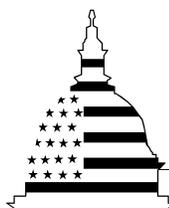


November 2005

DOD BUSINESS
SYSTEMS
MODERNIZATION

Important Progress
Made in Establishing
Foundational
Architecture Products
and Investment
Management
Practices, but Much
Work Remains



G A O

Accountability * Integrity * Reliability



Highlights of [GAO-06-219](#), a report to congressional committees

Why GAO Did This Study

For many years, the Department of Defense (DOD) has been attempting to modernize its business systems, and GAO has made numerous recommendations to help it do so. To further assist DOD, Congress included provisions in the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 aimed at ensuring that DOD develop a well-defined business enterprise architecture and transition plan by September 30, 2005, as well as establish and implement effective structures and processes for managing information technology (IT) business system investments.

In response to the act's mandate, GAO is reporting on DOD's compliance with requirements relating to DOD's architecture, transition plan, budgetary disclosure, and business system review and approval structures and processes. Given GAO's existing recommendations, it is not making additional recommendations at this time. In comments on a draft of this report, DOD recognized that GAO has been a constructive player in its business transformation efforts. While not specifically commenting on most of the report's findings and its conclusions, DOD also said that it disagreed with two points: the level of development for its "As Is" architecture and instances of nonintegration within the architecture and transition plan. However, it also commented that it is committed to addressing what GAO views to be the underlying basis of both points.

www.gao.gov/cgi-bin/getrpt?GAO-06-219.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

DOD BUSINESS SYSTEMS MODERNIZATION

Important Progress Made in Establishing Foundational Architecture Products and Investment Management Practices, but Much Work Remains

What GAO Found

In its efforts to comply with the act's provisions, DOD has made important progress in establishing needed modernization management capabilities.

However, much more remains to be done.

- The latest version of the business enterprise architecture (Version 3.0), which the department approved on September 28, 2005, partially satisfies the conditions of the act, but not entirely. For example, while Version 3.0 includes a target or "To Be" architecture, as required, it does not include a current ("As Is") architecture. Without this element, DOD could not analyze the gaps between the two architectures—critical input to a comprehensive transition plan. However, this version of the architecture represents significant progress and provides a foundation upon which the department can build.
- The transition plan associated with the current version of the architecture partially satisfies the act, but improvements are needed. Specifically, although it includes certain required information (such as milestones for major projects), it is inconsistent with the architecture in various ways. For instance, it identifies target systems (those that are to be included in the "To Be" architecture), but these are not always the same as those identified in the architecture itself. In addition, the transition plan does not include system performance metrics aligned with the plan's strategic goals and objectives.
- The department's fiscal year 2006 budget discloses some but not all required information. For example, it does not identify the approval authority for all business systems investments.
- DOD has satisfied some of the act's requirements regarding its business systems investments, but it either has not satisfied or is still in the process of satisfying others. For example, the department has fulfilled the act's requirement for delegating IT system responsibility and accountability to designated approval authorities as specified. In addition, DOD has largely satisfied the act's requirement to establish certain structures and define certain processes to review and approve IT investments. However, some of these structures are not yet in place, and some reviews and approvals to date have not followed the criteria in the act.

DOD agrees that additional work is required and states that under its incremental approach to developing the architecture and transition plan, and under its tiered accountability structure for reviewing and approving business system investments, improvements will occur in its architecture, transition plan, budgetary disclosure, and investment management and oversight. If these improvements do not occur, DOD's business systems modernization will continue to be a high-risk program.

Contents

Letter

Results in Brief	1
Background	2
DOD Has Satisfied Requirements in Its Fiscal Year Authorization Act to Varying Degrees	5
Conclusions	16
Agency Comments and Our Evaluation	50

Appendixes

Appendix I: Objective, Scope, and Methodology	55
Appendix II: Comments from the Department of Defense	59
Appendix III: Summary of Several Architecture Frameworks	61
Appendix IV: List of the DOD Architecture Framework Products	65
Appendix V: GAO Contact and Staff Acknowledgments	67

Tables

Table 1: Compliance with Act's Provisions	3
Table 2: Roles and Responsibilities of Governance Entities	11
Table 3: Core Business Missions and Associated Principal Staff Assistants	13
Table 4: Descriptions of Business Enterprise Priorities	19
Table 5: DOD Architecture Framework Products Included in Version 3.0	20
Table 6: Systems Receiving DBSMC Approval under Prior Criteria	49

Figure

Figure 1: Interdependent DODAF Views of an Architecture	62
---	----

Abbreviations

ASD(NII)/CIO	Assistant Secretary of Defense (Networks and Information Integration)/Chief Information Officer
AV	all view
BEIS	Business Enterprise Information Services
BTA	Business Transformation Agency
CIO	Chief Information Officer
DBSMC	Defense Business Systems Management Committee
DCAS	Defense Cash Accountability System
DIMHRS	Defense Integrated Military Human Resources System
DITPR	DOD Information Technology Portfolio Data Repository
DOD	Department of Defense
DODAF	Department of Defense Architecture Framework
ECSS	Expeditionary Combat Support System
FEA	Federal Enterprise Architecture
FEAF	Federal Enterprise Architecture Framework
FMSE	Financial Management System Entity
IT	information technology
JFMIP	Joint Financial Management Improvement Program
MOCAS	Mechanization of Contract Administration Services
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OV	operational view
SACS	Standard Accounting Classification Structure
SFIS	Standard Financial Information Structure
SV	systems view
TV	technical standards view

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



November 23, 2005

Congressional Committees

For decades, the Department of Defense (DOD) has not been successful in repeated attempts to modernize its timeworn business systems¹ and operations. In 2001, the Secretary of Defense launched the latest attempt as part of a broad initiative to “transform the way the department works and what it works on.” The Secretary has estimated that successful improvements to DOD business systems and operations could save the department 5 percent of its budget a year—potentially more than \$20 billion a year in savings.

In 1995, we first designated DOD’s business systems modernization as high risk, and it remains so today.² In May 2001, to help DOD transform its operations, we made eight recommendations to the Secretary of Defense that were aimed at providing the means for effectively developing and implementing an enterprise architecture³ and limiting systems investments by DOD components⁴ until the department had a well-defined architecture and the means to enforce it.⁵ We also recommended that DOD establish a corporate approach to investment control and decision making. In July 2001, the department initiated a business management modernization program with the aim, among others, of developing a business enterprise

¹Business systems include financial and nonfinancial systems, such as civilian personnel, finance, health, logistics, military personnel, procurement, and transportation, with the common element being the generation or use of financial data to support DOD’s business operations. See 10 U.S.C. § 2222 (j) (2).

²GAO, *High-Risk Series: An Update*, [GAO-05-207](#) (Washington, D.C.: January 2005).

³An enterprise architecture, or modernization blueprint, provides a clear and comprehensive picture of an entity, whether it is an organization (e.g., federal department or agency) or a functional or mission area that cuts across more than one organization (e.g., financial management). This picture consists of snapshots of both the enterprise’s current “As Is” operational and technological environment and its target or “To Be” environment, as well as a capital investment roadmap for transitioning from the current to the target environment. These snapshots further consist of “views,” which are basically one or more architecture products that provide conceptual or logical representations of the enterprise.

⁴DOD components include the military services, defense agencies, and DOD field activities.

⁵GAO, *Information Technology: Architecture Needed to Guide Modernization of DOD’s Financial Operations*, [GAO-01-525](#) (Washington, D.C.: May 17, 2001).

architecture and establishing the investment controls needed to effectively implement this architecture.

In response to DOD's challenges on its modernization efforts, Congress included provisions in the defense authorization act for fiscal year 2005⁶ that were aimed at ensuring DOD's development of a well-defined business enterprise architecture and associated enterprise transition plan by September 30, 2005, as well as establishment and implementation of effective information technology (IT) business system investment management structures and processes by various dates. More specifically, the act required the department to, among other things, (1) develop a business enterprise architecture, (2) develop a transition plan to implement the architecture, (3) establish a system investment approval and accountability structure, (4) establish an investment review process, (5) approve and certify system modernizations in excess of \$1 million, and (6) include systems information in its annual budget submission. The act also directed us to submit to congressional defense committees—within 60 days of the Secretary of Defense's approval of the department's enterprise architecture and its transition plan—an assessment of DOD's actions taken to comply with these requirements.

As agreed with your offices, our overall objective was to assess DOD's efforts to comply with the act's requirements. We performed our work from August through November 2005, in accordance with U.S. generally accepted government auditing standards. Details on our objective, scope, and methodology are contained in appendix I.

Results in Brief

DOD has either complied, partially complied, or is in the process of complying with six requirements—related to strengthening its institutional approach to managing its business systems modernization efforts—that are specified in the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005. Our assessment of DOD's degree of compliance with each is summarized in table 1.

⁶Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Pub. L. No. 108-375, § 332, 118 Stat. 1811, 1851-1856 (Oct. 28, 2004) (codified in part at 10 U.S.C. § 2222).

Table 1: Compliance with Act's Provisions

Summary of provision	Satisfaction ^a		
	Yes	Partial	In process
By September 30, 2005, the department must develop a business enterprise architecture that meets certain requirements.		x	
By September 30, 2005, the department must develop a transition plan for implementing the architecture that meets certain requirements.		x	
The department must identify each business system proposed for funding in its budget submission for fiscal year 2006 and subsequent fiscal years and identify funds for current services and for business systems modernization.		x	
The department must delegate the responsibility for business systems to designated approval authorities within the Office of the Secretary of Defense.	x		
By March 15, 2005, the department must require each approval authority to establish an investment review process.		x	
Effective October 1, 2005, the department may not obligate funds for a business system modernization with a cost exceeding \$1 million unless it is certified by the approval authority and the certification is approved by the Defense Business Systems Management Committee as meeting specific requirements.			x

Source: GAO.

^a“Yes” means that the department has satisfied the act’s requirements. “Partial” means that the department has satisfied some, but not all, aspects of the act’s requirements. “In process” means that the department is taking steps to satisfy the act’s requirements.

The department’s efforts to comply with the act represent important progress, but further steps are needed, particularly with regard to adding needed content and scope to the architecture and transition plan and ensuring that corporate investment management structures and processes are effectively implemented and full budgetary disclosure occurs. According to DOD, these additional steps will be taken as part of its incremental approach to developing the architecture and plan, and through the accountability framework that it has established for managing business system investments. Because our prior recommendations to the department already provide a roadmap for ensuring that these steps occur, we are not making additional recommendations at this time.

In its written comments on a draft of this report, signed by the Deputy Under Secretary of Defense (Business Transformation) and reprinted in

appendix II, the department recognized that our analysis, recommendations, guidance, and educational activities have made us a constructive player in DOD's business transformation efforts. The department also commented that it disagreed with two of our points.

First, DOD commented that development of a "comprehensive 'As Is' architecture" would not be an effective use of time and resources and that the results of its examination of its "As Is" conditions are not required to be in the enterprise architecture. Notwithstanding these comments, DOD added that it understood that there needs to be an "easily traceable direct link" between the results of examining its "As Is" conditions and the "To Be" solutions, and that it was committed to documenting the "As Is" and "To Be" relationship in an appropriate manner. DOD's comments are largely consistent with our findings and prior recommendations. Specifically, we agree that DOD needs to document its "As Is" architecture, as we have previously recommended. Moreover, our prior recommendations have neither presumed nor prescribed a "comprehensiveness" standard in doing so, as we recognize that overdevelopment of an architecture would not be a cost-effective use of resources. Rather, our prior recommendations have focused on developing "As Is" architectural products in a manner that is consistent with widely accepted best practice and federal guidance.

Second, DOD stated that most of our examples demonstrating a lack of integration within and between the business enterprise architecture and the transition plan are due to misunderstandings, and that it is committed to correcting them. We understand DOD's point, but would add that in cases where these examples (some explicit and others implicit) arise from lack of clarity in the architecture and transition plan, they would be more appropriately described as miscommunications. Moreover, we would emphasize that such miscommunications are directly attributable to ambiguity and inconsistencies in the architecture products and the transition plan that blur their intended meaning, which can lead to misunderstanding by both internal and external stakeholders. Given that a well-defined architecture is, among other things, clear and internally aligned, such ambiguity and inconsistency limit the utility and effectiveness of the products as reference tools for guiding and constraining system investment decisions. Accordingly, we agree with DOD's comment that addressing these limitations will create better transformation tools that will benefit all stakeholders, most importantly those within the department.

