deployment of commercial, modified, and defense-

unique systems, the department may be limited in its ability to effectively balance meeting system cost and performance objectives.

DOD Issued Guidance that Addresses New Certification Requirements, and the Military Departments Have Made Mixed Progress in Issuing Supporting Guidance

In addition to guidance for addressing the aforementioned legislative requirements for business systems management, the *NDAA for Fiscal Year 2016* requires the Secretary to direct the DCMO and the CMO of each of the military departments to issue and maintain supporting guidance, as appropriate and within their respective areas of responsibility. In this regard, one of the key areas for which the DCMO and military department CMOs are to provide supporting guidance is the review and certification of defense business systems in accordance with specific requirements.

Specifically, the act requires that, for any fiscal year in which funds are expended for development or sustainment pursuant to a covered defense business system program, the appropriate approval official is to review the system to determine if the system:

- has been, or is being, reengineered to be as streamlined and efficient as practicable, and whether the implementation of the system will maximize the elimination of unique software requirements and unique interfaces;

- is in compliance with the business enterprise architecture or will be in compliance as a result of planned modifications;

- has valid, achievable requirements, and a viable plan for implementing those requirements (including, as appropriate, market research, business process reengineering, and prototyping activities);

- has an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable; and

- is in compliance with the department's auditability requirements.

The act and *DOD Instruction 5000.75* define the systems that the DOD DCMO is responsible for certifying and the systems that military department CMOs are responsible for certifying.

Consistent with the act, in April 2017, the DCMO issued guidance for certifying officials that addresses the certification requirements.[30] Table 3 provides our rating and assessment of the DCMO's guidance for implementing defense business system certification requirements.

---

[30]Department of Defense, Office of the Deputy Chief Management Officer, *Defense Business Systems Investment Management Guidance, Version 4.0* (April 2017).

Table 3: Assessment of Department of Defense Guidance for Implementing Defense Business System Certification Requirements

Guidance requirement	Rating	Assessment
The certifying official is required to determine that the system has been, or is being, reengineered to be as streamlined and efficient as practicable, and the implementation of the system will maximize the elimination of unique software requirements and unique interfaces.	Fully implemented	The department's April 2017 *Defense Business Systems Investment Management Guidance, Version 4.0* requires the certification official to determine how appropriate business process reengineering efforts have been undertaken to ensure that the business processes supported by the business system are as streamlined (or are being streamlined) and efficient as practicable and match best commercial practices, to the maximum extent practicable. The guidance also requires that the certifying official determine how the system has an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements to the maximum extent practicable.
The certifying official is required to determine that the system and business system portfolio are or will be in compliance with the defense business enterprise architecture, or will be in compliance as a result of modifications planned.	Fully implemented	The April 2017 *Investment Management Guidance* requires the certifying official to determine how the defense business system is (or will be) in compliance with the business enterprise architecture.
The certifying official is required to determine that the system has valid, achievable requirements and a viable plan for implementing those requirements (including, as appropriate, market research, business process reengineering, and prototyping activities).	Fully implemented	The April 2017 *Investment Management Guidance* requires the certifying official to determine how the business system has valid, achievable requirements, and a viable plan for implementing the requirements.
The certifying official is required to determine that the system has an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable.	Fully implemented	The department's April 2017 *Investment Management Guidance* requires the certifying official to determine how the defense business system has an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements to the maximum extent practicable.
The certifying official is required to determine that the system is in compliance with the department's auditability requirements.	Fully implemented	The April 2017 *Investment Management Guidance* requires the certification official to determine how the defense business system is in compliance with the department's auditability requirements.

Source: GAO analysis of Department of Defense documentation. GAO-18-130

By establishing guidance requiring that defense business systems be certified on the basis of the legislative requirements, the department is better positioned to ensure that a covered system does not proceed into development (or, if no development is required, into production or fielding) without the appropriate due diligence. Further, the department has taken steps which should help ensure that funds are limited to systems in development or sustainment that meet these requirements.

Air Force and Navy Guidance Partially Addresses Certification Requirements; Army Has Not Yet Issued Guidance

The military departments have made mixed progress in developing supporting guidance to assist in making certification decisions regarding systems within their respective areas of responsibility. More specifically, the Air Force has issued supporting guidance that addresses three of the act's five certification requirements, but does not address the remaining two requirements. Navy has issued guidance that addresses two of the certification requirements, partially addresses one requirement, and does not address two requirements.[31] The Army has not yet issued guidance on any of the five certification requirements.[32]

Table 4 provides an overview of our assessment of the Air Force's, Navy's, and Army's guidance relative to the *NDAA for Fiscal Year 2016* certification requirements. Each department's efforts are further discussed following the table.

---

[31]Subsequent to sending a draft of this report to DOD for comment in December 2017, the Department of the Navy issued guidance that addresses all of the certification requirements.

[32]Subsequent to sending a draft of this report to DOD for comment, the Department of the Army issued its *Implementation Guidance for the DoDI 5000.75, Defense Business System Requirements and Acquisition Process* on March 23, 2018, and provided it to us on March 27, 2018. Due to the date on which we received the Army's guidance, we did not include an assessment of the guidance in this report.

Table 4: Assessment of Air Force's, Navy's, and Army's Guidance Relative to the NDAA for Fiscal Year 2016 Certification Requirements, as of February 2018

Certification requirement	Air Force	Navy	Army
Sufficient business process reengineering	Fully addressed:	Fully addressed:	Not addressed
Business enterprise architecture compliance	Fully addressed:	Fully addressed:	Not addressed
Valid requirements and a viable plan to implement them	Fully addressed:	Partially addressed	Not addressed
Acquisition strategy to eliminate or reduce the need to tailor commercial off-the-shelf systems	Not addressed	Not addressed	Not addressed
Compliance with the department's auditability requirements	Not addressed	Not addressed	Not addressed

Source: GAO analysis of Department of Defense documentation. | GAO-18-130

Note: NDAA FY 2016 = *National Defense Authorization Act for Fiscal Year 2016.*

- **Air Force.** In April 2017, the Department of the Air Force issued guidance for certifying business systems for fiscal year 2018. The guidance addresses the requirements that a system be certified on the basis of sufficient business process reengineering, business enterprise architecture compliance, and valid requirements and a viable plan to implement them. Specifically, the guidance states that Air Force core defense business systems are required to comply with the business process reengineering guidance prescribed in the DCMO's February 2015 *Defense Business Systems Investment Management Process Guidance*[33] and for systems to assert compliance with the architecture through DCMO's Integrated Business Framework—Data Alignment Portal. In addition, the guidance states that the department must follow *DOD Instruction 5000.75,* which requires that certifying officials determine that business requirements are valid and capability efforts have feasible implementation plans.

  However, the Air Force guidance does not address the remaining two certification requirements. Officials in the office of the Air Force DCMO acknowledged that the Air Force's business system certification guidance does not address determining how the acquisition strategy is designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable or is in compliance with DOD's auditability requirements.

---

[33]The Air Force issued its guidance on April 21, 2017, before DCMO updated its February 2015 guidance on April 26, 2017.

In May 2017, Air Force DCMO officials stated that the department was in the process of developing guidance. However, as of December 2017, the Air Force had not described specific plans to update its business system certification guidance.

- **Navy.** The Department of the Navy issued guidance in May 2016. This guidance addresses the requirements that a system be certified on the basis of sufficient business process reengineering and business enterprise architecture compliance. In this regard, the guidance provides guidelines for documenting business process reengineering and requires verification that business process reengineering is complete. The guidance also specifies that defense business systems are to map alignment with the business enterprise architecture in DCMO's Integrated Business Framework–Data Alignment Portal.

  Navy's guidance partially addresses the certification requirement for determining if a defense business system has valid requirements and a viable plan to implement them. Specifically, the guidance includes information on validating requirements; however, it does not include information on determining if a system has a viable plan to implement the requirements.

  In addition, Navy's guidance does not address the remaining two certification requirements, which are to determine that the covered defense business system has an acquisition strategy that eliminates or reduces the need to tailor commercial-off-the-shelf systems, and that the system is in compliance with DOD's auditability requirements. In August 2017, officials in the Office of the Under Secretary of the Navy (Management) stated that the office was in the process of updating its May 2016 *Defense Business System Investment Certification Manual*. The officials stated that the goal is to issue interim investment certification guidance by May 2018. As of November 2017, however, Navy had not established a plan for when it expects to publish finalized certification guidance.[34]

- **Army.** The Department of the Army has not issued guidance that addresses any of the act's certification requirements. The Army issued a template that was to be used to develop fiscal year 2018

---

[34]Subsequent to sending a draft of this report to DOD for comment in December 2017, in comments from the Department of the Navy, provided by DOD, Navy stated that it planned to issue guidance by February 2018. Navy issued guidance that addresses the certification requirements on March 8, 2018.

portfolio review submissions. However, the template does not address any of the certification requirements.

Officials in the Army's Office of Business Transformation explained that the Army used DOD DCMO's 2014 guidance to certify its business systems for fiscal year 2017. In May 2017, they stated that the Army was in the process of developing guidance to implement DOD's new instruction. In November 2017, an official in the Army's Office of Business Transformation stated that the office was in the process of completing the guidance and aimed to provide it to the Deputy Under Secretary's office for signature in January 2018. However, the department has not committed to a specific time frame for when the new guidance is expected to be issued.[35]

Without guidance for the certification authority to determine that defense business systems have addressed each of the act's certification requirements, the Air Force, Navy, and Army risk allowing systems to proceed into development or production that do not meet these requirements. In particular, the military departments risk wasting funds on developing and maintaining systems that do not have valid requirements and a viable plan to implement the requirements, introduce unnecessary complexity, or that do not adequately support the Department of Defense's efforts to meet its auditability requirements.

---

[35]Subsequent to sending a draft of this report to DOD for comment in December 2017, in comments from the Department of the Army, provided by DOD, Army stated that it planned to issue guidance by February 28, 2018. The department issued its *Implementation Guidance for the DoDI 5000.75, Defense Business System Requirements and Acquisition Process* on March 23, 2018, and provided it to us on March 27, 2018. Due to the date on which we received the Army's guidance, we did not include an assessment of guidance in this report.

DOD Has Efforts Underway to Improve Its Business Enterprise Architecture, but Its IT Architecture Is Not Complete

According to the *NDAA for Fiscal Year 2016,* DOD is to develop and maintain a defense business enterprise architecture to guide the development of integrated business processes within the department. In addition, the act states that the business architecture must be consistent with the policies and procedures established by the Director of the Office of Management and Budget. Among other things, OMB policy calls for agencies to develop an enterprise architecture that describes the current architecture, target architecture, and a transition plan to get to the target architecture.[36] The act also calls for the business architecture to contain specific content, including policies, procedures, business data standards, business information requirements, and business performance measures that are to apply uniformly throughout the department.

DOD has developed a business enterprise architecture that is intended to help guide the development of its defense business systems. The department issued version 10 of the business architecture, which is currently being used to support system certification decisions, in February 2013. The business architecture and related documentation[37] include content describing aspects of the current architecture, target architecture, and a transition plan to get to the target architecture. In addition, the business architecture includes content that addresses the act's requirements. Table 5 provides examples of required content in DOD's business enterprise architecture.

---

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

[37]The department has defined its business enterprise architecture as information available in version 10 of the architecture, as well as certain data contained in repositories such as the Integrated Business Framework–Data Alignment Portal and the DOD IT Portfolio Repository. The Integrated Business Framework–Data Alignment Portal includes information such as DOD business transformation priorities; the business capabilities required to support those priorities; and initiatives that enable those capabilities. The DOD IT Portfolio Repository includes defense business system attributes such as transition plan state (i.e., legacy or core), life cycle phase, and whether legacy system migration is planned to be full or partial, among other attributes.

Table 5: Examples of Required Content Included in the Department of Defense's Business Enterprise Architecture

NDAA FY 2016 Requirement	Content included in the business enterprise architecture
Policies and procedures that are to apply uniformly throughout the department.	The architecture includes a repository of laws, regulations, and policies that describe compliance constraints that are to apply throughout the department's business mission areas.
Business data standards that are to apply uniformly throughout the department.	The architecture includes a standard financial information structure matrix that contains a list of data structures intended to help standardize financial reporting across DOD.
Business information requirements that apply throughout the department.	The architecture includes conceptual data models that capture business information requirements for DOD's core business missions, such as financial management, human resources management, and materiel supply and services management.
Business performance measures that apply throughout the department.	The information captured in the department's Integrated Business Framework—Data Alignment Portal system[a] includes performance measures that apply throughout the department. For example, the system includes functional strategies, which include initiatives and performance measures associated with the initiatives.
Identification of whether each existing business system is a part of the business systems environment outlined by the defense business enterprise architecture, will become a part of that environment with appropriate modifications, or is not a part of that environment.	Data captured in the DOD IT portfolio repository[b] describe business systems as either core (i.e., part of the target business systems environment) or legacy (i.e., scheduled for termination within 36 months), based on system life cycle end dates. In addition, the repository documents legacy systems that are to become core systems after appropriate modifications.

Source: GAO analysis of Department of Defense documentation. | GAO-18-130

Note: NDAA FY 2016 = *National Defense Authorization Act for Fiscal Year 2016*.

[a]The department defines its business enterprise architecture as including data found in its Integrated Business Framework–Data Alignment Portal system.

[b]The department defines its business enterprise architecture as including data found in its DOD IT Portfolio Repository

Nevertheless, some content included in version 10 of the business architecture is outdated and incomplete. For example, version 10 of the business architecture's repository of laws, regulations, and policies was last updated in February 2013, and officials in the Office of the DOD CIO and Office of the DCMO confirmed that they are not current. Further, the department's March 2017 business architecture compliance guidance stated that not all relevant business data standards are identified in the business architecture. In addition, based on our review, information about performance measures documented in the architecture is incomplete. For example, target values for performance measures associated with acquisition and logistics initiatives are not identified.

According to officials in the Office of the DCMO, the department is working to update the business architecture. Specifically, the department has developed version 11 of the business architecture to, in part, replace outdated architecture content. According to the officials, version 11 of the architecture is currently available online, but version 10 remains the

official version of the business enterprise architecture used for system certification decisions. The officials stated that the department continues to add content to version 11, and they expect that it will be used as the basis of system certification decisions for fiscal year 2019.

In addition, DOD has ongoing work to address a key recommendation we made in July 2015 associated with improving the usefulness of its business architecture. In particular, we reported that the majority of military department portfolio managers that we surveyed[38] believed that the business architecture had not been effective in meeting intended outcomes.[39] For example, only 25 percent of the survey respondents reported that the business architecture effectively enabled DOD to routinely produce timely, accurate, and reliable business and financial information for management purposes. In addition, only 38 percent reported that the business architecture effectively guided the implementation of interoperable defense business systems. As a result, we reported that the architecture had produced limited value and recommended that the department use the results of our survey to determine additional actions that can improve the department's management of its business enterprise architecture activities.

In response to our recommendation, DOD identified opportunities to address our survey findings and developed a plan for improving its ability to achieve architecture-related outcomes.[40] DOD's business enterprise architecture improvement plan was signed by the Assistant DCMO in January 2017. However, the department has not yet demonstrated that it has delivered the capabilities described by the plan; thus, we will continue to monitor DOD's progress to fully address this recommendation.

---

[38]In 2015, GAO developed a structured data collection instrument (survey) to gather information on the extent to which DOD's business enterprise architecture and business process reengineering efforts were achieving their intended outcomes and their effectiveness in achieving associated benefits. As described in GAO-15-627, the survey was directed to military department portfolio managers, who managed groups of systems in defined portfolios.

[39]The outcomes we evaluated at that time were substantially similar to the outcomes described in the *NDAA for Fiscal Year 2016*.

[40]Department of Defense, Office of the Deputy Chief Management Officer, *Business Enterprise Architecture Improvements* (January 2017).

DOD Has Taken Steps to Develop Its IT Enterprise Architecture, but Does Not Have a Plan That Provides a Road Map for Improving the Department's IT and Computing Infrastructure

In addition to the business enterprise architecture, according to the act, the DOD CIO is to develop an IT enterprise architecture. This architecture is to describe a plan for improving the IT and computing infrastructure of the department, including for each of the major business processes.

Officials in the Office of the DOD CIO stated that the department considers its information enterprise architecture to be its IT enterprise architecture.[41] The DOD CIO approved version 2.0 of its information enterprise architecture in August 2012. According to DOD documentation, this architecture describes the department's current information enterprise (i.e., information resources, assets, and processes used to share information across the department and with its mission partners) and includes a vision for the target information enterprise; documents required capabilities, and the activities, rules, and services needed to provide them; and includes information for applying and complying with the architecture.

Nevertheless, while the architecture includes content describing the department's current and target information enterprise, which is consistent with OMB guidance, it does not include a transition plan that provides a road map for improving the department's IT and computing infrastructure. Related to this finding, DCMO officials did not agree with our assessment concerning the department's IT enterprise architecture transition plan. In this regard, officials in the Office of the DCMO stated that the department's DOD IT Portfolio Repository includes information for managing efforts to improve IT and computing infrastructure at the system level. According to the repository's data dictionary, this

---

[41]*DOD Directive 8000.01: Management of the Department of Defense Information Enterprise* (March 17, 2016, and incorporating change 1, July 27, 2017) defines the DOD information enterprise architecture as the architecture that describes the DOD information enterprise. The directive states that the information enterprise architecture includes the infrastructure, communications systems and services, computing systems and services, and the functional processes for DOD information enterprise customers. According to the directive, the information enterprise architecture is the DOD CIO's contribution to the DOD enterprise architecture, which also consists of the business enterprise architecture; the architectures from the intelligence and warfighting mission areas; and the DOD component architectures.

information can include system life cycle start and end dates, as well as information that supports planning for a target environment.

However, documentation describing DOD's information enterprise architecture does not identify the DOD IT Portfolio Repository as being part of the architecture. Moreover, it does not include a plan for improving the department's IT and computing infrastructure for each of the major business processes. Officials in the Office of the CIO acknowledged that the architecture does not include such plans. According to the officials, the department is currently developing version 3.0 of its information enterprise architecture (i.e., its IT enterprise architecture). The officials stated that the department does not currently intend for the architecture to include a plan for improving the department's IT and computing infrastructure that addresses each of the major business processes. They added, however, that there is an effort to ensure that functional areas, such as human resources management, are included. DCMO officials stated that the department has not defined how the DOD IT enterprise architecture needs to be segmented for each major business process because the infrastructure requirements seem to be similar for each of the processes.