Background

DOD is a massive and complex organization. In fiscal year 2004, the department reported that its operations involved \$1.2 trillion in assets, \$1.7 trillion in liabilities, over 3.3 million military and civilian personnel, and over \$605 billion in net cost of operations. For fiscal year 2005, the department received appropriations of about \$417 billion. The department comprises a wide range of organizations, including the military services and their respective major commands and functional activities, numerous defense agencies and field activities, and various combatant and joint operational commands, which are responsible for military operations for specific geographic regions or theaters of operations.

In support of its military operations, the department performs an assortment of interrelated and interdependent business functions, including logistics management, procurement, health care management, and financial management. Earlier this year, DOD reported that, in order to support these business functions, it relied on about 4,200 business systems, for which the department received approximately \$13.3 billion in fiscal year 2005 for operations, maintenance, and modernization. For fiscal year 2006, DOD received approximately \$15.5 billion to operate, maintain, and modernize its business systems. As we have previously reported,⁷ DOD's systems environment is overly complex and error prone and is characterized by (1) little standardization across the department, (2) multiple systems performing the same tasks, (3) the same data stored in multiple systems, and (4) the need for manual data entry into multiple systems. In addition, our reports⁸ continue to show that the department's nonintegrated and duplicative systems contribute to fraud, waste, and abuse. Of the 25 areas on GAO's governmentwide high-risk list, 8 are DOD

⁷GAO, *DOD Business Systems Modernization: Long-standing Weaknesses in Enterprise Architecture Development Need to Be Addressed*, [GAO-05-702](#) (Washington, D.C.: July 22, 2005).

⁸See, for example, GAO, *Defense Inventory: Opportunities Exist to Improve Spare Parts Support Aboard Deployed Navy Ships*, [GAO-03-887](#) (Washington, D.C.: Aug. 29, 2003); *Military Pay: Army National Guard Personnel Mobilized to Active Duty Experienced Significant Pay Problems*, [GAO-04-89](#) (Washington, D.C.: Nov. 13, 2003); and *DOD Travel Cards: Control Weaknesses Resulted in Millions of Dollars of Improper Payments*, [GAO-04-576](#) (Washington, D.C.: June 9, 2004).

program areas, and the department shares responsibility for 6 other governmentwide high-risk areas.⁹ DOD's business systems modernization is one of the high-risk areas.

Enterprise Architecture and Information Technology Investment Management Are Critical to Achieving Successful Systems Modernization

Effective use of an enterprise architecture, or a modernization blueprint, is a hallmark of successful public and private organizations. For more than a decade, we have promoted the use of architectures to guide and constrain systems modernization, recognizing them as a crucial means to a challenging goal: agency operational structures that are optimally defined in both the business and technological environments. Congress, the Office of Management and Budget (OMB), and the federal Chief Information Officer (CIO) Council have also recognized the importance of an architecture-centric approach to modernization, and OMB and the CIO Council, in collaboration with us, have issued enterprise architecture guidance.¹⁰ The Clinger-Cohen Act of 1996¹¹ mandates that an agency's CIO develop, maintain, and facilitate the implementation of an IT architecture. Further, the E-Government Act of 2002¹² requires OMB to oversee the development of enterprise architectures within and across agencies. In addition, we and OMB have issued guidance that, among other things, emphasizes the need for system investments to be consistent with these architectures.¹³

A corporate approach to IT investment management is also characteristic of successful public and private organizations. Recognizing this, Congress

⁹GAO-05-207. The 8 specific DOD high-risk areas are (1) approach to business transformation, (2) business systems modernization, (3) contract management, (4) financial management, (5) personnel security clearance program, (6) supply chain management, (7) support infrastructure management, and (8) weapon systems acquisition. The 6 governmentwide high-risk areas are (1) disability programs, (2) interagency contracting, (3) information systems and critical infrastructure, (4) information sharing for homeland security, (5) human capital, and (6) real property.

¹⁰CIO Council, *A Practical Guide to Federal Enterprise Architecture, Version 1.0* (February 2001).

¹¹The Clinger-Cohen Act of 1996, 40 U.S.C. § 11312 and 11315(b)(2).

¹²The E-Government Act of 2002, Public Law 107-347 (Dec. 17, 2002).

¹³This guidance is provided in the Office of Management and Budget (OMB) Capital Programming Guide, Version 1.0 (July 1997) and GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G (Washington, D.C.: March 2004).

developed and enacted the Clinger-Cohen Act in 1996,¹⁴ which requires OMB to establish processes to analyze, track, and evaluate the risks and results of major capital investments in information systems made by executive agencies.¹⁵ In response to the Clinger-Cohen Act and other statutes, OMB developed policy for planning, budgeting, acquisition, and management of federal capital assets and issued guidance.¹⁶ We have also issued guidance in this area,¹⁷ which defines institutional structures, such as investment review boards, and associated processes, such as common investment criteria.

Enterprise Architecture: A Brief Description

An enterprise architecture provides a clear and comprehensive picture of an entity, whether it is an organization (e.g., a federal department) or a functional or mission area that cuts across more than one organization (e.g., financial management). This picture consists of snapshots of both the enterprise's current or "As Is" environment and its target or "To Be" environment. These snapshots consist of "views," which are one or more architecture products (e.g., models, diagrams, matrixes, and text) that provide logical or technical representations of the enterprise. The architecture also includes a transition or sequencing plan, which is based on an analysis of the gaps between the "As Is" and "To Be" environments; this plan provides a temporal roadmap for moving between the two environments that incorporates such considerations as technology opportunities, marketplace trends, fiscal and budgetary constraints, institutional system development and acquisition capabilities, new and legacy system dependencies and life expectancies, and the projected value of competing investments.

¹⁴The Clinger-Cohen Act of 1996, 40 U.S.C. sections 11101-11704. This act expanded the responsibilities of OMB and the agencies that had been set under the Paperwork Reduction Act with regard to information technology management. See 44 U.S.C. 3504(a)(1)(B)(vi) (OMB); 44 U.S.C. 3506(h)(5) (agencies).

¹⁵We have made recommendations to improve OMB's process for monitoring high-risk IT investments; see GAO, *Information Technology: OMB Can Make More Effective Use of Its Investment Reviews*, [GAO-05-276](#) (Washington, D.C.: Apr. 15, 2005).

¹⁶This policy is set forth and guidance is provided in OMB Circular No. A-11 (Nov. 2, 2005) (section 300) and in OMB's Capital Programming Guide, which directs agencies to develop, implement, and use a capital programming process to build their capital asset portfolios.

¹⁷GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, [GAO-04-394G](#) (Washington, D.C.: March 2004).

The suite of products produced for a given entity's enterprise architecture, including their structure and content, are largely governed by the framework used to develop the architecture. Since the 1980s, various architecture frameworks have emerged and been applied. Appendix III provides a discussion of these various frameworks.

The importance of developing, implementing, and maintaining an enterprise architecture is a basic tenet of both organizational transformation and systems modernization. Managed properly, an enterprise architecture can clarify and help to optimize the interdependencies and relationships among an organization's business operations and the underlying IT infrastructure and applications that support these operations. To support effective architecture management in the federal government, we have issued architecture management guidance, as has the federal CIO Council and OMB.¹⁸ This guidance recognizes that when an enterprise architecture is employed in concert with other important management controls, such as portfolio-based capital planning and investment control practices, architectures can greatly increase the chances that an organization's operational and IT environments will be configured to optimize its mission performance. Our experience with federal agencies has shown that investing in IT without defining these investments in the context of an architecture often results in systems that are duplicative, not well integrated, and unnecessarily costly to maintain and interface.¹⁹

¹⁸GAO, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1)*, [GAO-03-584G](#) (Washington, D.C.: April 2003); and CIO Council, *A Practical Guide to Federal Enterprise Architecture, Version 1.0* (February 2001).

¹⁹See, for example, GAO, *Homeland Security: Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains*, [GAO-04-777](#) (Washington, D.C.: Aug. 6, 2004); *DOD Business Systems Modernization: Limited Progress in Development of Business Enterprise Architecture and Oversight of Information Technology Investments*, [GAO-04-731R](#) (Washington, D.C.: May 17, 2004); *Information Technology: Architecture Needed to Guide NASA's Financial Management Modernization*, [GAO-04-43](#) (Washington, D.C.: Nov. 21, 2003); *DOD Business Systems Modernization: Important Progress Made to Develop Business Enterprise Architecture, but Much Work Remains*, [GAO-03-1018](#) (Washington, D.C.: Sept. 19, 2003); *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: DLA Should Strengthen Business Systems Modernization Architecture and Investment Activities*, [GAO-01-631](#) (Washington, D.C.: June 29, 2001); and *Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture*, [GAO/AIMD-00-212](#) (Washington, D.C.: Aug. 1, 2000).

IT Investment Management: A Brief Description

IT investment management is a process for linking IT investment decisions to an organization's strategic objectives and business plans. Generally, it includes structures (including decision-making bodies known as Investment Review Boards), processes for developing information on investments (such as costs and benefits), and practices to inform management decisions (such as whether a given investment is aligned with an enterprise architecture). The federal approach to IT investment management is based on establishing systematic processes for selecting, controlling, and evaluating investments that provides a systematic way for agencies to minimize risks while maximizing the returns of investments.²⁰

- During the selection phase, the organization (1) identifies and analyzes each project's risks and returns before committing significant funds to any project and (2) selects those IT projects that will best support its mission needs.
- During the control phase, the organization ensures that, as projects develop and investment expenditures continue, the project is continuing to meet mission needs at the expected levels of cost and risk. If the project is not meeting expectations or if problems have arisen, steps are quickly taken to address the deficiencies.
- During the evaluation phase, actual versus expected results are compared once a project has been fully implemented. This is done to (1) assess the project's impact on mission performance, (2) identify any changes or modifications to the project that may be needed, and (3) revise the investment management process based on lessons learned.

Consistent with our architecture management framework,²¹ our investment management framework²² recognizes the importance of an enterprise

²⁰GAO, *Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology*, [GAO/AIMD-94-115](#) (Washington, D.C.: May 1994); Office of Management and Budget, *Evaluating Information Technology Investments, A Practical Guide* (Washington, D.C.: November 1995); GAO, *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making*, [GAO/AIMD-10.1.13](#) (Washington, D.C.: February 1997); and [GAO-04-394G](#).

²¹[GAO-03-584G](#).

²²[GAO-04-394G](#).

architecture as a critical frame of reference for organizations making IT investment decisions, stating that only investments that move the organization toward its target architecture, as defined by its sequencing plan, should be approved, unless a waiver is provided or a decision is made to modify the architecture. Moreover, this framework states that an organization's policies and procedures should describe the relationship between its architecture and its investment decision-making authority.

Our experience has shown that mature and effective management of IT investments can vastly improve government performance and accountability, and can help to avoid wasteful IT spending and lost opportunities for improving delivery of services to the public.

DOD's Business Systems Modernization Program History and Structure

The Business Management Modernization Program was established in July 2001 in order to improve the efficiency and effectiveness of DOD's business operations through, among other things, the development and implementation of an architecture. When the program was initially established, the Secretary assigned oversight responsibility to the Under Secretary of Defense (Comptroller), in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Assistant Secretary of Defense (Networks and Information Integration)/Chief Information Officer.

In 2001, the Comptroller established several governance bodies and assigned them responsibilities associated with developing, maintaining, and implementing the architecture. Specifically, the Comptroller established (1) the Executive and Steering Committees—which were made up of senior leaders from across the department—to provide program guidance; (2) a program office to execute daily program activities necessary to develop, maintain, and implement the architecture; and (3) domain owners,²³ who were responsible for achieving business transformation, implementing the architecture, developing and executing the transition plan, and performing portfolio management. In 2003, the Comptroller also established the Domain Owners Integration Team, which comprised various senior executives from each domain and the director of the program office. This team reported to the steering committee and was

²³There were five business area domains: (1) acquisition, (2) financial management, (3) human resources management, (4) installations and environment, and (5) logistics. There was also one mission area domain—enterprise information environment.

responsible for facilitating communication and coordination across the domains for program activities, including extending and evolving the architecture.

In 2005, the department revised the program’s governance structure. Program direction and oversight is now provided by the Deputy Secretary through the dual leadership of the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Under Secretary of Defense (Comptroller). In addition, DOD has reassigned responsibility for providing executive leadership for the direction, oversight, and execution of its business transformation and systems modernization efforts to several entities. These entities include the Defense Business Systems Management Committee (DBSMC), which serves as the highest ranking governance body for business systems modernization activities; the Principal Staff Assistants, who serve as the certification authorities for business system investments in their respective core business missions; and the Investment Review Boards, which form the review and decision-making bodies for business system investments in their respective areas of responsibility. Table 2 lists these entities and their roles and responsibilities.

Table 2: Roles and Responsibilities of Governance Entities

Entity	Roles and responsibilities	Membership
Defense Business Systems Management Committee (DBSMC)	<ul style="list-style-type: none"> • Provides strategic direction and plans for the business mission area, in coordination with the warfighting and enterprise information environment mission areas. • Approves business mission area transformation plans and coordinates transition planning in a documented program baseline with critical success factors, milestones, metrics, deliverables, and periodic program reviews. • Establishes key metrics and targets by which to track business transformation progress. • Establishes policies and approves the business mission area strategic plan, the transition plan for implementation for business systems modernization, the transformation program baseline, and the business enterprise architecture. • Executes a comprehensive communications strategy. 	<p>Chaired by the Deputy Secretary of Defense; Vice Chair is the Under Secretary of Defense for Acquisition, Technology, and Logistics.</p> <p>Includes senior leadership in the Office of the Secretary of Defense, the military services’ secretaries, and defense agencies’ heads, such as the Assistant Secretary of Defense (Networks and Information Integration)/Chief Information Officer (ASD(NII)/CIO), the Vice Chairman of the Joint Chiefs of Staff, and the Commanders of the U.S. Transportation Command and Joint Forces Command.</p>

(Continued From Previous Page)

Entity	Roles and responsibilities	Membership
Principal Staff Assistants	<ul style="list-style-type: none"> • Support the DBSMC's management of enterprise business information technology investments. • Serve as the certification authorities accountable for obligation of funds for respective business system investments within designated core business missions.^a • Provide the DBSMC with recommendations for system investment approval. 	Officials who report directly to the Secretary or Deputy Secretary of Defense. These include the Under Secretaries of Defense; the Assistant Secretaries of Defense; the General Counsel of the Department of Defense; the Assistants to the Secretary of Defense; and the Directors of the Office of the Secretary of Defense.
Investment Review Boards	<ul style="list-style-type: none"> • Serve as the oversight and investment decision-making bodies for those business capabilities that support activities under their designated areas of responsibility. • Assess investments relative to their impact on end-to-end business process improvements supporting warfighter needs. • Certify that all business systems investments over \$1 million are integrated and compliant with the business enterprise architecture. 	Include the Deputy Secretary of Defense; the Under Secretary of Defense (Comptroller); Under Secretary of Defense for Acquisition, Technology, and Logistics; Assistant Secretary of Defense (Personnel and Readiness); ASD(NII)/CIO; military services; defense agencies; and combatant commands.

Source: DOD.

^aThe five core business missions are described in table 3.

DOD has defined five departmentwide core business missions to be addressed through identification of corporate business needs and analysis of capability gaps. The core business missions transcend DOD's various functional areas (e.g., planning, budgeting, information technology, procurement, and maintenance) and are intended to be the means through which end-to-end warfighter support is delivered. Responsibility for the core business missions is assigned to specific Principal Staff Assistants. Table 3 provides descriptions of the core business missions and associated responsible parties.

Table 3: Core Business Missions and Associated Principal Staff Assistants

DOD core business mission	Description	Principal Staff Assistants
Human Resources Management	This mission includes all human resources–related processes necessary to recruit, train, and prepare personnel for warfighter organizations. It also includes providing trained, healthy, and ready personnel to combatant and combat support organizations and ensuring timely and accurate access to compensation and benefits for all DOD personnel.	Under Secretary of Defense (Personnel and Readiness)
Weapon System Lifecycle Management	This mission includes full life-cycle management of Defense acquisition of weapons systems and automated information systems, including requirements, technology, development, production, and sustainment.	Under Secretary of Defense for Acquisition, Technology, and Logistics
Materiel Supply and Service Management	This mission includes the management of supply chains of materiel supply and services to maintain the readiness of nondeployed and deployed warfighters to support operations. It also includes all aspects associated with acquiring, storing, and transporting all classes of supplies.	Under Secretary of Defense for Acquisition, Technology, and Logistics
Real Property and Installations Lifecycle Management	This mission includes the provision of installations and facilities to house military forces, to store and maintain military equipment, and to serve as training and deployment platforms for dispatch of warfighter units.	Under Secretary of Defense for Acquisition, Technology, and Logistics
Financial Management	This mission includes the provision of accurate and reliable financial information in support of the planning, programming, budgeting, and execution process to ensure adequate financial resources for warfighting mission requirements. It also includes providing information to reliably cost the conduct, output, and performance of DOD operations and missions and the programs to support them.	Under Secretary of Defense (Comptroller)

Source: DOD.

On October 7, 2005, DOD established the Business Transformation Agency (BTA) to advance DOD-wide business transformation efforts, particularly with regard to business systems modernization. The BTA reports directly to the vice chair of the DBMSC.²⁴ Among other things, the BTA includes a Defense Business Systems Acquisition Executive who is to be responsible for centrally managing 28 DOD-wide business projects, programs, systems, and initiatives.²⁵ In addition, the BTA is to be responsible for integrating

²⁴The vice chair of the DBMSC is the Under Secretary of Defense for Acquisition, Technology, and Logistics.

²⁵Examples of some of these DOD-wide programs, systems, and initiatives include the Defense Travel System, the Standard Procurement System, the Defense Integrated Military Human Resources System, and the Standard Financial Information Structure.

and supporting the work of the Office of the Secretary of Defense Principal Staff Assistants, who include the approval authorities that chair the business system investment review boards. Until a permanent director is named, the Deputy Under Secretary of Defense for Business Transformation and the Deputy Under Secretary of Defense for Financial Management will jointly function as directors and will report to the vice chair of the DBSMC.

According to a program official, the department has spent approximately \$440 million on the Business Management Modernization Program since it was established in 2001.

Recent Reviews Have Assessed DOD's Efforts to Develop, Maintain, and Implement an Architecture

Since 2001, we have regularly reported on DOD's efforts to develop an architecture and to establish and implement effective investment management structures and processes.²⁶ Our reports have continued to identify problems and raise concerns about the department's architecture program, the quality of the architecture and the transition plan, and the lack of an investment management structure and controls to implement the architecture. Our most recent reports, which were issued in the third and fourth quarters of fiscal year 2005, made the following points:²⁷

²⁶GAO-01-525; *DOD Business Systems Modernization: Improvements to Enterprise Architecture Development and Implementation Efforts Needed*, GAO-03-458 (Washington, D.C.: Feb. 28, 2003); *Information Technology: Observations on Department of Defense's Draft Enterprise Architecture*, GAO-03-571R (Washington, D.C.: Mar. 28, 2003); GAO-03-877R; *DOD Business Systems Modernization: Important Progress Made to Develop Business Enterprise Architecture, but Much Work Remains*, GAO-03-1018 (Washington, D.C.: Sept. 19, 2003); *DOD Business Systems Modernization: Limited Progress in Development of Business Enterprise Architecture and Oversight of Information Technology Investments*, GAO-04-731R (Washington, D.C.: May 17, 2004).

²⁷GAO, *DOD Business Systems Modernization: Billions Being Invested without Adequate Oversight*, GAO-05-381 (Washington, D.C.: Apr. 29, 2005); and GAO-05-702.

-
- DOD had not established effective structures and processes for managing the development of its architecture. For example, the department had yet to finalize, approve, and effectively implement its plan, procedures, and charter governing the configuration management process.²⁸ In addition, DOD had yet to establish an independent quality assurance function that addressed process standards and program performance.
 - DOD had not developed a well-defined architecture. The products that it had produced did not provide sufficient content and utility to effectively guide and constrain ongoing and planned systems investments. For example, the latest versions of the architecture did not include products describing the “As Is” business and technology environments. Further, although these versions included products describing the “To Be” environment, the descriptions were inadequate because the descriptions (1) did not have a clearly defined purpose that linked to the goals and objectives of the architecture; (2) were missing important content, such as the actual systems to be developed or acquired to support future business operations and the physical infrastructure needed to support the business systems; and (3) contained products that were neither consistent nor integrated. In short, the “To Be” environment lacked the detail needed to provide DOD with a common vision for defining the transition plan and informing investment decision making.
 - DOD had not developed a plan for transitioning from the “As Is” to the “To Be” architectural environments. The transition plan is based on an analysis of the gaps between these two environments and serves as an enterprisewide IT capital investment plan and acquisition strategy.

²⁸According to relevant guidance, an effective configuration management process consists of four primary elements: (1) configuration identification, which includes procedures for identifying, documenting, and assigning unique identifiers (e.g., serial number and name) to product types generated for the architecture program, generally referred to as configuration items; (2) configuration control, which includes procedures for evaluating and deciding whether to approve changes to a product’s baseline configuration, generally accomplished through configuration control boards, which evaluate proposed changes on the basis of costs, benefits, and risks and decide whether to permit a change; (3) configuration status accounting, which includes procedures for documenting and reporting on the status of configuration items as a product evolves; and (4) configuration auditing, which includes procedures for determining alignment between the actual product and the documentation describing it, thereby ensuring that the documentation used to support the configuration control board’s decision making is complete and correct. Each of these elements should be described in a configuration management plan and implemented according to the plan.

-
- DOD did not have an effective departmentwide management structure for controlling its business investments. Although the department had established organizations to oversee its business system investments, these organizations were unable to do so, because the components controlled budget authority and continued to make their own parochial investment decisions.
 - DOD had not established common investment criteria for system reviews, and as a result different organizations were using different criteria. DOD also had not conducted a comprehensive review of its ongoing business system investments.
 - DOD had not included all of the reported systems in its fiscal year 2005 IT budget request. It lacked accurate information on the costs and number of its business systems.
 - The Under Secretary of Defense (Comptroller) had not certified all systems investments with reported obligations exceeding \$1 million, as required by the fiscal year 2003 National Defense Authorization Act.²⁹ Obligations totaling about \$243 million were made for systems modernizations in fiscal year 2004 that were not referred to the DOD Comptroller for the required review.

DOD Has Satisfied Requirements in Its Fiscal Year Authorization Act to Varying Degrees

Section 2222 of Title 10, United States Code, as added by section 332 of the defense authorization act for fiscal year 2005, cites six requirements that DOD is required to meet.³⁰ Generally, these are as follows:

1. By September 30, 2005, develop a business enterprise architecture that meets certain requirements.
2. By September 30, 2005, develop a transition plan for implementing the architecture that meets certain requirements.

²⁹Bob Stump National Defense Authorization Act for Fiscal Year 2003, Pub. L. No. 107-314, § 1004, 116 Stat. 2458, 2629-2631 (Dec. 2, 2002).

³⁰Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Pub. L. No. 108-375, § 332, 118 Stat. 1811, 1851-1856 (Oct. 28, 2004) (codified in part at 10 U.S.C. § 2222).

-
3. Identify each business system proposed for funding in DOD's fiscal year 2006 and subsequent budget submissions and identify funds for current services and business systems modernization.
 4. Delegate the responsibility for business systems to designated approval authorities within the Office of the Secretary of Defense.
 5. By March 15, 2005, require each approval authority to establish a business system investment review process.³¹
 6. Effective October 1, 2005, obligate funds for business system modernizations with a total cost exceeding \$1 million only after the system is certified by the designated approval authority and the certification is approved by the DBSMC.

DOD has partially satisfied the four legislative provisions relating to architecture development, transition plan development, budgetary disclosure, and investment review; it has satisfied the provision concerning designated approval authorities; and it is in the process of satisfying the provision for systems costing in excess of \$1 million. According to DOD, the requirements of each provision will be fully implemented under its incremental approach to developing the architecture and transition plan, and its tiered accountability approach to business system investment management. Until they are, the department's business systems modernization program will continue to be a high-risk endeavor.