Without an architecture that includes a plan for improving its IT and computing infrastructure, including for each of the major business processes, DOD risks not ensuring that stakeholders across the department have a consistent understanding of the steps needed to achieve the department's future vision, agency priorities, potential dependencies among investments, and emerging and available technological opportunities.

DOD Has Not Demonstrated That Its Business and IT Architectures Are Integrated

According to the act, the DOD business enterprise architecture is to be integrated into the DOD IT enterprise architecture. The department's business architecture compliance guide also recognizes that the business architecture is to be integrated with the IT enterprise architecture.

However, the department has not demonstrated that it has integrated the business enterprise architecture into the information enterprise architecture. Specifically, the department did not provide documentation associated with either architecture that describes how the two are, or are to be, integrated. The business enterprise architecture compliance guide states that *DOD Directive 8000.01* implements the requirement that the

two architectures are to be integrated. However, the directive does not address how they are, or are to be, integrated.

Officials in the Offices of the CIO and the DCMO described steps they were taking to coordinate the development of the next versions of the information enterprise architecture (i.e., IT enterprise architecture) and business enterprise architecture. However, these steps were not sufficient to help ensure integration of the two architectures. Specifically, in June 2017, officials in the Office of the DOD CIO stated they were participating in the development of the next version of the business architecture and that the DOD CIO is represented on the Business Enterprise Architecture Configuration Control Board.[42] Officials in the Office of the DCMO confirmed that DOD CIO officials participate on the board. However, officials from the Office of the DCMO said that, until it met in June 2017 the board had not met since 2014. Moreover, documentation of the June 2017 meeting, and a subsequent November 2017 meeting, did not indicate that the board members had discussed integration of the department's business and information enterprise architectures.

In addition, officials in the Office of the DCMO reported that the office has not actively participated in the information enterprise architecture working group. Further, our review of meeting minutes from this working group did not identify participation by officials in the Office of the DCMO, or that integration of the architectures was discussed. The Office of the DCMO described other mechanisms for its sharing of information about architectures with the Office of the DOD CIO. For example, the Office of the DCMO stated that it participates with DOD CIO bodies governing version 3.0 development. Nevertheless, the Office of the DCMO reiterated that technical integration of the architectures has not been designed.

Until DOD ensures that its business architecture is integrated into its IT enterprise architecture, the department may not be able to ensure that its business strategies capitalize on technologies and that its IT infrastructure will support DOD's business priorities and related business strategies.

---

[42]The Business Enterprise Architecture Configuration Control Board was established in August 2013 to assess and recommend changes to the business architecture. It is composed of the business enterprise architecture Chief Architect and representatives of the department's Office of the CIO and other DOD organizations.

The Defense Business Council Addressed Legislative Provisions to Provide Advice on Defense Business Systems to the Secretary of Defense

The *NDAA for Fiscal Year 2016* requires the Secretary to establish a Defense Business Council, chaired by the DCMO and the DOD CIO, to provide advice to the Secretary on:

- developing the business enterprise architecture,

- reengineering the department's business processes,

- developing and deploying business systems, and

- developing requirements for business systems.

DOD established the department's Defense Business Council in October 2012, prior to the act. According to its current charter, dated December 2014, the Council is co-chaired by the DCMO and the DOD CIO. In addition, the Council is to serve as the principal governance body for vetting issues related to managing and improving defense business operations. Among other things, it serves as the investment review board for defense business system investments.

The Defense Business Council charter also states that the Council was established as a principal supporting tier of governance to the Deputy's Management Action Group. The Deputy's Management Action Group was established by an October 2011 memorandum issued by the Deputy Secretary of Defense. According to information published on DCMO's website, the group was established to be the primary civilian-military management forum that supports the Secretary of Defense, and is to address top department issues that have resource, management, and broad strategic and/or policy implications.[43] The group's primary mission is to produce advice for the Deputy Secretary of Defense in a collaborative environment and to ensure that the group's execution aligns with the Secretary of Defense's priorities. According to the Office of the DCMO, the Defense Business Council determines whether or not to elevate a topic to the Deputy's Management Action Group to address on behalf of the Secretary.

---

[43]Department of Defense, Deputy Chief Management Officer, *Deputy's Management Action Group (DMAG)*, accessed Aug. 29, 2017, http://dcmo.defense.gov/Governance/Deputys-Management-Action-Group/

Based on our review of meeting documentation for 27 meetings that the Defense Business Council held between January 2016 and August 2017, the Council discussed the four topics on which the *NDAA for Fiscal Year 2016* requires it to provide advice to the Secretary. According to the Office of the DCMO, during the discussions of these topics, the Council did not identify any issues related to the topics that needed to be elevated to the Deputy's Management Action Group. Table 6 identifies the number of meetings in which the Council discussed each topic during this time period.

Table 6: Number of DOD Defense Business Council Meetings Held During January 2016-August 2017 That Addressed Business Systems Topics on Which the NDAA for Fiscal Year 2016 Required Advice Be Provided to the Secretary of Defense

Topic	2016	2017 (January-August)	Total
Developing the business enterprise architecture	6	5	**11**
Reengineering the department's business processes	9	7	**16**
Developing and deploying business systems	14	7	**21**
Developing requirements for business systems	15	5	**20**

Source: GAO analysis of Department of Defense information. | GAO-18-130

Notes: The Defense Business Council held a total of 29 meetings in January 2016 through August 2017. Of these meetings, we reviewed documentation of 27 meetings. The other 2 meetings were classified. NDAA = National Defense Authorization Act.

By ensuring that the required business system topics are discussed during Defense Business Council meetings, the department should be positioned to raise issues to the Deputy's Management Action Group, and ultimately, to advise the Secretary of Defense on matters associated with these topics.

DOD Certified Selected Business Systems for Fiscal Year 2017 on the Basis of Earlier Certification Requirements

The *NDAA for Fiscal Year 2016* requires that, for any fiscal year in which funds are expended for development or sustainment pursuant to a covered defense business system program, the Secretary of Defense is to ensure that a covered business system not proceed into development (or, if no development is required, into production or fielding) unless the appropriate approval official reviews the system to determine if the system meets five key requirements, as previously discussed in this report. In addition, the act requires that the appropriate approval official certify, certify with conditions, or decline to certify that the system satisfies these five requirements.

The department issued *DOD Instruction 5000.75,* which established business system categories and assigned certifying officials, consistent with the act. Table 7 describes the business system categories and the assigned certifying officials, as defined in *DOD Instruction 5000.75.*

Table 7: Defense Business System Categories and Assigned Certifying Officials

Category	Description	Certifying official
I (Priority)	Systems expected to have a total amount of budget authority of more than $250 million over the period of the current future-years defense program or are designated by the Deputy Chief Management Officer (DCMO) as priority based on complexity, scope, and technical risk.	Category I systems are to be certified by the Department of Defense (DOD) DCMO unless delegated.
II	Systems that do not meet the criteria for priority systems and are expected to have a total amount of budget authority of between $50 million and $250 million, over the period of the current future-years defense program, or are designated by the DMCO or military department Chief Management Officer as requiring certification.	Category II systems owned by military departments are to be certified by the military department's Chief Management Officer unless delegated, and Category II systems owned by other DOD components are to be certified by the DOD DCMO unless delegated
III	Systems that do not meet criteria for category II systems.	Category III systems are not required to be certified.

Source: GAO analysis of the National Defense Authorization Act for Fiscal Year 2016 and Department of Defense documentation. | GAO-18-130

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

The DOD DCMO certified the five systems in our sample (which included the military departments' systems) for fiscal year 2017. However, these certifications were issued in accordance with the previous fiscal year's (fiscal year 2016) certification requirements. Those requirements had stipulated that a defense business system program was to be reviewed and certified on the basis of the system's compliance with the business enterprise architecture and appropriate business process reengineering, rather than on the basis of having met all five requirements identified in the *NDAA for Fiscal Year 2016.*

Specifically, DCMO certified the systems on the basis of determining that the systems were in compliance with the business enterprise architecture and had been sufficiently reengineered. However, none of the systems were certified on the basis of a determination that they had valid, achievable requirements and a viable plan for implementing them; had an acquisition strategy to reduce or eliminate the need to tailor commercial off-the-shelf systems; or were in compliance with the department's auditability requirements.

Officials in the Offices of the DOD DCMO, the Air Force DCMO, the Under Secretary of the Navy (Management), and Army Business Transformation told us that the systems were not certified relative to three of the requirements because the department did not issue guidance to reflect changes made by the *NDAA for Fiscal Year 2016* in time for the fiscal year 2017 certification process. Prior to the *NDAA for Fiscal Year 2016,* relevant legislation and DOD guidance only called for annual determinations to be made regarding whether a system complied with the business enterprise architecture and whether appropriate business process reengineering had been conducted.

In January 2016, the DCMO issued a memorandum stating that the department planned to issue new guidance and policy to implement the new legislation by the end of February 2016. However, the department did not issue additional guidance addressing the new certification requirements until April 2017. The system certifications, which were required by the act to be completed before systems could spend fiscal year 2017 funds, occurred in August and September 2016.

In explaining the delay in issuing new guidance on the certification requirements, officials in the Office of the DCMO stated that the statutory deadline for issuing guidance was December 31, 2016. They added that, given this statutory deadline, and the start of fiscal year 2017 on October 1, 2016, it was their determination that Congress did not intend for the *NDAA for Fiscal Year 2016's* certification requirements to be fully implemented before fiscal year 2017 started. DCMO officials stated that they intend for the department to use the certification requirements established by the *NDAA for Fiscal Year 2016* for future system certifications.