Latest Version of Enterprise Architecture Partially Satisfies Act and Provides a Foundation upon Which to Add Missing Scope and Content

The defense authorization act for fiscal year 2005 requires DOD to develop a business enterprise architecture by September 30, 2005. According to the act, the architecture must satisfy three major requirements:³²

1. It must include an information infrastructure that, at a minimum, would enable DOD to

³¹This process must be consistent with section 11312 of Title 40, United States Code, which is the Capital Planning and Investment Control section of the Clinger-Cohen Act.

³²Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Pub. L. No. 108-375, § 332, 118 Stat. 1811, 1851-1856 (Oct. 28, 2004) (codified in part at 10 U.S.C. § 2222).

-
- comply with all federal accounting, financial management, and reporting requirements;
 - routinely produce timely, accurate, and reliable financial information for management purposes;
 - integrate budget, accounting, and program information and systems; and
 - provide for the systematic measurement of performance, including the ability to produce timely, relevant, and reliable cost information.
2. The architecture must include policies, procedures, data standards, and system interface requirements that are to be applied uniformly throughout the department.
 3. The architecture must be consistent with OMB policies and procedures.

On September 28, 2005, the Acting Deputy Secretary of Defense approved Version 3.0 of the business enterprise architecture. According to DOD, this version is intended to provide a blueprint to help ensure near-term delivery of the right capabilities, resources, and materiel to the warfighter. To do so, this version focused on six business enterprise priorities, which DOD states are short-term objectives to achieve immediate results. These priorities are Personnel Visibility, Acquisition Visibility, Common Supplier Engagement, Materiel Visibility, Real Property Accountability, and Financial Visibility. According to DOD, these priorities will evolve and expand in future versions of the architecture. Table 4 provides a brief description of each of the six business enterprise priorities.

Table 4: Descriptions of Business Enterprise Priorities

Business enterprise priority	Description of priority and expected benefits of achieving it
Personnel Visibility	<p>Providing access to reliable, timely, and accurate personnel information for warfighter mission planning.</p> <p>Benefits include accurate and timely access to compensation, decreased operation costs, reduced cycle times, and better management of DOD human resources in a combined (military, civilian, and contract support) environment.</p>
Acquisition Visibility	<p>Providing transparency and access to acquisition information that is critical to supporting life-cycle management of the department's processes for delivering weapon systems and automated information systems.</p> <p>Benefits include cost savings in consumables, manpower, and infrastructure; ability to share information that is accurate, relevant, and consistent; and reduced acquisition and management oversight workloads at all levels.</p>
Common Supplier Engagement	<p>Aligning and integrating policies, processes, data, technology, and people to simplify and standardize the methods that DOD uses to interact with commercial and government suppliers.</p> <p>Benefits include reliable and accurate delivery of acceptable goods and services to the warfighter, reduced backlogs, and the elimination of redundant program-specific reporting systems.</p>
Materiel Visibility	<p>Improving supply chain performance.</p> <p>Benefits include timely and accurate information on the location, movement, status, and identification of materiel and supplies for the warfighter.</p>
Real Property Accountability	<p>Acquiring access to real-time information on DOD real property assets.</p> <p>Benefits include increased access to more reliable, accurate real property information and decreased operational costs.</p>
Financial Visibility	<p>Providing immediate access to accurate and reliable financial information that will enhance efficient and effective decision making.</p> <p>Benefits include standardized financial data and reporting processes that enable decision makers to reliably evaluate program options and resource constraints.</p>

Source: DOD.

In addition to focusing the scope of Version 3.0 of the architecture on these priorities, the extent to which each priority was to be addressed, according to DOD, was limited to answering four key questions:

- Who are our people, what are their skills, and where are they located?
- Who are our industry partners, and what is the state of our relationship with them?

- What assets are we providing to support the warfighter, and where are these assets deployed?
- How are we investing our funds to best enable the warfighting mission?

To produce a version of the architecture according to the above scope, DOD created 12 of the 26 recommended products identified in the DOD Architecture Framework (DODAF)—the structural guide that the department has established for developing an architecture³³—including 7 products that the DODAF designates as essential. Table 5 shows the DODAF products included in the architecture. (See app. IV for a complete list of the DODAF products.)

Table 5: DOD Architecture Framework Products Included in Version 3.0

Product	Product title	Product description
All views (AV)		
AV-1 ^a	Overview and Summary Information	Executive-level summary information on the scope, purpose, and context of the architecture
AV-2 ^a	Integrated Dictionary	Architecture data repository with definitions of all terms used in all products
Operational view (OV)		
OV-2 ^a	Operational Node Connectivity Description	Graphic depiction of the operational nodes (or organizations) with needlines that indicate a need to exchange information
OV-3 ^a	Operational Information Exchange Matrix	Information exchanged between nodes and the relevant attributes of that exchange
OV-5 ^a	Operational Activity Model	Operations that are normally conducted in the course of achieving a mission or a business goal, such as capabilities, operational activities (or tasks), input and output flows between activities, and input and output flows to and from activities that are outside the scope of the architecture
OV-6a	Operational Rules Model	One of three products used to describe operational activity—identifies business rules that constrain operations
OV-6c	Operational Event-Trace Description	One of three products used to describe operational activity—traces actions in a scenario or sequence of events
OV-7	Logical Data Model	System data requirements and structural business process rules of the operational view

³³DOD, *Department of Defense Architecture Framework*, Version 1.0, Volume 1 (August 2003) and Volume 2 (February 2004).

(Continued From Previous Page)

Product	Product title	Product description
Systems view (SV)		
SV-1 ^a	Systems Interface Description	Systems nodes, systems, and systems items and their respective interconnections
SV-5	Operational Activity to Systems Function Traceability Matrix	Mappings of relationships between the set of operational activities and the set of system functions
SV-6	Systems Data Exchange Matrix	Characteristics of the data exchanged between systems
Technical standards view (TV)		
TV-1 ^a	Technical Standards Profile	Listing of standards that apply to SV elements

Source: DOD.

^aProduct that the DODAF designates as essential.

Version 3.0 of DOD's business enterprise architecture partially satisfies each of the three major requirements specified in the act.

With respect to the first requirement, regarding an information infrastructure, the act cites four requirements, each of which Version 3.0 partially addresses, as described below.

- *Comply with federal accounting, financial management, and reporting requirements.*

Partial compliance is achieved based on the architecture's inclusion of the Standard Financial Information Structure (SFIS), which includes a Standard Accounting Classification Structure (SACS) that can allow DOD to standardize financial data elements necessary to support budgeting, accounting, cost/performance management, and external reporting. The SFIS and SACS are based upon mandated requirements defined by external regulatory entities, such as the U.S. Treasury, OMB, the Federal Accounting Standards Advisory Board, and the Joint Financial Management Improvement Program.³⁴ As a result, SFIS can enable compliance with these entities' requirements if implemented properly. SFIS, while not

³⁴The Joint Financial Management Improvement Program (JFMIP) was a joint and cooperative undertaking of the Department of the Treasury, GAO, OMB, and the Office of Personnel Management (OPM), working in cooperation with each other and other federal agencies to improve financial management practices in the federal government. Leadership and program guidance were provided by the four Principals of JFMIP—the Secretary of the Treasury, the Comptroller General of the United States, and the Directors of OMB and OPM. Although JFMIP ceased to exist as a stand-alone organization as of December 1, 2004, the JFMIP Principals will continue to meet at their discretion.

complete, has been used to develop and incorporate business rules in the architecture for such areas as managerial cost accounting, general ledger, and federally owned property. Business rules are important because they explicitly translate important business policies and procedures into specific, unambiguous rules that govern what can and cannot be done.

However, the architecture does not provide for compliance with all federal accounting, financial, and reporting requirements. For example, it does not do the following:

- It does not contain the information needed to achieve compliance with the Department of the Treasury's United States Standard General Ledger.³⁵ In particular, the logical data model (OV-7) does not contain all the data elements or attributes that are needed to facilitate information sharing and reconciliation with the Treasury. The architecture also does not include a strategy for achieving compliance with the Treasury's general ledger. For example, it does not state whether DOD will adopt the Treasury data model or simply map its data model to the one for the Treasury. Program officials agreed and stated that this limitation is being reviewed and may be addressed in Version 3.1 of the architecture.
- It does not address the locations where specified activities are to occur and where the systems are to be located. Program officials agreed; however, they stated that the architecture is not intended to include this level of detail because it is capabilities-based rather than solutions-based and that this information will be contained either within the department's Global Information Grid³⁶ or individual system programs' documentation. We disagree with the department's position that information pertaining to locations is better captured in a solutions-based architecture rather than in the business enterprise architecture. The identification of operationally significant and strategic business locations, as well as the need for a business

³⁵The United States Standard General Ledger provides a uniform Chart of Accounts and technical guidance to be used in standardizing federal agency accounting.

³⁶DOD defines the Global Information Grid as the globally interconnected, end-to-end set of information, capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

logistics model, is a generally accepted best practice for defining the business operations.³⁷ This is because the cost and performance of implemented business operations and technology solutions are affected by where they are located, and thus need to be examined, assessed, and decided in an enterprise context, rather than in a piecemeal systems-specific fashion.

- *Routinely produce timely, accurate, and reliable financial information for management purposes.*

Partial compliance is achieved in light of the financial information that is to be produced through (1) SFIS, which can support data accuracy, reliability, and integrity requirements for budgeting, financial accounting, cost and performance management, and external reporting across DOD, and (2) a “Manage Business Enterprise Reporting” system function, which is intended to support the reporting of financial management and program performance information, including agency financial statements.

However, as previously discussed, SFIS is not complete and has yet to be implemented. Moreover, accurate and reliable information depends, in part, on using standard definitions of key terms in the architecture. The architecture does not include definitions for all such terms. In particular, the department has yet to define all enterprise-level terms, meaning terms relating to information that needs to be aggregated to support DOD-wide reporting. For example, in Version 3.0 of the architecture, terms such as “balance forwarded” and “receipt balances” were not defined in the integrated dictionary, even though these terms were used in process descriptions. In the absence of these definitions, component organizations (military services, defense agencies, and field activities) could continue to use local terms and definitions. Such locally meaningful terms cannot be reliably and accurately aggregated to permit DOD-wide visibility, as defined by the department’s business enterprise priorities. This inability to aggregate information for reporting purposes has historically required the department to produce financial information through inefficient methods (e.g., data calls or data translations), which have proven neither accurate nor timely. Program officials agreed and stated that they are currently

³⁷See, for example, J. A. Zachman, “A Framework for Information Systems Architecture,” *IBM Systems Journal* 26, no. 3 (1987); Paula Hagan, “Relating Elements of the Zachman Framework, Spewak’s Enterprise Architecture Planning, and DOD Products” (June 18, 2002); and B. Craig Meyers and Patricia Oberndorf, *Managing Software Acquisition Open Systems and COTS Products* (Addison-Wesley, 2001).

working to complete SFIS and that they would continue to incorporate and define terms as appropriate as the architecture is evolved.

- *Integrate budget, accounting, and program information and systems.*

Partial compliance is accomplished through information and systems that are to be integrated using (1) an enterprise-level automated reporting system known as Business Enterprise Information Services (BEIS), which is intended to provide timely, accurate, and reliable business information across the department to support auditable financial statements and provide detailed financial information visibility for management in support of the warfighter, and to integrate budget, accounting, and program information that is widely dispersed among systems and organizations across the department; (2) a generic system entity called “Financial Management System Entity,” which is to roll up component-level systems, or potential systems, that support current or future interface requirements; (3) the “Manage Business Enterprise Reporting” system function, which is to aggregate and distribute information according to requirements; and (4) other architectural elements, such as definitions and standards of data exchanges³⁸ to ensure that the data can be mutually understood, received, processed, and potentially aggregated and analyzed, as well as some terms used in the architecture.

However, the architecture does not include certain elements:

- It does not include a fully defined and yet to be implemented SFIS—that is, an SFIS that includes all data exchanges as well as the business rules that are to be automated by SFIS, BEIS, and user activities, and are to be supported by procedure manuals.
- It does not include all systems needed to achieve integration, as evidenced by instances in which the architecture provides “placeholders” or generic references for yet to be defined future systems (e.g., Financial Management System Entity). Program officials agreed and stated that these systems would be added as solutions are defined to address identified capability gaps.