While it was reasonable for the department to use the earlier guidance for its fiscal year 2017 certifications, given that the new guidance had not yet been issued, it will be important going forward that the department certifies business systems on the basis of the certification requirements established in the *NDAA for Fiscal Year 2016* and its related guidance addressing these requirements.[44] Certifying systems on the basis of the act's requirements should help ensure that funds are not wasted on

---

[44]In technical comments on a draft of this report, DOD stated that the department certified many systems to meet fiscal year 2016 NDAA requirements during the 2018 certification cycle. However, we did not verify whether the systems were certified because our assessment focused on certifications conducted for fiscal year 2017.

developing and maintaining systems that do not have valid requirements and a viable plan to implement the requirements, that introduce unnecessary complexity, or that impede the Department of Defense's efforts to meet its auditability requirements.

Conclusions

Since the *NDAA for Fiscal Year 2016* was signed in November 2015, DOD has issued guidance that addresses most provisions of the *NDAA for Fiscal Year 2016* related to managing defense business system investments. However, the department has not established policies requiring consideration of sustainability and technology requirements and the use of best systems engineering practices in the procurement and deployment of its systems. Having these policies would better enable the department to ensure it is efficiently and effectively procuring and deploying its business systems.

In addition, the Air Force, the Army, and Navy have made mixed progress in issuing guidance to assist in making certification decisions regarding systems within their respective areas of responsibility. Specifically, the Air Force and Navy issued guidance on the certification of business systems that does not fully address new certification requirements, while the Army has not issued any updated guidance for its certifications. As a result, the Air Force, Navy, and Army risk wasting funds on developing and maintaining systems that do not have valid requirements and a viable plan to implement the requirements, introduce unnecessary complexity, or do not adequately support the Department of Defense's efforts to meet its auditability requirements.[45]

Also, DOD has developed an IT architecture, but this architecture does not address the act's requirement that it include a plan for improving the department's IT and computing infrastructure, including for each business process. In addition, DOD's plans for updating its IT architecture do not address how the department intends to integrate its business and IT architectures, as called for by the act. As a result, DOD risks not having a

---

[45]Subsequent to sending a draft of this report to DOD for comment in December 2017, the Department of the Navy issued guidance that addresses all of the certification requirements. In addition, the Department of the Army issued its *Implementation Guidance for the DoDI 5000.75, Defense Business System Requirements and Acquisition Process,* on March 23, 2018, and provided it to us on March 27, 2018. Due to the date on which we received this guidance, we did not include an assessment of the guidance in this report.

consistent understanding of what is needed to achieve the department's future vision, agency priorities, potential dependencies among investments, and emerging and available technological opportunities.

Recommendations for Executive Action

We are making six recommendations, including three to the Secretary of Defense and one to each of the Secretaries of the Air Force, the Navy and the Army:

The Secretary of Defense should define a specific time frame for finalizing, and ensure the issuance of (1) policy requiring full consideration of sustainability and technological refreshment requirements for its defense business system investments; and (2) policy requiring that best systems engineering practices are used in the procurement and deployment of commercial systems, modified commercial systems, and defense-unique systems to meet DOD missions. (Recommendation 1)

The Secretary of the Air Force should define a specific time frame for finalizing, and ensure the issuance of guidance for certifying the department's business systems on the basis of (1) having an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable; and (2) being in compliance with DOD's auditability requirements. (Recommendation 2)

The Secretary of the Navy should define a specific time frame for finalizing, and ensure the issuance of guidance for certifying the department's business systems on the basis of (1) having a viable plan to implement the system's requirements; (2) having an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable; and (3) being in compliance with DOD's auditability requirements. (Recommendation 3)

The Secretary of the Army should define a specific time frame for finalizing, and ensure the issuance of guidance for certifying the department's business systems on the basis of (1) being reengineered to be as streamlined and efficient as practicable, and determining that

implementation of the system will maximize the elimination of unique software requirements and unique interfaces; (2) being in compliance with the business enterprise architecture; (3) having valid, achievable requirements and a viable plan to implement the requirements; (4) having an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable; and (5) being in compliance with DOD's auditability requirements. (Recommendation 4)

The Secretary of Defense should ensure that the DOD CIO develops an IT enterprise architecture which includes a transition plan that provides a road map for improving the department's IT and computing infrastructure, including for each of its business processes. (Recommendation 5)

The Secretary of Defense should ensure that the DOD CIO and Chief Management Officer work together to define a specific time frame for when the department plans to integrate its business and IT architectures and ensure that the architectures are integrated. (Recommendation 6)

Agency Comments and Our Evaluation

DOD provided written comments on a draft of this report, which are reprinted in appendix III. In the comments, the department stated that it concurred with three of the recommendations and partially concurred with three of the recommendations. DOD also provided evidence that it has fully addressed one of the recommendations. In addition, DOD provided technical comments that we incorporated in the report, as appropriate.

DOD stated that it concurred with our first recommendation, which called for it to define a specific time frame for finalizing, and ensure the issuance of, policies that fully address provisions in the *NDAA for Fiscal Year 2016*. Furthermore, the department stated that it had complied with the recommendation. Specifically, the department stated that it had published its defense business systems investment management guidance in April 2017. This guidance identifies DOD's *Financial Management Regulation*, Volume 2B, Chapter 18 "Information Technology" and supporting IT budget policy and guidance as well as *DOD Instruction 5000.75* and supporting acquisition policy and guidance. The department stated that the Financial Management Regulation specifically addresses the requirement for sustainability and technological refreshment requirements for its defense business system investments.

While DOD reported taking this action, we do not agree that the department has complied with our recommendation. In reviewing the department's guidance, we found that none of the cited management documents includes a policy requiring consideration of sustainability and technological refreshment requirements for DOD's defense business systems. Further, none of these documents includes a policy requiring that best systems engineering practices be used in the procurement and deployment of commercial, modified-commercial, and defense unique systems.

Without a policy requiring full consideration of sustainability and technological refreshment requirements for its defense business system investments, the department may not be able to ensure that it has a full understanding of the costs associated with these requirements. Further, without a policy requiring the use of best systems engineering practices in systems procurement and deployment, the department may be limited in its ability to effectively balance meeting system cost and performance objectives. Accordingly, we continue to believe that our recommendation is valid.

The department concurred with our second recommendation, that the Secretary of the Air Force define a specific time frame for finalizing, and ensure the issuance of, guidance that fully addresses certification requirements, in accordance with the *NDAA for Fiscal Year 2016*. Moreover, the department stated that the Air Force has complied with the recommendation. Specifically, DOD stated that *Air Force Manual 63-144* details the consideration of using existing commercial solutions without modification or tailoring.

However, while the manual provides a foundation on which the Air Force can build, it is not sufficient to fully address our recommendation because it does not include guidance on certifying business systems on the basis of having an acquisition strategy that eliminates or reduces the need to tailor commercial-off-the-shelf systems. In addition, the department did not demonstrate that the Air Force has issued guidance for certifying business systems on the basis of being in compliance with DOD's auditability requirements. Rather, the Air Force stated that it has pending guidance that addresses the acquisition strategy and auditability requirements. We plan to evaluate the guidance to determine the extent to which it addresses our recommendation after it is issued.

The department partially agreed with our third recommendation, that the Secretary of the Navy define a specific time frame for finalizing, and

ensure the issuance of, guidance that fully addresses certification requirements. Specifically, DOD stated that Navy agreed to issue guidance. Subsequently, on March 8, 2018, Navy issued its updated guidance.

However, Navy disagreed with the recommendation, as written, and suggested that GAO revise the recommendation to state that "The Secretary of the Navy should ensure guidance is issued according to [the] established timeline for certifying the department's business systems. . ." According to Navy, this change would support alignment with the timeline for certifying the department's business systems driven by the Chief Management Officer investment review timeline.

Based on our analysis, we found the guidance that Navy issued to be consistent with our recommendation. Thus, we plan to close the recommendation as fully implemented. We have also annotated this report, where appropriate, to explain that the Navy issued guidance while the draft of this report was at the department for comment. On the other hand, we did not revise the wording of our recommendation, as we believe it appropriately reflected the importance of Navy taking action to ensure the issuance of its guidance.

The department stated that it concurred with our fourth recommendation, which called for the Secretary of the Army to define a specific time frame for finalizing, and ensure the issuance of, guidance for certifying the department's business systems on the basis of the certification requirements. Furthermore, on March 23, 2018, the Army issued its guidance. However, because of the timing of this report relative to when the Army provided its guidance to us (on March 27, 2018), we have not yet completed an assessment of the guidance.[46] We have annotated this report, where appropriate, to reflect the Army's action on our recommendation.

The department stated that it partially concurred with our fifth recommendation. This recommendation called for the DOD CIO to develop an IT enterprise architecture which includes a transition plan that

---

[46]Army's *Implementation Guidance for the DoDI 5000.75, Defense Business System Requirements and Acquisition Process* was signed by the Under Secretary of the Army on March 23, 2018, and provided to us on March 27, 2018. When we have completed our review of the guidance, we will provide the status of the recommendation on our website, http://www.gao.gov.

provides a road map for improving the department's IT and computing infrastructure, including for each of its business processes. Toward this end, the department agreed that the DOD CIO should develop an architecture that enables improving the department's IT and computing infrastructure for each of its business processes. However, the department also stated that the recommendation is not needed because the goal is already being accomplished by a set of processes, organizations, protocols, and architecture data.