³⁸Examples of data exchanges cited in the architecture include those associated with disbursing, collecting, and obligating data. Data exchange standards cited in the technical reference model include the Electronic Data Interchange, the American National Standards Institute Accredited Standards Committee X12, and the Extensible Markup Language 1.0.

-
- *Systematic measurement of performance, including the ability to produce timely, relevant, and reliable cost information.*

Partial compliance is achieved via identification of operational activities that are to be established to monitor the performance of the DOD business mission area and to develop performance plans that include performance levels, outcomes, and expected risks.

However, the architecture does not do the following:

- It does not provide for the systematic measurement of performance, because it has not established operationally acceptable performance thresholds for such measures as timeliness, accuracy, and reliability of financial information. These operative thresholds have significant influence on how business process activities are to be organized and controlled. Program officials agreed and stated that this issue is being addressed.
- It does not describe the “As Is” business and technology environments needed to conduct the gap analysis that is to show the performance shortfalls to be addressed, and thus it does not provide the underlying basis for the transition plan. Program officials agreed that the architecture does not contain an “As Is” architecture description. They stated that they have nevertheless examined the “As Is” conditions in identifying the “To Be” solutions in the architecture. They also stated that they recognize that these “As Is” conditions are not in the architecture and they have yet to be provided to us, and that they need to link this information to the “To Be” architecture.

With respect to the act’s second requirement, that the architecture includes policies, procedures, data standards, and system interface requirements to be applied departmentwide, Version 3.0 partially complies. In particular, the architecture identifies federal guidance relevant to core business missions, such as the financial management and the human resources

missions.³⁹ In addition, the architecture identifies a specific policy entitled “Supply Chain Materiel Management Policy”—dated April 22, 2004—that is relevant to guiding and controlling the department’s core business mission and business processes for materiel and logistics. Moreover, the architecture identifies conceptual, operational, and automated business rules that can be used to govern the implementation of systems investments in accordance with policies. However, not all relevant policies are included in the architecture. For example, policies governing the development, maintenance, and implementation of the architecture are not included. Program officials agreed, and stated that the decision memorandums that were used to guide the development of Version 3.0 will be formalized as a departmental policy.

In addition, Version 3.0 of the architecture includes a logical data model (OV-7) that contains data entities, attributes, and their relationships and an enterprise Technical Standards Profile (TV-1) that comprises a list of data standards (e.g. Extensible Markup Language 1.0 data exchange standard); however, the architecture does not include a systems standards profile that would ensure data sharing and interoperability among departmentwide business systems. Version 3.0 also identifies some, but not all, system interface requirements.⁴⁰ For example, the architecture has yet to identify interface requirements with DOD systems that provide infrastructure services, such as network routing. Program officials acknowledged that the architecture does not include a systems standards profile and all system interface requirements and stated that they will address this in future versions.

With respect to the act’s third requirement, that the architecture be consistent with OMB policies and procedures, Version 3.0 partially complies. According to OMB guidance, an enterprise architecture should

³⁹As examples, for the financial management core business mission area, DOD’s business enterprise architecture identified guidance, such as the Joint Financial Management Improvement Program and OMB Circular No. A-19 entitled *Title 5 (Organization and Employees), Part I, Chapter 5, Subchapter II, Section 552a (The Privacy Act of 1974)*. For the human resources core business mission area, the architecture identified chapter 14 of Title 29 relating to age discrimination in employment.

⁴⁰An example of a system interface requirement is the Human Resources interface “DCPDS-DIMHRS,” which represents the requirements needed to exchange data between the Defense Civilian Personnel Data System and the Defense Integrated Military Human Resources System.

describe the “As Is” and “To Be” environments and a transition plan.⁴¹ Further, this guidance requires the architecture to include, among other things, the following:

- *Business processes.* The work performed to support the agency’s mission, vision, and performance goals. Agencies must also document change agents, such as legislation or new technologies that will drive architecture changes.
- *Information flow and relationships.* The information used by the agency in its business processes, including where it is used and its movement among locations. These information flows are intended to show what information is needed where and how the information is shared to support mission functions.
- *Technology infrastructure.* The functional characteristics, capabilities, and interconnections of the hardware, software, and telecommunications.
- *Security architecture.* The support provided to secure information, systems, and operations.

Version 3.0 of the architecture includes a “To Be” architecture and a transition plan; however, it does not include an “As Is” architecture, which is essential to performing a gap analysis to identify capability and system performance shortfalls that the transition plan is to address. As previously discussed, program officials agreed and stated that they plan to address this. In addition:

- Version 3.0 defines some of the business processes at a high level. However, it does not include all business processes. For example, the architecture does not describe key aspects of the planning, programming, budgeting, and execution processes. In particular, the architecture does not yet define a clear planning process that balances requirements with resources and provides direction for execution.
- It includes information flows and relationships.

⁴¹OMB Circular No. A-130, *Management of Federal Information Resources* (Nov. 30, 2000).

-
- It does not include a description of the technology infrastructure.
 - It does not include a security architecture.

Beyond the above described areas in which Version 3.0 of the business enterprise architecture does not fully satisfy the requirements in the fiscal year 2005 defense authorization act, Version 3.0 has other limitations. Specifically:

- The scope of Version 3.0 is not fully consistent with the scope of the enterprise transition plan. For example, we identified 21 systems in the architecture that are not included in the transition plan's "Master List of Systems and Initiatives" that support the business enterprise priorities and should therefore be funded. Instead of being on this master list, 19 of these 21 systems are included in the transition plan as part of a master list of "Non-priority DOD programs." Therefore, the systems identified as targeted solutions in the architecture are not being recognized in the transition plan as systems to be funded to provide the needed business capabilities. The remaining 2 of the 21 systems, "Industry System" and "Unstructured Data Sources," are not identified at all in the transition plan. As a result, the transition plan does not yet explicitly recognize the need to transition to the capabilities implied by these two systems, or else these systems exceed the scope of the transition plan, the Overview and Summary Information product (AV-1), or both.
- In addition, the AV-1 states that the scope of Version 3.0 is limited to the six DOD business enterprise priorities. In contrast, the list of "Non-priority DOD programs" in the transition plan is described as a listing of systems "that are not DOD Enterprise or Component Priority Programs" and thus would not be targeted solutions for the business enterprise priorities. As a result, the stated scope of the AV-1 is narrower than the implied scope of the transition plan.
- The transition plan treats certain entities, such as the Financial Management System Entity, as system solutions in the Master List of Systems, whereas Version 3.0 treats these entities as contextual placeholders. This difference is not explained.
- Finally, another system (the Expeditionary Combat Support System) is explicitly related to four business enterprise priorities (Financial Visibility, Acquisition Visibility, Materiel Visibility, and Common

Supplier Engagement) in the Master List of Systems in the transition plan, but it is not included in the architecture.

- Version 3.0 refers to “Recruit Candidate” as a needed business capability, but this capability is not reflected in the transition plan. This is important because needed capabilities in the architecture should be reflected in the transition plan to ensure that they are addressed. As another example, “Access Candidate” is referred to as a needed business capability in the transition plan, but it is defined as an existing operational activity in the architecture. If it is in fact an operational activity, this means that the department plans to invest resources to achieve a business capability to address a performance shortfall that does not exist. Program officials stated that these are errors and that they will be corrected.

Version 3.0 does not explicitly state the time frame covered for the “To Be” environment. Rather, it describes the time frame as being “near-term To Be,” but it does not clearly define what is meant by “near-term,” nor does it link this time frame to the milestones associated with the business enterprise priorities or the capabilities and systems in the transition plan. According to relevant guidance,⁴² the “To Be” architecture should be fiscally and technologically achievable, and therefore it should generally project 3 to 5 years into the future to accommodate rapid changes in technologies, changes in mission focus and priorities, and uncertainty in future resource availability. Program officials agreed and stated that they would use “near-term” consistently in future versions of the architecture and transition plan.

Version 3.0 does not represent a fully integrated set of architecture products, although we did find greater product integration than in prior versions of the architecture. Examples of instances in which product integration was not apparent follow.

- First, the Operational Event-Trace Description product (OV-6c)—which depicts when activities are to occur within operational processes—includes a process entitled “Send Statements of

⁴²GAO, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1)*, [GAO-03-584G](#) (Washington, D.C.: April 2003); and CIO Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0 (February 2001).

Accountability or Transactions or Trial Balance to Treasury.” However, the Operational Activity Model (OV-5)—which shows the operational activities (or tasks) that are to occur and the input and output process flows among these activities— identifies no corresponding activity. Instead, the OV-5 has an activity entitled “Perform Treasury Operations,” which has four subactivities, none of which is linked to the above process.⁴³ Program officials agreed that these were not linked; however, they stated that the “Perform Treasury Operations” activity and its subactivities are not intended to link with the above mentioned process. However, intended linkages are not clear because the architecture does not include a traceability matrix that shows the connection between the two architecture products (OV-6c and OV-5). Program officials have acknowledged the need for greater product integration.

- Second, one identified event in the architecture—“triggers the supplier process that provides supplier inventory information to the DOD”—is depicted as two separate events at different levels in the process decomposition. In particular, there are different names for this event on the parent diagrams and the child diagrams, and different templates were used to prepare the diagrams. Program officials agreed that these names differed and stated that this would be addressed.
- Third, certain business rules are not explicitly linked to the events included in the architecture description, such as “ENT Post Concurrent Months” and “ENT_Estimate_Receivable.” Program officials stated that the guidelines being used by the department require the business rules to be linked to process steps or decision gateway objects, not events. However, because an event is something that “happens” during the course of a business process, it affects the flow of the process and usually has a cause (trigger) or an effect (result). Therefore, best practices⁴⁴ recognize the need to integrate or link the “triggers” that are reflected in the Operational Information Exchange Matrix (OV-3) to both the business rules shown in the

⁴³The four subactivities are Manage Disbursements, Manage Collections, Manage Cash, and Manage Investments.

⁴⁴See, for example, Business Process Management Initiative, *Business Process Modeling Notation*, Version 1.0 (May 2004); and Ronald Ross, *Business Rule Concepts: Getting to the Point of Knowledge* (Business Rule Solutions, LLC, 2005).

Operational Rules Model (OV-6a) and the business events shown in the Operational Event-Trace Description (OV-6c). Program officials stated that they will consider revising their guidelines to link business rules to events.

- Fourth, the interface diagram for the Financial Management System Entity (FMSE) does not include 4 of the 21 relevant interfaces identified in the AV-2 product, which is the integrated dictionary. Instead, these four interfaces are shown in other system interface diagrams, which are not linked to the FMSE diagram. Program officials stated that they will address this.
- Fifth, the timelines reflected in the transition plan are difficult to map to the “To Be” description, according to DOD’s contractor responsible for verification and validation of the architecture and transition plan.⁴⁵
- Sixth, the architecture is not adequately linked to the component architectures and transition plans, although such linkage is particularly important given the department’s newly adopted federated approach to developing and implementing the architecture. According to DOD, a federated architecture is composed of a set of coherent but distinct entity architectures. The members of the federation collaborate to develop an integrated enterprise architecture that conforms to the enterprise view and to the overarching rules of the federation. Program officials agreed and stated that greater levels of integration will be a key goal of future versions of the architecture.

Moreover, while Version 3.0 of the architecture is easier to navigate through than prior versions because of improved product integration, it is still difficult to navigate and use this version, making verification and validation of completeness and correctness unnecessarily time consuming. For example, to trace business rules to their associated events (e.g., the business rule entitled “ENT Post Concurrent Months” to the event “trial balance closing is complete”), we had to first locate and review the description of the business rule, then locate the descriptions of the events by manually searching through numerous process diagrams. This was

⁴⁵*Transformation Support Office IV&V Participation in, and Review of, BEA 3.0* (Sept. 28, 2005).

necessary because the architecture does not include a systematic function that enables the user to list all business rules that are associated with events and all events that are associated with business rules. Such a function is an accepted verification and validation method recommended by industry experts.⁴⁶

DOD and its verification and validation contractor have also identified limitations in Version 3.0 of the architecture, which program officials told us would be addressed in future versions. For example, the architecture does not do the following:

- It does not explicitly link to the department’s primary non-business enterprise architecture (the Global Information Grid Architecture, which covers the warfighting mission area).
- It does not adequately address “net-centricity,” a DOD term that refers to having a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data and services (e.g., security services) are shared “timely and seamlessly” among users, applications, and platforms. According to DOD, the architecture must be improved to better designate enterprise data sources, business services, and IT infrastructure services.
- It does not accurately and completely address stakeholder comments and their change requests.

Program officials, including the Director of the Transformation Support Office, the Chief Architect, and the Enterprise Transition Plan Team Lead, stated that the department has taken an incremental approach to developing the business enterprise architecture and meeting the act’s requirements. Accordingly, the Special Assistant to the Deputy Under Secretary of Defense for Business Transformation and contractor officials said that Version 3.0 was appropriately scoped to provide for that content that could be produced in the time available to both lay the foundation for fully meeting the act’s requirements and provide a blueprint for delivering near-term capabilities and systems to meet near-term business enterprise priorities. Because of this, they stated that Version 3.0 fully satisfies the intent of the act.

⁴⁶See, for example, Ronald Ross, *Business Rule Concepts: Getting to the Point of Knowledge* (Business Rule Solutions, LLC, 2005).

We support DOD taking an incremental approach to developing the business enterprise architecture, recognizing that adopting such an approach is a best practice that we have advocated. In addition, we believe that Version 3.0 provides a foundation upon which to build a more complete architecture. However, we do not agree that Version 3.0 fully satisfies the requirements in the fiscal year 2005 defense authorization act. Further, the missing scope and content and related shortcomings described above mean that while this version is a reasonable baseline upon which to build, it is not yet a sufficient frame of reference for defining a common vision and the kind of comprehensive transition plan needed to effectively and efficiently guide and constrain system investment decision making.

Transition Plan Partially Satisfies the Act, but Improvements Are Needed

The defense authorization act for fiscal year 2005 requires that DOD develop, by September 30, 2005, a transition plan for implementing its business enterprise architecture, and that this plan meet three requirements. The requirements are that it include

- an acquisition strategy for new systems that are expected to be needed to complete the defense business enterprise architecture;
- listings of the legacy systems that will and will not be part of the target business systems environment, and a strategy for making modifications to those systems that will be included; and
- specific time-phased milestones, performance metrics, and a statement of financial and nonfinancial resource needs.

On September 28, 2005, the Acting Deputy Secretary of Defense approved the transition plan. This plan, as described below, partially satisfies the three requirements.

With respect to the first requirement, concerning an acquisition strategy, the plan does describe a high-level approach for transforming the department's business operations and systems, and the approach is driven by a set of priorities and a targeted set of business capabilities that are to be provided through the implementation of key programs. In general, the plan includes information (e.g., the lead core business mission, budget

information, and milestones) for the 39 transformational initiatives⁴⁷ and the 60 business systems⁴⁸ that are to be part of the “To Be” architectural environment, including an acquisition strategy for each system.

However, the plan is largely based on a bottom-up planning process in which ongoing programs were examined and categorized in the plan around business enterprise priorities and capabilities, including a determination as to which programs would be designated and managed as DOD-wide programs versus component programs. This bottom-up approach to developing the plan does not explicitly reflect transition planning key practices cited in federal guidance, such as consideration of technology opportunities, marketplace trends, fiscal and budgetary constraints, institutional system development and acquisition capabilities, and new and legacy system dependencies and life expectancies, and the projected value of competing investments.⁴⁹ Moreover, it means that the plan is not based on a top-down capability gap analysis between the “As Is” and “To Be” architectures in which capability and performance shortfalls are described, and investments (such as transformation initiatives and systems) that are to address these shortfalls are clearly identified. For example, those programs and systems that need to be acquired, developed, or modified and by when to meet the department’s time frame to have a general ledger capability in fiscal year 2006 or 2007 are not clearly identified. According to DOD, this general ledger capability is to be addressed by systems and initiatives that are spread across various appendixes in the transition plan. However, the transition plan should clearly describe the collective investments, including the components and their respective systems, the specific strategies to be used, and the estimated timelines for completion, to address this capability shortfall. This is not yet the case because for example, the transition plan states that “each component is still identifying the optimal path to achieve the capability to post to a United States Standard General Ledger compliant DOD corporate ledger.”

⁴⁷These initiatives include, for example, the Air Force Information Reliability and Integration Action Plan and the Defense Logistics Agency Integrated Data Environment.

⁴⁸The 60 systems include 23 enterprise systems and 37 component systems.

⁴⁹[GAO-03-584G](#) and CIO Council, *A Practical Guide to Federal Enterprise Architecture, Version 1.0* (February 2001).

With respect to the second requirement, about identifying legacy systems that will and will not be part of the “To Be” architectural environment, including modifications to these systems, the plan does show some of the legacy systems that are to be replaced by ongoing programs. For example, it identifies the Defense Cash Accountability System (DCAS) as a target system and listed several legacy systems that would be replaced by DCAS (e.g., the Cash Reconciliation System, the Financial Operations Support system, and the International Balance of Payments system). It also provides a list of legacy systems that will be modified to provide capabilities associated with the target architecture environment, such as the Standard Procurement System and the Navy Marine Corps Intranet.

However, the transition plan does not include a number of elements:

- It does not include a complete listing of the legacy systems that will not be part of the target architecture. For example, the plan identified 145 legacy systems that would be migrating to the target system Expeditionary Combat Support System (ECSS). However, DOD documentation shows that this system includes over 659 legacy logistics systems and other legacy management information systems.⁵⁰ This means that the plan does not account for 514 systems related to the integration and migration of ECSS. Program officials agreed and stated that the 145 systems included account for 90 percent of the Air Force’s Installation and Logistics portfolio. They also said that the Air Force is currently assessing the remaining 514 systems to identify interfaces and to determine duplication, and will update the transition plan to reflect this assessment.

⁵⁰DOD, *Expeditionary Combat Support System Sources Sought Synopsis* (May 10, 2004).

-
- The plan does not include system and budget information for 13 of its 15 defense agencies⁵¹ and for 8 of its 9 combatant commands.⁵² Exclusion of the Defense Information Systems Agency is particularly limiting, given that this agency provides IT infrastructure services that business systems will need to use. This omission makes it unclear whether the new business systems will be able to reuse existing components, thereby leveraging established capabilities, or will be allowed to introduce duplicative capabilities. According to program officials, the transition plan excluded information for 13 of the defense agencies and for 8 of its combatant commands because it was focused on the largest business-focused organizations in DOD—those meeting Tier 1 and Tier 2 investment review board certification criteria.⁵³ They noted that the

⁵¹DOD included system and budget information for the following defense agencies in the transition plan: (1) Defense Financial and Accounting Service and (2) Defense Logistics Agency. DOD did not include this information for the following defense agencies: (1) Ballistic Missile Defense Organization, (2) Defense Advanced Research Projects Agency, (3) Defense Commissary Agency, (4) Defense Contract Audit Agency, (5) Defense Contract Management Agency, (6) Defense Information Systems Agency, (7) Defense Intelligence Agency, (8) Defense Legal Services Agency, (9) Defense Security Cooperation Agency, (10) Defense Security Service, (11) Defense Threat Reduction Agency, (12) National Imagery and Mapping Agency, and (13) National Security Agency.

⁵²DOD included system and budget information for the Transportation Command in the transition plan. DOD did not include this information for the (1) Central Command, (2) Joint Forces Command, (3) Pacific Command, (4) Southern Command, (5) Space Command, (6) Special Operations Command, (7) European Command, and (8) Strategic Command.

⁵³As defined in the department's Investment Review Process Overview and Concept of Operations for Investment Review Boards, Tier 1 systems include all systems that are classified as a Major Automated Information System or a Major Defense Acquisition Program. A Major Automated Information System is a program or initiative that is so designated by the Assistant Secretary of Defense (Networks and Information Integration)/Chief Information Officer or that is estimated to require program costs in any single year in excess of \$32 million (fiscal year 2000 constant dollars), total program costs in excess of \$126 million (fiscal year 2000 constant dollars), or total life-cycle costs in excess of \$378 million (fiscal year 2000 constant dollars). A Major Defense Acquisition Program is so designated by the Secretary of Defense, or it is a program estimated by the Secretary of Defense to require an eventual total expenditure for research, development, test, and evaluation of more than \$300 million (fiscal year 1990 constant dollars) or an eventual total expenditure for procurement of more than \$1.8 billion (fiscal year 1990 constant dollars). Tier 2 systems include those with modernization efforts of \$10 million or greater but that are not designated as a Major Automated Information System or a Major Defense Acquisition Program, or programs that have been designated as investment review board interest programs because of their impact on DOD transformation objectives. The tier system includes another tier in addition to these two: Tier 3 systems are modernization efforts that have anticipated costs greater than \$1 million but less than \$10 million.

majority of these organizations do not meet these threshold criteria and therefore were not included in the transition plan.⁵⁴

- The plan does not include a complete listing of the legacy systems that will be part of the target architecture, nor explicit strategies for modifying those legacy systems identified in the plan's system migration diagrams. For example, other DOD documentation shows that ECSS, the Defense Enterprise Accounting Management System, and the Defense Integrated Military Human Resources System (DIMHRS) must interface to provide needed business capabilities. However, the transition plan does not reflect this needed integration or the specific capabilities that will be provided by ECSS. According to the transition plan, these strategies are incorporated in the components' architectures. However, as we stated in the previous section of this report, the components' architectures have yet to be linked to the business enterprise architecture. Program officials stated that this issue will be addressed through the department's tiered accountability approach.

With respect to the third requirement, concerning milestones, performance metrics, and resource needs, the plan includes key milestone dates for the 60 systems identified. For example, September 2006 was given as the milestone date for the Defense Travel System to achieve full operational capability, and performance metrics were cited for some systems; for example, for DIMHRS, the plan cites a metric of reducing manual workarounds for military pay by 90 percent. However, the plan does not show specific dates for terminating or migrating many legacy systems, such as the Cash Reconciliation System and the Financial Operations Support system, and it does not include milestone dates for some ongoing programs, such as the Navy Tactical Command Support System. Further, the plan does not include benefits or measures and metrics focused on mission outcomes for each system that can be linked to the plan's strategic goals. In addition, although the plan does identify resource needs in terms of funding, these needs are a reflection of the funding needs contained in the fiscal year 2006 budget submission; this submission was approved before the programs included in the transition plan were reevaluated by the DBMSC as to their fit within the "To Be" architectural environment and the reasonableness of their respective plans. According to program officials,

⁵⁴Per DOD, components that have Tier 1 and Tier 2 systems that were excluded from the transition plan are (1) Defense Commissary Agency, (2) Defense Information Systems Agency, (3) Defense Threat Reduction Agency, and (4) TRICARE.

this means that the resource needs in the transition plan for some programs are not current.

Beyond the transition plan's partial compliance with the three requirements in the act, as described above, the plan is also missing relevant context and is not consistent with the architecture in various ways. For example:

- The plan identifies 60 systems as target systems (e.g., DCAS), but the “To Be” architecture includes only 23 of these systems. Program officials agreed and stated that the other 37 systems are contained within component architectures and transition plans. However, as we previously stated, the component architectures have not been linked to Version 3.0.
- The plan identifies 21 enterprise initiatives⁵⁵ (e.g., SFIS, Defense Acquisition Management Information Retrieval, and Customer Relationship Management), but only 1 of these—Defense Acquisition Management Information Retrieval—is included in the architecture, and it is shown in the architecture as a system, not an initiative. It is important for the architecture to include these initiatives and their relationships to systems. Program officials agreed and stated that Defense Acquisition Management Information Retrieval will be appropriately reflected as a system in the next version of the plan.
- The plan includes a list of 66 systems that are characterized as nonpriority DOD enterprise or component programs that will be part of the target architecture, but the target architecture does not identify all these systems. Further, some systems on the list, such as the Mechanization of Contract Administration Services (MOCAS), are systems that in the past were considered eligible for elimination. Program officials agreed and stated that some of these systems are component-level systems and therefore are reflected within the yet to be linked component architectures and transition plans. With regard to systems that, like MOCAS, are slated for termination, these officials

⁵⁵According to DOD, “systems” can be an information system—including financial systems, mixed systems, financial data feeder systems—and IT and information assurance infrastructure used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. The term “initiative” typically refers to nonsystem programs or activities that are focused on policy changes, data standards, or other business practice changes.

stated that replacement systems for such legacy systems have not yet been identified. Until they are, the legacy systems will continue to be shown as target solutions.