For example, the department described processes and relationships between the Office of the DOD CIO and the Office of the Chief Management Officer and the boards that support the department's business and IT enterprise architectures. In particular, the department stated that information enterprise architecture data relevant to the business enterprise are accessed via the DOD Information Enterprise Architecture Data Selection Wizard and imported into the business enterprise architecture. The department further stated that, if the business capability acquisition cycle process indicates a need to improve the IT or computing infrastructure, the Office of the Chief Management Officer has a protocol to initiate a proposal to change the information enterprise architecture.

We agree that the department's processes, organizations, protocols, and architecture data are keys to successful IT management. However, during the course of our audit, we found that documentation describing DOD's IT architecture did not include a plan for improving the department's IT and computing infrastructure for each of the major business processes. Moreover, officials in the Office of the CIO acknowledged that the architecture did not include such a plan.

Without a transition plan that provides a road map for improving the department's IT and computing infrastructure, including for each of its business processes, it will be difficult for the department to rely on its personnel to timely and proactively manage and direct modernization efforts of such a magnitude as DOD's systems modernization efforts. Further, without such a plan, DOD risks not being able to ensure that stakeholders across the department have a consistent understanding of the steps needed to achieve the department's future vision, agency priorities, potential dependencies among investments, and emerging and available technological opportunities. Thus, we maintain that the department should fully implement our recommendation.

The department stated that it partially concurred with our sixth recommendation, that the DOD CIO and DCMO work together to define a specific time frame for when the department plans to integrate its business and IT architectures. In particular, the department stated that it agrees that the DOD CIO and Chief Management Officer should work together to establish a time frame and ensure coordination and consistency of the IT and business architectures. However, the department disagreed with the use and intent of the term "integrate," as stated in the recommendation, although it did not explain the reason for this disagreement. Instead, it proposed that we change our recommendation to read "The GAO recommends the Secretary of Defense ensure the DoD CIO and CMO work together to define a specific timeline for coordinating its business and IT architectures to achieve better enterprise alignment among the architectures."

We agree that it is important to achieve coordination and consistency between the business and IT architectures. However, the department did not provide documentation associated with either architecture that describes how the two are, or are to be, integrated, as called for by the *NDAA for Fiscal Year 2016* and DOD guidance.

Integrating the architectures would help ensure that business strategies better capitalize on existing and planned technologies and that IT solutions and infrastructure support business priorities and related business strategies. Thus, we continue to believe that our recommendation is valid. However, we have updated the recommendation to state that the DOD CIO and the Chief Management Officer should work together. We made this change because, effective February 1, 2018, the Secretary of Defense eliminated the DCMO position and expanded the role of the Chief Management Officer, in accordance with the National Defense Authorization Act for Fiscal Year 2018.

We are sending copies of this report to appropriate congressional committees; the Secretary of Defense; the Secretaries of the Army, Navy, and Air Force; and the Director of the Office of Management and Budget. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff members have any questions about this report, please contact me at (202) 512-4456 or harriscc@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 contributions to this report are listed in appendix IV.

Carol C. Harris
Director
Information Technology Acquisition Management Issues

List of Committees

The Honorable John McCain
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Richard Shelby
Chairman
The Honorable Richard Durbin
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Mac Thornberry
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Kay Granger
Chairwoman
The Honorable Peter J. Visclosky
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objective, Scope, and Methodology

Our objective was to determine the actions taken by the Department of Defense (DOD) to comply with provisions included in the *National Defense Authorization Act for Fiscal Year 2016* (NDAA).[1] These provisions require DOD to perform certain activities aimed at ensuring that its business system investments are managed efficiently and effectively. Specifically, we determined to what extent DOD has

1. established guidance for effectively managing its defense business system investments;

2. developed and maintained a defense business enterprise architecture and information technology (IT) enterprise architecture, in accordance with relevant laws and Office of Management and Budget (OMB) policies and guidance;

3. used the Defense Business Council to provide advice to the Secretary on developing the business enterprise architecture, reengineering the department's business processes, developing and deploying business systems, and developing requirements for business systems; and

4. ensured that covered business systems are reviewed and certified in accordance with the act.

To address the extent to which DOD has established guidance for effectively managing defense business system investments, we obtained and analyzed the department's guidance, as well as the guidance established by the Departments of the Air Force, Army, and Navy, for managing defense business systems relative to the act's requirements. Specifically, the *NDAA for Fiscal Year 2016* required the Secretary of Defense to issue guidance, by December 31, 2016, to provide for the coordination of and decision making for the planning, programming, and control of investments in covered defense business systems. The act required this guidance to include the following six elements:

- Policy to ensure DOD business processes are continuously reviewed and revised to implement the most streamlined and efficient business processes practicable and eliminate or reduce the need to tailor

---

[1]Pub. L. No. 114-92, § 883, 129 Stat. 726, 942 (2015).

commercial off-the-shelf systems to meet or incorporate requirements or interfaces that are unique to the department.

- Process to establish requirements for covered defense business systems.

- Mechanisms for planning and controlling investments in covered defense business systems, including a process for the collection and review of programming and budgeting information for covered defense business systems.

- Policy requiring the periodic review of covered defense business systems that have been fully deployed, by portfolio, to ensure that investments in such portfolios are appropriate.

- Policy to ensure full consideration of sustainability and technological refreshment requirements, and the appropriate use of open architectures.

- Policy to ensure that best acquisition and systems engineering practices are used in the procurement and deployment of commercial systems, modified commercial systems, and defense-unique systems to meet DOD missions.

We assessed the February 2017 *DOD Instruction 5000.75, Business Systems Requirements and Acquisitions,* and April 2017 defense business system investment management guidance, which the department issued to address the act's requirements.[2] In addition, we assessed the department's Financial Management Regulation[3] and directive on its planning, programming, budgeting, and execution process,[4] which the department stated also address the act's provisions.

We also assessed DOD's guidance for managing business system investments relative to the act's business system certification requirements. The act requires that the Secretary of Defense ensure that

---

[2]Department of Defense, *DOD Instruction 5000.75: Business Systems Requirements and Acquisition* (Feb. 2, 2017) and Department of Defense, Office of the Deputy Chief Management Officer, *Defense Business Systems Investment Management Guidance, Version 4.0* (April 2017).

[3]Department of Defense, Under Secretary of Defense (Comptroller), *DOD 7000.14-R: Financial Management Regulation, Volume 2B: "Budget Formulation and Presentation (Chapters 4-19)."*

[4]Department of Defense, *Directive Number 7045.14, The Planning, Programming, Budgeting, and Execution (PPBE) Process* (Jan. 25, 2013).

a covered defense business system not proceed into development (or, if
no development is required, into production or fielding) unless the
appropriate approval official determines that the system meets five
requirements. The act further requires for any fiscal year in which funds
are expended for development or sustainment pursuant to a covered
defense business system program, the appropriate approval official to
review the system to determine if the system:

- has been, or is being, reengineered to be as streamlined and efficient
  as practicable, and whether the implementation of the system will
  maximize the elimination of unique software requirements and unique
  interfaces;

- is in compliance with the business enterprise architecture or will be in
  compliance as a result of planned modifications;

- has valid, achievable requirements, and a viable plan for
  implementing those requirements (including, as appropriate, market
  research, business process reengineering, and prototyping activities);

- has an acquisition strategy designed to eliminate or reduce the need
  to tailor commercial off-the-shelf systems to meet unique
  requirements, incorporate unique requirements, or incorporate unique
  interfaces to the maximum extent practicable; and

- is in compliance with the department's auditability requirements.

We compared Office of the Deputy Chief Management Office (DCMO)
certification guidance with the act's certification requirements. In addition,
we compared the guidance established by the Departments of the Air
Force, the Army, and the Navy for certifying their business systems with
the act's certification requirements.

We also interviewed cognizant officials responsible for managing defense
business system investments at DOD, including the military departments.
Specifically, we interviewed officials in the Office of the DCMO, the Office
of the Under Secretary of Defense for Acquisition, Technology, and
Logistics, the Office of the Chief Information Officer (CIO), and the Offices
of the CMOs in the Departments of the Air Force, Army, and Navy.

To determine the extent to which DOD has developed and maintained a
defense business enterprise architecture and IT enterprise architecture, in
accordance with relevant laws and OMB policy and guidance, we
assessed the business enterprise architecture against the relevant laws
and OMB policy and guidance; the IT enterprise architecture against the
relevant laws and OMB policy and guidance; and the department's efforts

to integrate its business and IT architectures against the act's requirement.

To determine the extent to which the department has developed and maintained a business enterprise architecture in accordance with relevant laws and OMB policy and guidance, we reviewed version 10 of its business enterprise architecture,[5] which was released in February 2013, and related information[6] relative to the act's requirements; U.S. Code, Title 44, Section 3601, which defines an enterprise architecture;[7] and OMB policy and guidance.[8] We also reviewed version 11 of the architecture to determine the extent to which it differed from version 10.