- The specific business capabilities to be provided by the system solutions for the six business enterprise priorities have not been completely defined in the plan. For example, the Materiel Visibility business enterprise priority requires additional capabilities related to the supply chain planning process, according to DOD, but these capabilities have yet to be defined in the plan. Program officials stated that these will be addressed in future versions of the architecture and transition plan.

According to program officials, including the Director of the Transformation Support Office, the Chief Architect, and the Enterprise Transition Plan Team Lead, the transition plan is evolving, and any limitations will be addressed in future iterations of the plan. The Special Assistant to the Deputy Under Secretary of Defense for Business Transformation and contractor officials stated that the department has taken an incremental approach to developing a transition plan and that the plan, as constrained by the scope of Version 3.0 of the architecture, satisfies the intent of the act's requirements.

We support an incremental approach to developing the transition plan, which is a best practice that we have advocated. However, the plan does not fully comply with the act's requirements. Moreover, it was not derived on the basis of a gap analysis between "As Is" and "To Be" architectures, and it is not of sufficient scope, content, and alignment to effectively and efficiently manage the disposition of the department's existing inventory of systems or for sequencing the introduction of modernized business operations and supporting systems.

Fiscal Year 2006 IT Budget Submission Includes Some but Not All Information That the Act Specifies

The fiscal year 2005 defense authorization act specifies information that the department is to incorporate in its budget request for fiscal year 2006 and each fiscal year thereafter. Specifically, the act states that each budget request must include information on

- each defense business system for which funding is being requested;
- all funds, by appropriation, for each such business system, including funds by appropriation specifically for current services (Operation and Maintenance) and systems modernization; and

-
- the designated approval authority for each business system.

DOD's fiscal year 2006 IT budget submission partially satisfies these three requirements. With regard to the first requirement, to identify each business system for which funding is requested, the fiscal year 2006 budget does not reflect all business systems. Specifically, when DOD submitted its fiscal year 2006 budget submission in February 2005, it did not yet have a comprehensive single inventory of its business systems. As we reported in May 2004,⁵⁶ DOD was relying at that time on several separate, inconsistent, and unreconciled databases to establish an inventory of its business and national security systems. Accordingly, we recommended that the department establish a single database for its inventory of business systems. On July 13, 2004, the Assistant Secretary of Defense (Networks and Information Integration)/Chief Information Officer (ASD(NII)/CIO) directed establishment of the DOD Information Technology Portfolio Data Repository (DITPR), and on September 28, 2005, the Deputy Assistant Secretary of Defense (Deputy CIO), issued guidance to begin merging the DOD IT registry⁵⁷ into DITPR. According to DOD, all business systems will be entered into DITPR by December 31, 2005. According to DOD, all systems will be entered into DITPR by September 30, 2006. However, the establishment and merger of these repositories had not been completed before the development and submission of the fiscal year 2006 IT budget.

With respect to the fiscal year 2007 and future IT budget submissions, DOD plans to use a separate database, entitled the Select and Native Programming Data Collection System–Information Technology to develop the department's IT budget submissions. For these future submissions, it will be important for DOD to ensure that this system contains all business systems investments.

The extent to which any of these repositories include all business systems, and thus the extent to which the fiscal year 2006 and future budget submissions will as well, is also a function of whether DOD classifies a

⁵⁶GAO, *DOD Business Systems Modernization: Billions Continue to Be Invested with Inadequate Management Oversight and Accountability*, [GAO-04-615](#) (Washington, D.C.: May 27, 2004).

⁵⁷The IT Registry is a database of mission-critical and mission-essential IT systems maintained by the Assistant Secretary of Defense (Networks and Information Integration)/Chief Information Officer.

given system as a business system or a national security system.⁵⁸ We previously reported that DOD reclassified 56 systems in its fiscal year 2005 budget request from business systems to national security systems.⁵⁹ The net effect of the reclassification was a decrease of approximately \$6 billion in the fiscal year 2005 budget request for business systems and related infrastructure. While some of the reclassifications appeared reasonable, we reported that others were questionable.⁶⁰ According to DOD, it is currently reviewing the 56 systems, and it plans to complete these reviews by February 2006 to ensure they are properly classified in the fiscal year 2007 IT budget submission.

Further reclassifications are in the fiscal year 2006 budget submission. Specifically, 13 systems have been reclassified from business systems to national security systems in the fiscal year 2006 submission. In addition, 10 national security systems have been reclassified as business systems in the fiscal year 2006 submission. For example:

- The Air Force's Aviation Resource Management System, with a fiscal year 2006 budget of \$3.3 million, was reclassified from a business to a national security system. DOD included this system in the department's original inventory of business systems in April 2003 and also reported it as a business system under the Logistics domain in the fiscal year 2005 IT budget request.
- The TRICARE Management Agency's Medical Readiness Decision Support System, with a fiscal year 2006 budget of \$1.3 million, was reclassified from a national security system to a business system.

Identification of each business system is also complicated by the fact that DOD's definition of a business system, as given in its budget submission, differs from the definition of a business system in the fiscal year 2005 defense authorization act. According to the act, a defense business system is "an information system, other than a national security system, operated

⁵⁸National security systems are intelligence systems, cryptologic activities related to national security, military command and control systems, and equipment that is an integral part of a weapon or weapons system or is critical to the direct fulfillment of military or intelligence missions.

⁵⁹[GAO-05-381](#).

⁶⁰[GAO-05-381](#).

by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities.”⁶¹ In contrast, the definition that DOD used as the basis for its fiscal year 2006 IT budget request notes that IT infrastructure and information assurance funding supports both business systems and national security systems. As a result, DOD’s position is that shared IT infrastructure and information assurance funding cannot be classified as related to business systems or to national security systems.

With regard to the second requirement, to identify the type of funding (i.e., appropriation) being requested and whether the funding was for current services or modernization, the fiscal year 2006 budget submission identifies the type of funding (i.e., appropriation) being requested and whether the funding was for current services or modernization. However, a number of systems are assigned to a category designated “All Other.” It is not clear what is included in the budget submission under this category. In the fiscal year 2006 IT budget submission, this category totaled about \$1.2 billion, and includes, for example, about \$22.6 million for financial management. As we previously reported, the ASD(NII)/CIO and military services’ budget officials told us that the “All Other” category in the IT budget includes system projects that do not have to be identified by name because they fall below the \$2 million reporting threshold for budgetary purposes.⁶² This budgetary threshold is not consistent with the \$1 million threshold that the act requires for modernization review and approval, as discussed later in this report, and thus could affect DOD’s ability to identify all system investments that are subject to the requirements of the act. According to ASD(NII)/CIO officials, the fiscal year 2007 budget submission will identify all business systems for which planned spending is equal to or greater than \$1 million.

With respect to the third requirement, to identify the designated approval authority for each system, the fiscal year 2006 IT budget submission does so for most systems. However, the approval authority was not identified for 57 business systems. For example, the Navy’s C2 On-the-Move Network Digital Over-the-Horizon Relay system and the Defense Commissary

⁶¹10 U.S.C. § 2222 (j) (2).

⁶²[GAO-04-615](#).

Agency's Enterprise Business System had a designated approval authority of "Other."

DOD officials told us that the department recognizes the need to improve the accuracy of its budget submission to provide better information to both DOD management and the Congress on the department's business systems.

Full compliance with the act's requirements relative to budgetary disclosure is an important enabler of informed DOD budgetary decision making and congressional oversight. Lacking such disclosure, whether due to incomplete system repositories or incorrect system classification, hinders the department's efforts to improve its control and accountability over its business systems investments and constrains the Congress's ability to effectively monitor and oversee the billions of dollars spent annually to maintain, operate, and modernize the department's business systems environment.

Act's Requirement for Delegating IT System Responsibilities and Accountabilities to Designated Approval Authorities Has Been Satisfied

The defense authorization act for fiscal year 2005 directs DOD to put in place a specifically defined structure that is responsible and accountable for controlling business system investments to ensure compliance and consistency with the business enterprise architecture. More specifically, the act directs the Secretary of Defense to delegate responsibility for review, approval, and oversight of the planning, design, acquisition, deployment, operation, maintenance, and modernization of defense business systems to designated approval authorities or "owners" of certain business missions. These are as follows:

- The Under Secretary of Defense for Acquisition, Technology, and Logistics is to be responsible and accountable for any defense business system the primary purpose of which is to support acquisition, logistics, or installations and environment activities.
- The Under Secretary of Defense (Comptroller) is to be responsible and accountable for any defense business system the primary purpose of which is to support financial management activities or strategic planning and budgeting.
- The Under Secretary of Defense for Personnel and Readiness is to be responsible and accountable for any defense business system the primary purpose of which is to support human resource management activities.

-
- The Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer of the Department of Defense is to be responsible and accountable for any defense business system the primary purpose of which is to support information technology infrastructure or information assurance activities.
 - The Deputy Secretary of Defense or an Under Secretary of Defense, as designated by the Secretary of Defense is to be responsible for any defense business system to support any DOD activity not covered above.

DOD has satisfied this requirement under the act. On March 19, 2005, the Deputy Secretary of Defense issued a memorandum that delegated the authority in accordance with the criteria specified in the act, as described above.

Our research and evaluations, as reflected in the guidance that we have issued, show that clear assignment of senior executive investment management responsibilities and accountabilities is crucial to having an effective institutional approach to IT investment management.

Act's Requirements for Certain IT Investment Review Structures and Processes Have Been Partially Satisfied

The defense authorization act for fiscal year 2005 also required DOD to establish investment review structures and processes, including a hierarchy of investment review boards, each with representation from across the department, and a standard set of investment review and decision-making criteria for these boards to use to ensure compliance and consistency with the business enterprise architecture. In this regard, the act cites three specific requirements. First, it requires the establishment of the DBSMC for overseeing DOD's business systems modernization efforts, and it specifically identifies the DOD positions to chair and be members of this committee. Second, it requires each designated approval authority to establish by March 15, 2005, an investment review board for investments falling under that authority's responsibility. Third, the act requires establishment of an investment review process that includes, among other things, the use of common decision criteria, threshold criteria to ensure appropriate levels of review and accountability, and at least annual reviews of every business system investment.

DOD has partially satisfied this requirement in the act. Among other things, it has done the following.

-
- In February 2005, DOD chartered the DBSMC, identifying it as the highest ranking governance body responsible for overseeing business systems modernization efforts.⁶³ The DBSMC is responsible for ensuring that DOD improves its management and oversight of the department's business systems. Consistent with the act, the DBSMC is chaired by the Deputy Secretary of Defense, and its members include those positions specified in the act: namely, the designated approval authorities previously discussed, the secretaries of the military services, and the heads of the defense agencies. The vice-chair of the committee is the Under Secretary of Defense for Acquisition, Technology, and Logistics.
 - DOD established four investment review boards to improve the control and accountability over business system investments. The four are (1) Financial Management, (2) Human Resources Management, (3) Real Property and Installations Lifecycle Management, and (4) Weapon Systems Lifecycle Management and Materiel Supply and Services Management.⁶⁴ Each is chaired by the appropriate approval and certification authority (see previous section) and has DOD-wide representation, including membership from the combatant commands, military services, defense agencies, and the Joint Chiefs of Staff.
 - On June 2, 2005, the Under Secretary of Defense for Acquisition, Technology, and Logistics issued guidance entitled the Investment Review Process Overview and Concept of Operations for Investment Review Boards. This guidance integrates the policies, specifies responsibilities, and identifies the processes to govern the establishment and operation of investment review boards. Among other things, the guidance provides for these boards to review all business system investments, at least annually, and certify defense business system modernizations costing over \$1 million, as required by the act. The guidance also specifies the certification process, including criteria to be used.

⁶³See 10 U.S.C. § 186.

⁶⁴The Human Resources Management investment review board was established on June 14, 2005; the Weapon Systems Lifecycle Management and Materiel Supply and Services Management investment review board was established on July 21, 2005; the Real Property and Installations Lifecycle Management investment review board was established on July 27, 2005; and the Financial Management investment review board was established on August 9, 2005.