Further, we reviewed the department's business enterprise architecture improvement plan,[9] which it developed in response to a recommendation we made in July 2015.[10] Specifically, we recommended that the department use the results of our portfolio manager survey to determine additional actions that could improve the department's management of its enterprise architecture activities. In response to our recommendation, the department developed and approved a plan in January 2017. We assessed the extent to which the department had delivered the planned capabilities relative to the plan. We also reviewed the extent to which the delivery dates of the three planned capabilities and associated tasks changed over time relative to the plan.

---

[5]Version 10 was the version to be used for fiscal year 2018 business system certifications.

[6]The department has defined its business enterprise architecture as certain data available in version 10 of the architecture, as well as information contained in repositories such as the Integrated Business Framework–Data Alignment Portal and the DOD IT Portfolio Repository. The Integrated Business Framework–Data Alignment Portal includes information such as DOD business transformation priorities; the business capabilities required to support those priorities; and initiatives that enable those capabilities. The DOD IT Portfolio Repository includes defense business system attributes such as transition plan state (i.e., legacy or core), life cycle phase, and whether legacy system migration is planned to be full or partial, among other attributes.

[7]44 U.S.C. § 3601.

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

[9]Department of Defense, Office of the Deputy Chief Management Officer, *Business Enterprise Architecture Improvements,* January 2017.

[10]GAO, *DOD Business Systems Modernization: Additional Action Needed to Achieve Intended Outcomes*, GAO-15-627 (Washington, D.C.: July 16, 2015).

To assess the extent to which the department developed and maintained an IT enterprise architecture in accordance with relevant laws and OMB policy and guidance, we reviewed content from the department's IT enterprise architecture and compared it with requirements from the act, U.S. Code, Title 44, Section 3601, and OMB policy and guidance. Specifically, we reviewed version 2.0 of the department's information enterprise architecture, which was released in August 2012, relative to the act's requirement for the DOD CIO to develop an IT enterprise architecture that is to describe a plan for improving the IT and computing infrastructure of the department, including for each of the major business processes. We reviewed volumes I and II of the information enterprise architecture and the four enterprise-wide reference architectures to determine if the architecture described a plan for improving the IT and computing infrastructure of the department, as called for by the act. We also reviewed whether the architecture included content that described the current and the target environments, and a transition plan to get from the current to the target environment, consistent with OMB policy and guidance.[11]

To determine the extent to which the department has integrated its business and IT architectures, as required by the act, we reviewed *DOD Directive 8000.01, Management of the Department of Defense Information Enterprise.*[12] We also reviewed meeting documentation from the information enterprise architecture working group responsible for the development of an updated architecture. In addition, we reviewed meeting documentation from the Business Enterprise Architecture Configuration Control Board to identify any discussions among CIO and DCMO officials regarding integration of the two architectures, as well as the level of participation by both parties.

Finally, we interviewed officials in the Office of the DCMO and the Office of the CIO about efforts to develop and maintain a business enterprise architecture, develop an IT enterprise architecture, and integrate the business and IT architectures.

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

[12]Department of Defense*, Directive 8000.01: Management of the Department of Defense Information Enterprise* (March 17, 2016, and incorporating change 1, July 27, 2017).

To determine the extent to which the department has used the Defense
Business Council to provide advice to the Secretary of Defense on
developing the business enterprise architecture, reengineering the
department's business processes, developing and deploying business
systems, and developing requirements for business systems, in
accordance with the act, we analyzed the department's December 2014
Defense Business Council Charter and April 2017 defense business
systems investment management guidance. We compared information in
the charter and guidance to the requirement that the Secretary establish
the Defense Business Council to advise the Secretary on the required
defense business system topics.

In addition, we obtained and analyzed meeting summaries and briefings
for 27 Defense Business Council meetings that took place from January
2016 through August 2017.[13] Specifically, we assessed the frequency
with which the meetings held during this time period addressed the
required topics. We chose this time period because 2016 was the first
calendar year following the enactment of the *NDAA for Fiscal Year 2016.*
Further, we chose August 2017 as our end date because it was the last
month's data that we could reasonably expect to obtain and review within
our reporting time frame. We also interviewed officials in the Offices of the
DCMO and CIO about the Defense Business Council and the Deputy's
Management Action Group, which is the governance entity to which the
Council reports.

To determine the extent to which DOD has ensured that covered
business systems are reviewed and certified in accordance with the act,
we reviewed a nongeneralizable sample of business systems from DOD's
two categories of covered defense business systems that require
certification. To select the sample, we considered Category I systems,
which were systems that were expected to have a total amount of budget
authority of more than $250 million over the period of the current future-
years defense program,[14] and Category II systems, which were systems

---

[13]The Defense Business Council held a total of 29 meetings in January 2016 through
August 2017. Of these meetings, we reviewed documentation from 27 meetings. The
other 2 meetings were classified.

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

that were expected to have a total amount of budget authority of between $50 million and $250 million over the period of the future-years defense program.

We further categorized the Category II systems into four groups—those owned by the Air Force, the Army, Navy, and the remaining DOD components. We selected one system with the highest expected cost over the course of the department's future-years defense program from each group. This resulted in our selection of five systems: one Category I system, one Category II system from each military department, and one Category II system from the remaining DOD components.

We reviewed, respectively, DOD's Healthcare Management System Modernization Program; Air Force's Maintenance, Repair and Overhaul initiative; Army's Reserve Component Automation System; Navy's Electronic Procurement System; and the Defense Logistics Agency's Defense Agencies Initiative Increment 2. We determined that the number of systems we selected was sufficient for our evaluation.

For each system, we assessed the extent to which it had been certified on the basis of the five certification requirements in the act. Specifically, we evaluated investment decision memos and certification assertions to determine if each system had been certified according to the act's requirements, which include ensuring that the system had been, or was being, reengineered to be as streamlined and efficient as practicable, and the implementation of the system would maximize the elimination of unique software requirements and unique interfaces; was in compliance with the business enterprise architecture or would be in compliance as a result of planned modifications; had valid, achievable requirements, and a viable plan for implementing those requirements; had an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable; and was in compliance with the department's auditability requirements. We did not determine whether the certification assertions were valid. For example, we did not evaluate business process reengineering activities to determine if they were sufficient. We also interviewed DOD DCMO and military department officials about the certification of these systems.

To determine the reliability of the business system cost data used to select the systems, we reviewed system documentation for the three systems DOD uses to store data, which include the Defense Information

Technology Investment Portal, the DOD Information Technology Portfolio Repository, and the Select and Native Programming-Information Technology system. In this regard, we requested and reviewed department responses to questions about the systems and about how the department ensures the quality and reliability of the data. In addition, we requested and reviewed documentation related to the systems (e.g., data dictionaries, system instructions, and user training manuals) and reviewed the data for obvious issues, including missing or questionable values. We also reviewed available reports on the quality of the inventories (e.g., inspector general reports). We found the data to be sufficiently reliable for our purpose of selecting systems for evaluation.

We conducted this performance audit from January 2017 to March 2018 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 Reports on Department of Defense Business System Modernization

Since 2005, we have issued 11 reports assessing DOD's actions to respond to business system modernization provisions contained in U.S. Code, Title 10, Section 2222. The reports are listed below.

DOD Business Systems Modernization: Additional Action Needed to Achieve Intended Outcomes, GAO-15-627 (Washington, D.C.: July 16, 2015).

Defense Business Systems: Further Refinements Needed to Guide the Investment Management Process, GAO-14-486 (Washington, D.C. May 12, 2014).

DOD Business Systems Modernization: Further Actions Needed to Address Challenges and Improve Accountability, GAO-13-557 (Washington, D.C.: May 17, 2013).

DOD Business Systems Modernization: Governance Mechanisms for Implementing Management Controls Need to Be Improved, GAO-12-685 (Washington, D.C.: June 1, 2012).

Department of Defense: Further Actions Needed to Institutionalize Key Business System Modernization Management Controls, GAO-11-684 (Washington, D.C.: June 29, 2011).

Business Systems Modernization: Scope and Content of DOD's Congressional Report and Executive Oversight of Investments Need to Improve, GAO-10-663 (Washington, D.C.: May 24, 2010).

DOD Business Systems Modernization: Recent Slowdown in Institutionalizing Key Management Controls Needs to Be Addressed, GAO-09-586 (Washington, D.C.: May 18, 2009).

DOD Business Systems Modernization: Progress in Establishing Corporate Management Controls Needs to Be Replicated Within Military Departments, GAO-08-705 (Washington, D.C.: May 15, 2008).

DOD Business Systems Modernization: Progress Continues to Be Made in Establishing Corporate Management Controls, but Further Steps Are Needed, GAO-07-733 (Washington, D.C.: May 14, 2007).

Business Systems Modernization: DOD Continues to Improve Institutional Approach, but Further Steps Needed, GAO-06-658 (Washington, D.C.: May 15, 2006).

DOD Business Systems Modernization: Important Progress Made in Establishing Foundational Architecture Products and Investment Management Practices, but Much Work Remains, GAO-06-219 (Washington, D.C.: November 23, 2005).

Appendix III: Comments from the Department of Defense

OFFICE OF THE CHIEF MANAGEMENT OFFICER
9010 DEFENSE PENTAGON
WASHINGTON, DC 20301-9010

March 2, 2018

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

Dear Ms. Harris:

This is the Department of Defense response to the Government Accountability Office (GAO) draft report GAO-18-130, "DEFENSE BUSINESS SYSTEMS: DoD Needs to Continue Improving Guidance and Plans for Effectively Managing Investments" dated December 18, 2017 (GAO Code 101359). The Department concurs with three and partially concurs with three of the six recommendations.

The Department appreciates the opportunity to respond to your draft report. We look forward to your continued cooperation and dialog toward our common goal of effectively managing investments within the Department of Defense business operations. Should you have any questions, please contact Monica Prince, (571) 372-3087, monica.r.prince.civ@mail.mil.

Sincerely,

TILLOTSON.DAVI Digitally signed by
TILLOTSON.DAVID.III.110996681
D.III.1109966815 5
Date: 2018.03.02 14:47:14 -05'00'

David Tillotson III
Assistant Chief Management Officer

GAO DRAFT REPORT dated December 18, 2017
GAO-18-130 (GAO CODE 101359)

"DEFENSE BUSINESS SYSTEMS: DOD NEEDS TO CONTINUE IMPROVING GUIDANCE AND PLANS FOR EFFECTIVELY MANAGING INVESTMENTS"

DoD COMMENTS TO THE GAO RECOMMENDATIONS

Recommendation One: The Secretary of Defense should define a specific time frame for finalizing, and ensure the issuance of (1) policy requiring full consideration of sustainability and technological refreshment requirements for its defense business system investments; and (2) policy requiring that best systems engineering practices are used in the procurement and deployment of commercial systems, modified commercial systems, and defense-unique systems to meet DoD mission.

DoD RESPONSE: Concur. The Department concurs and has complied by publishing Defense Business Systems Investment Management Guidance, Version 4.0 in April 2017. The guidance identifies the DoD Financial Management Regulation Volume 2B, Chapter 18 "Information Technology" and supporting IT budget policy and guidance which addresses the requirement for sustainability and technological refreshment requirements for its defense business system investments. Also identified, is the DoD Instruction 5000.75 "Business Systems Requirements and Acquisition" and supporting acquisition policy and guidance.

Recommendation Two: The Secretary of the Air Force should define a specific time frame for finalizing, and ensure the issuance of guidance for certifying the department's business systems on the basis of (1) having an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable; and (2) being in compliance with DoD's auditability requirements.

DoD RESPONSE: Concur. The Department of the Air Force concurs and has complied with the recommendation. The AFMAN 63-144 details the consideration of using existing commercial solutions without modification or tailoring. This includes COTS products. In addition, the AFMAN 63-144 addresses compliance with auditability. The AFMAN 63-144 is currently in re-publishing to account for changes in DoDi 5000.75; however, can be provided to demonstrate full compliance.

Recommendation Three: The Secretary of the Navy should define a specific time frame for finalizing, and ensure the issuance of guidance for certifying the department's business systems on the basis of (1) having a viable plan to implement the system's requirements; (2) having an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable; and (3) being in compliance with DOD's auditability requirements.

DoD RESPONSE: Partially concur. Department of the Navy (DON) agrees and has a Defense Business Systems Investment Certification Manual. The manual has been revised to incorporate

2

GAO DRAFT REPORT dated December 18, 2017
GAO-18-130 (GAO CODE 101359)

the FY16 NDAA, DoD Instruction 5000.75, and the OCMO Defense Business Systems Investment Management Guidance dated April 2017. The current publication date for the revised manual is February 2018. DON disagrees with the recommendation as written and recommends GAO revise the recommendation from "the Secretary of the Navy should define a specific time frame for finalizing, and ensure the issuance of guidance for certifying the department's business systems..." to "The Secretary of the Navy should ensure guidance is issued according to established timeline for certifying the department's business systems..." This recommended change would support alignment with the timeline for certifying the department's business systems driven by the CMO investment review timeline. DON agrees with guidance being issued but not for DON to specify a "specific time frame".

Recommendation Four: The Secretary of the Army should define a specific time frame for finalizing, and ensure the issuance of guidance for certifying the department's business systems on the basis of (1) being reengineered to be as streamlined and efficient as practicable, and determining that implementation of the system will maximize the elimination of unique software requirements and unique interfaces; (2) being in compliance with the business enterprise architecture; (3) having valid, achievable requirements and a viable plan to implement the requirements; (4) having an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable; and (5) being in compliance with DOD's auditability requirements.

DoD RESPONSE: Concur. Department of the Army agrees and has developed a draft policy to strengthen the use of the business capability acquisition cycle for Defense Business System requirements and acquisition. The draft policy implements a process to record achieving statutory requirements for the acquisition and sustainment strategies, requirements documentation and auditability compliance. The draft policy provides authoritative direction for business process reengineering focusing on eliminating or reducing COTS customization and limiting incorporation of unique interfaces. The plan is to have the draft policy signed by February 28, 2018. This draft policy is the Army's implementation and execution of the DoDI 5000.75.
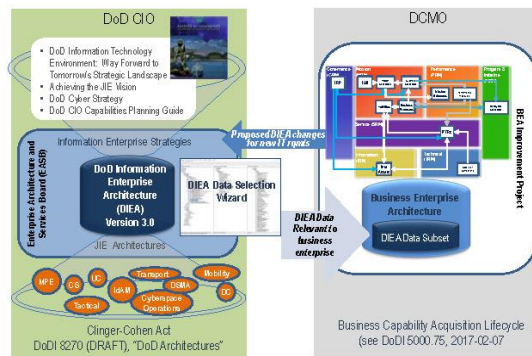
The Army's annual Portfolio Review (Organizational Execution Plan) process implements title 10 U.S.C. § 2222 and involves an approval of funds certification. This process enables the management of a well-defined IT investment portfolio for the Business Mission Area (BMA) through enforcement of the business enterprise architecture (BEA), business process reengineering (BPR), and portfolio management.

Recommendation Five: The Secretary of Defense should ensure that the DOD CIO develops an IT enterprise architecture which includes a transition plan that provides a road map for improving the department's IT and computing infrastructure, including for each of its business processes.

DoD RESPONSE: Partially concur. The DoD agrees the DoD CIO should develop a DoD Information Enterprise Architecture (DIEA) that enables improving the department's IT and

3

**GAO DRAFT REPORT dated December 18, 2017
GAO-18-130 (GAO CODE 101359)**

computing infrastructure for each of its business processes. The DoDs plan and ongoing
activities to make such improvements occur are shown in the figure below. It shows the DoD
CIO and DoD's business capability organization, CMO, have interacting processes and
architecture relationships. The processes are those associated with Clinger-Cohen Act such as
those required by DoDI 8270 (DRAFT) and the Business Capability Acquisition Lifecycle
(BCAC) described in DoDI 5000.75.

They are supported by the DoD CIO's Enterprise Architecture and Services Board (EASB) and
BEA Configuration Control Board (CCB), respectively. The EASB is the configuration
management body for architectures related to the Information Enterprise (IE) while the
configuration management for the business architectures is within the purview of the Defense
Business Council as delegated to the BEA CCB BEA Improvement Project. At the core of both
are the DoD IE Architecture (DIEA) and the Business Enterprise Architecture (BEA). As can be
seen, the DIEA incorporates strategic guidance (top-down) as well as detailed architectures for
improving the department's IT and computing infrastructure via the Joint Information
Environment (JIE) initiative (bottom-up). The BEA supports the BCAC via an ongoing BEA
improvement project by providing business reference models needed by the BCAC processes.
Because the IE supports the business enterprise, DIEA architecture data that is relevant to the
business enterprise is accessed via the DIEA Data Selection Wizard and imported into the BEA.
Subsequently, if any of the BCAC processes indicate a need to improve IT or computing
infrastructure, e.g., to achieve Performance Measures to achieve Mission Outcomes, the CMO
has a protocol to initiate a proposal to change the DIEA via their membership in the EASB.
Encoding IT and computing infrastructure improvements in the DIEA via strategic guidance,
JIE, and EASB configuration management direction and then embedding relevant DIEA
structure and data into mission area architectures such as the BEA provides a comprehensive
way to promulgate improvement architectures that is consistent and leads to interoperability and
cybersecurity within and across mission areas. This demonstrates that GAOs Recommendation 5
is not needed due to the goal already being accomplished by a set of processes, organizations,
protocols, and architecture data that is appropriate for the DoD.

4

GAO DRAFT REPORT dated December 18, 2017
GAO-18-130 (GAO CODE 101359)

Recommendation Six: The Secretary of Defense should ensure that the CIO and CMO work together to define a specific time frame for when the department plans to integrate its business and IT architectures and ensure that the architectures are integrated.

DoD RESPONSE: Partially concur. The DoD agrees the DoD CIO and CMO should work together to establish a timeframe and ensure coordination and consistency of the IT and business architectures. The DoD disagrees with the use and intent of the term "integrate" in the recommendation. The DoD proposes to change the recommendation to read "The GAO recommends the Secretary of Defense ensure the DoD CIO and CMO work together to define a specific timeline for coordinating its business and IT architectures to achieve better enterprise alignment among the architectures. Maintaining consistency dictates the IT architecture evolves with full consideration of business architecture requirements and business architectures incorporate IT architecture capabilities and services."

5

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Carol C. Harris, (202) 512-4456 or HarrisCC@gao.gov

Staff Acknowledgments

In addition to the contact above, individuals making contributions to this report include Michael Holland (Assistant Director), Cheryl Dottermusch (Analyst in Charge), John Bailey, Chris Businsky, Camille Chaires, Nancy Glover, James Houtz, Anh Le, Tyler Mountjoy, Monica Perez-Nelson, Priscilla Smith, and Adam Vodraska.

Appendix V: Accessible Data

Data Tables

Data Table for Figure 1: Department of Defense (DOD) Fiscal Year 2018 Information Technology Budget by Mission Area (projected)

DOD Mission Area	Dollars in billions	T&V
EIEMA	$16.8	JB 9/21/2017
BMA	$8.7	JB 9/21/2017
WMA	$7.5	JB 9/21/2017
DIMA	$0.1	JB 9/21/2017

Data Table for Figure 2: Department of Defense (DOD) Information Technology Business Mission Area Fiscal Year 2018 Budget, by Segment (projected)

DOD BMA Segment	Dollars in millions	T&V
logistics/supply chain management	2714	JB 9/21/2017
human resource management	2093	JB 9/21/2017
health	1751	JB 9/21/2017
financial management	1079	JB 9/21/2017
Acquisition	550	JB 9/21/2017
installation support	403	JB 9/21/2017
business services	152	JB 9/21/2017

Agency Comment Letter

Text of Appendix III: Comments from the Department of Defense

Page 1

March 2, 2018

Ms. Carol C. Harris

Director, Information Technology

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548 Dear Ms. Harris:

This is the Department of Defense response to the Government Accountability Office (GAO) draft report GAO-18-130, "DEFENSE BUSINESS SYSTEMS: DoD Needs to Continue Improving Guidance and Plans for Effectively Managing Investments" dated December 18, 2017 (GAO Code 101359). The Department concurs with three and partially concurs with three of the six recommendations.

The Department appreciates the opportunity to respond to your draft report. We look forward to your continued cooperation and dialog toward our common goal of effectively managing investments within the Department of Defense business operations. Should you have any questions, please contact Monica Prince, (571) 372-3087, monica.r.prince.civ@mail.mil.

Sincerely,

David Tillotson III

Assistant Chief Management Officer

Page 2

"DEFENSE BUSINESS SYSTEMS: DOD NEEDS TO CONTINUE IMPROVING GUIDANCE AND PLANS FOR EFFECTIVELY MANAGING INVESTMENTS"

DoD COMMENTS TO THE GAO RECOMMENDATIONS

Recommendation One:

The Secretary of Defense should define a specific time frame for finalizing, and ensure the issuance of (1) policy requiring full consideration of sustainability and technological refreshment requirements for its defense business system investments; and (2) policy requiring that best systems engineering practices are used in the procurement and deployment of commercial systems, modified commercial systems, and defense-unique systems to meet DoD mission.

DoD RESPONSE: Concur.

The Department concurs and has complied by publishing Defense Business Systems Investment Management Guidance, Version 4.0 in April 2017. The guidance identifies the DoD Financial Management Regulation Volume 2B, Chapter 18 "Information Technology" and supporting IT budget policy and guidance which addresses the requirement for sustainability and technological refreshment requirements for its defense business system investments. Also identified, is the DoD Instruction 5000.75 "Business Systems Requirements and Acquisition" and supporting acquisition policy and guidance.

Recommendation Two:

The Secretary of the Air Force should define a specific time frame for finalizing, and ensure the issuance of guidance for certifying the department's business systems on the basis of (1) having an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable; and (2) being in compliance with DoD's auditability requirements.

DoD RESPONSE: Concur.

The Department of the Air Force concurs and has complied with the recommendation. The AFMAN 63-144 details the consideration of using existing commercial solutions without modification or tailoring. This includes COTS products. In addition, the AFMAN 63-144 addresses compliance with auditability. The AFMAN 63-144 is currently in re-publishing to account for changes in DoDi 5000.75; however, can be provided to demonstrate full compliance.

Recommendation Three:

The Secretary of the Navy should define a specific time frame for finalizing, and ensure the issuance of guidance for certifying the department's business systems on the basis of (1) having a viable plan to implement the system's requirements; (2) having an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable; and (3) being in compliance with DOD's auditability requirements.

DoD RESPONSE: Partially concur.

Department of the Navy (DON) agrees and has a Defense Business Systems Investment Certification Manual. The manual has been revised to incorporate

Page 3

the FY16 NDAA, DoD Instruction 5000.75, and the OCMO Defense Business Systems Investment Management Guidance dated April 2017. The current publication date for the revised manual is February 2018. DON disagrees with the recommendation as written and recommends GAO revise the recommendation from "the Secretary of the Navy should define a specific time frame for finalizing, and ensure the issuance of guidance for certifying the department's business systems…" to "The Secretary of the Navy should ensure guidance is issued according to established timeline for certifying the department's business systems…" This recommended change would support alignment with the timeline for certifying the department's business systems driven by the CMO investment review timeline. DON agrees with guidance being issued but not for DON to specify a "specific time frame".

Recommendation Four:

The Secretary of the Army should define a specific time frame for finalizing, and ensure the issuance of guidance for certifying the department's business systems on the basis of (1) being reengineered to be as streamlined and efficient as practicable, and determining that implementation of the system will maximize the elimination of unique software requirements and unique interfaces; (2) being in compliance with the business enterprise architecture; (3) having valid, achievable requirements and a viable plan to implement the requirements; (4) having an acquisition strategy designed to eliminate or reduce the need to tailor commercial off-the-shelf systems to meet unique requirements, incorporate unique requirements, or incorporate unique interfaces to the maximum extent practicable; and (5) being in compliance with DOD's auditability requirements.

DoD RESPONSE: Concur.

Department of the Army agrees and has developed a draft policy to strengthen the use of the business capability acquisition cycle for Defense Business System requirements and acquisition. The draft policy

implements a process to record achieving statutory requirements for the acquisition and sustainment strategies, requirements documentation and auditability compliance. The draft policy provides authoritative direction for business process reengineering focusing on eliminating or reducing COTS customization and limiting incorporation of unique interfaces. The plan is to have the draft policy signed by February 28, 2018. This draft policy is the Army's implementation and execution of the DoDI 5000.75.

The Army's annual Portfolio Review (Organizational Execution Plan) process implements title 10 U.S.C. § 2222 and involves an approval of funds certification. This process enables the management of a well-defined IT investment portfolio for the Business Mission Area (BMA) through enforcement of the business enterprise architecture (BEA), business process reengineering (BPR), and portfolio management.

Recommendation Five:

The Secretary of Defense should ensure that the DOD CIO develops an IT enterprise architecture which includes a transition plan that provides a road map for improving the department's IT and computing infrastructure, including for each of its business processes.

DoD RESPONSE: Partially concur.

The DoD agrees the DoD CIO should develop a DoD Information Enterprise Architecture (DIEA) that enables improving the department's IT and

Page 4

computing infrastructure for each of its business processes. The DoDs plan and ongoing activities to make such improvements occur are shown in the figure below. It shows the DoD CIO and DoD's business capability organization, CMO, have interacting processes and architecture relationships. The processes are those associated with Clinger-Cohen Act such as those required by DoDI 8270 (DRAFT) and the Business Capability Acquisition Lifecycle (BCAC) described in DoDI 5000.75.

They are supported by the DoD CIO's Enterprise Architecture and Services Board (EASB) and BEA Configuration Control Board (CCB), respectively. The EASB is the configuration management body for architectures related to the Information Enterprise (IE) while the configuration management for the business architectures is within the

purview of the Defense Business Council as delegated to the BEA CCB BEA Improvement Project. At the core of both are the DoD IE Architecture (DIEA) and the Business Enterprise Architecture (BEA). As can be seen, the DIEA incorporates strategic guidance (top-down) as well as detailed architectures for improving the department's IT and computing infrastructure via the Joint Information Environment (JIE) initiative (bottom-up). The BEA supports the BCAC via an ongoing BEA improvement project by providing business reference models needed by the BCAC processes.

Because the IE supports the business enterprise, DIEA architecture data that is relevant to the business enterprise is accessed via the DIEA Data Selection Wizard and imported into the BEA. Subsequently, if any of the BCAC processes indicate a need to improve IT or computing infrastructure, e.g., to achieve Performance Measures to achieve Mission Outcomes, the CMO has a protocol to initiate a proposal to change the DIEA via their membership in the EASB. Encoding IT and computing infrastructure improvements in the DIEA via strategic guidance, JIE, and EASB configuration management direction and then embedding relevant DIEA structure and data into mission area architectures such as the BEA provides a comprehensive way to promulgate improvement architectures that is consistent and leads to interoperability and cybersecurity within and across mission areas. This demonstrates that GAOs Recommendation 5 is not needed due to the goal already being accomplished by a set of processes, organizations, protocols, and architecture data that is appropriate for the DoD.

Page 5

Recommendation Six:

The Secretary of Defense should ensure that the CIO and CMO work together to define a specific time frame for when the department plans to integrate its business and IT architectures and ensure that the architectures are integrated.

DoD RESPONSE: Partially concur.

The DoD agrees the DoD CIO and CMO should work together to establish a timeframe and ensure coordination and consistency of the IT and business architectures. The DoD disagrees with the use and intent of the term "integrate" in the recommendation. The DoD proposes to change the recommendation to read "The GAO recommends the Secretary of

Defense ensure the DoD CIO and CMO work together to define a specific timeline for coordinating its business and IT architectures to achieve better enterprise alignment among the architectures. Maintaining consistency dictates the IT architecture evolves with full consideration of business architecture requirements and business architectures incorporate IT architecture capabilities and services."

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 GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

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, http://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, LinkedIn, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

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

Strategic Planning and External Liaison

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