-
- On July 15, 2005, the Under Secretary of Defense for Acquisition, Technology, and Logistics issued supplemental guidance and criteria for the components (military services, defense agencies, and DOD field activities) to use in preparing their respective defense business system modernization submissions to the investment review boards.
 - Overall, DOD's investment structures and processes employ a concept that it refers to as "tiered accountability."⁶⁵ According to the department, tiered accountability is intended to place more responsibility for the management and oversight of business systems investments with the military services and defense agencies' leaderships. Accordingly, DOD's guidance describe a process in which business systems investments must be certified by multiple levels of approval and certification authorities, including the component program manager, the component-level precertification authority, the investment review board certification authority, and the DBSMC. As part of this process, a certification package for each system investment must be submitted to the approval authority, and this package is to include basic system information (e.g., system description and funding), justification as to how the system addresses enterprise-level or component-specific requirements; and analysis demonstrating compliance with the business enterprise architecture. A standard system certification template has been developed for use by all components and decision authorities.

The act designates the ASD(NII)/CIO as one of five designated approval authorities for which an investment review board is to be established. According to the act and the Deputy Secretary's March 19, 2005, memorandum, the ASD(NII)/CIO is responsible and accountable for any business system the primary purpose of which is to support IT infrastructure or information assurance activities. However, the ASD(NII)/CIO has not established an investment review board. According to DOD officials, a separate investment review board has not been established because the ASD(NII)/CIO does not consider the IT infrastructure, information assurance, and related activities that are under its purview to be business systems. They added that the ASD(NII)/CIO is represented on the other investment review boards and can thus oversee

⁶⁵See footnote 53. Both Tier 1 and Tier 2 certification submissions require a component precertification letter, a certification template, and the defense business systems dashboard. In addition, a component economic viability analysis and an independent cost review authority validation letter are applicable to all tiers and are available upon request from the component.

issues related to infrastructure and information assurance at those meetings.

DOD's not having established this investment review board is one of the reasons that the department's satisfaction of this requirement in the act is as yet only partial. In addition, a key aspect of the act and DOD's tiered accountability approach is the effective implementation of the defined structures and processes. It is important that such implementation occurs in a continuous and consistent fashion across the department, as we have previously stated. If it does not, the result could be investment decisions that perpetuate the existence of overly complex, error-prone, nonintegrated system environments and limit introduction of corporate solutions to long-standing business problems.

DOD Is Taking Actions Intended to Satisfy the Act's Requirement for Reviewing Projects over \$1 Million

The defense authorization act for fiscal year 2005 specifies two basic requirements, effective October 1, 2005, for obligation of funds for business system investments costing more than \$1 million. First, it requires that these investments be certified by a designated "approval authority" as meeting specific criteria.⁶⁶ Second, it requires that the DBSMC approve each certification. The act also states that failure to do so before the obligation of funds constitutes a violation of the Anti-Deficiency Act.⁶⁷

The department has taken a number of actions to comply with these two requirements. As mentioned in the previous section, the department has established an investment review process, and this process requires, among other things, that any defense business system modernization costing more than \$1 million obtain component precertification, investment review board approval, approval authority certification, and DBSMC approval. This process, as described in investment review board guidance (including DOD Business Systems Investment Review Proposal Submission Guideline), defines the information that programs are to

⁶⁶A key condition identified in the act includes certification by designated approval authorities that the defense business system modernization is (1) in compliance with the enterprise architecture; (2) necessary to achieve critical national security capability or address a critical requirement in an area such as safety or security; or (3) necessary to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration the alternative solutions for preventing such an adverse effect.

⁶⁷U.S.C. § 1341(a) (1) (A); see 10 U.S.C § 2222(b).

submit to obtain certification for systems meeting certain thresholds, referred to as tiers. Further, the process states that the component's precertification authority must certify that the system is not a duplicative effort and that it is compliant with the DOD business enterprise architecture before sending the system's certification package forward to an investment review board.

The department has identified 210 business system modernizations that meet this \$1 million threshold and thus need to be approved by the DBSMC. Of the 210, 166 were approved by the DBSMC before September 30, 2005. The remaining 44 have yet to be approved. This means that under the law, DOD cannot obligate fiscal year 2006 funds for these 44 systems until they receive DBSMC approval. It is important to note, however, that the department can continue to invest in these systems by using funds that are still available from previous fiscal years.

Just as with the identification of business systems in DOD's IT budget submissions (discussed earlier), the extent to which DOD ultimately complies with the act with regard to obligations costing more than \$1 million depends, in part, on the proper classification of systems as business versus national security. The following example illustrates this point.

- In its fiscal year 2006 budget, the department is requesting about \$167 million for the modernization of the Army's Global Combat Support System. The system, as we previously reported, was reclassified as a national security system in the fiscal year 2005 budget, even though it was included in the department's reported inventory of about 4,200 business systems and approved by the DOD Comptroller in January 2004.⁶⁸ Also, the DBSMC approved this Army system in September 2005, even though the system remains listed in the fiscal year 2006 IT budget request as a national security system. In contrast, the department is requesting about \$31 million for the modernization of the Air Force's version of this system (Global Combat Support System-Air Force) in its fiscal year 2006 budget. However, this system is not listed as one of the 210 systems requiring DBSMC approval, even though the system was reclassified as a business system in the fiscal year 2006 budget.

⁶⁸GAO-05-381.

Another issue that will affect the degree to which the department complies with the act is whether it relies on system certifications and approvals that preceded the act's requirements. According to financial management investment review board officials, not all of the financial management systems were reviewed in accordance with the fiscal year 2005 act's requirements. More specifically, four business systems that had already been reviewed in accordance with the criteria specified in the defense authorization act for fiscal year 2003 were granted DBSMC approval in August 2005 on the basis of this prior approval. Table 6 shows the specific systems, fiscal year 2006 modernization funding, and the date of the previous approval.

Table 6: Systems Receiving DBSMC Approval under Prior Criteria

Dollars in millions

System	Fiscal year 2006 modernization funding	Date of previous approval
General Fund Enterprise Business System	\$60.1	May 2005
Defense Enterprise Accounting Management System	55.2	February 2005
Nonappropriated Funds Financial Transformation System	9.8	June 2005
Standard Accounting and Reporting System	1.8	May 2005
Total	\$126.9	

Sources: GAO analysis based on DOD data.

However, the act does not provide for DBSMC approval based upon the previous review of a system. The act is specific in terms of what constitutes DBSMC review and approval, and these criteria were not followed for the above four systems. According to financial management investment review board officials, the systems listed in table 6 will go through the current investment review process no later than February 2006.

The department's actions to review and approve business systems investments can be viewed as work in process. According to DOD, it intends to perform the requisite reviews and approvals of all applicable systems before it obligates fiscal year 2006 funds. If it does, it will have complied with the act.

Conclusions

The defense authorization act for fiscal year 2005 contains provisions aimed at strengthening DOD's institutional approach to investing in IT business systems. To varying degrees, the department has satisfied six specific requirements in the act, and thus has made important progress in establishing the kind of fundamental management structures and processes that are needed to correct the long-standing and pervasive IT management weaknesses that have led to our designation of DOD business systems modernization as a high-risk program. This progress provides a foundation upon which to build. However, much more remains to be accomplished to fully satisfy the act and address the department's IT management weaknesses, particularly with regard to sufficiently developing the enterprise architecture and transition plan and ensuring that investment review and approval processes are institutionally implemented. The road map for fully addressing these areas is embedded in our prior recommendations to the department. Therefore, we are not making additional recommendations at this time.

Agency Comments and Our Evaluation

In its written comments on a draft of this report, signed by the Deputy Under Secretary of Defense (Business Transformation) and reprinted in appendix II, the department recognized that our analysis, recommendations, guidance, and educational activities have made us a constructive player in DOD's business transformation efforts. While not commenting on most of the findings in the report, the department also stated that it disagreed with us on two points—the level of development of an “As Is” architecture and consistency within and between the business enterprise architecture and the transition plan.

With respect to the first point, DOD stated that the sheer size and scope of its business operations makes development of a comprehensive “As Is” architecture an ineffective use of time and resources. Instead, according to DOD, while it understood that there needs to be an “easily traceable direct link” between the results of examining its “As Is” conditions and the “To Be” solutions, it maintained that the results of this “As Is” examination are not required to be in the enterprise architecture itself. According to DOD, such “As Is” related work “is more properly aligned with business process review than architecture management.” Notwithstanding these comments, DOD also stated that it was committed to documenting the “As Is” and “To Be” relationship in an appropriate manner.

We agree that both the “As Is” and the “To Be” architectures need to be documented in an appropriate manner. To date, DOD has yet to document its “As Is” architecture in a manner consistent with best practices and federal guidance, and thus we stand by our previous recommendations concerning development of an “As Is” architecture, and we look forward to DOD fulfilling the commitment it made in its comments to address this void in its business enterprise architecture. In this regard, we also agree that developing what the department termed in its comments as a “comprehensive ‘As Is’ architecture” may not be an effective use of time and resources. Accordingly, our prior recommendations for an “As Is” architecture have neither presumed nor prescribed a specific level of comprehensiveness for this “As Is” description, beyond recognizing that it should be defined in accordance with widely accepted best practices and federal guidance. According to these practices and guidance, it should capture the current inventory of enterprise capabilities (in terms of business processes and performance measures) in sufficient scope and detail to permit meaningful analysis of capability gaps in the “To Be” architecture in those areas of the enterprise that are likely to change during the defined transition period. In addition, it should capture descriptions of the information/data, services/applications, and technology environments currently in use, so that transition planning activities can appropriately take into account and address such things as data redundancies, application duplication, shared services, and infrastructure capacity. Our prior recommendations were, however, clear that these “As Is” descriptions should be part of the enterprise architecture (as opposed to what DOD referred to as a business process review), because including such descriptions is a widely accepted best practice and a condition in federal guidance.

With respect to the second point, DOD stated that great effort was made to integrate the business enterprise architecture and the transition plan and that “virtually all” of our examples demonstrating a lack of integration within and between the business enterprise architecture and the transition plan “would be more accurately described as misunderstandings regarding the scope, purpose or intent of the information presented.” It also stated that it was committed to correcting any integration issues.

We agree that considerable effort was made to integrate architecture products and the architecture with the transition plan, and we acknowledge this in the report by stating that the integration of products in this version of the architecture was an improvement over prior versions. However, because our “misunderstandings” arise directly from ambiguity

and inconsistencies in the architecture products and the transition plan that blur their intended meaning, this is clear evidence that a well-defined architecture is needed and that current levels of ambiguity and inconsistency limit the utility and effectiveness of the products as reference tools for guiding and constraining system investment decisions. We agree with DOD that addressing these limitations will create better transformation tools that will benefit all stakeholders, most importantly those within the department.

We are sending copies of this report to interested congressional committees; the Director, Office of Management and Budget; the Secretary of Defense; the Deputy Secretary of Defense; the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense (Comptroller); the Assistant Secretary of Defense (Networks and Information Integration)/Chief Information Officer; the Under Secretary of Defense (Personnel and Readiness); and the Director, Defense Finance and Accounting Service. This report will also be available at no charge on our Web site at <http://www.gao.gov>.

If you or your staff have any questions on matters discussed in this report, please contact me at (202) 512-3439 or hiter@gao.gov, or McCoy Williams at (202) 512-6906 or williamsM1@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix V.



Randolph C. Hite
Director
Information Technology Architecture and Systems Issues



McCoy Williams
Director
Financial Management Assurance

List of Committees

The Honorable John Warner
Chairman
The Honorable Carl Levin
Ranking Minority Member
Committee on Armed Services
United States Senate

The Honorable Ted Stevens
Chairman
The Honorable Daniel K. Inouye
Ranking Minority Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Duncan L. Hunter
Chairman
The Honorable Ike Skelton
Ranking Minority Member
Committee on Armed Services
House of Representatives

The Honorable C.W. Bill Young
Chairman
The Honorable John P. Murtha
Ranking Minority Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

The Honorable Jim Saxton
Chairman
The Honorable Martin T. Meehan
Ranking Minority Member
Subcommittee on Terrorism, Unconventional
Threats and Capabilities
Committee on Armed Services
House of Representatives

Objective, Scope, and Methodology

Our objective was to assess the Department of Defense's (DOD) efforts to comply with the requirements of the defense authorization act for fiscal year 2005.¹ Consistent with the act and as agreed with congressional defense committees' staffs, we evaluated DOD's efforts relative to six provisions in the act: (1) development of an enterprise architecture that includes an information infrastructure enabling DOD to support specific capabilities, such as data standards and system interface requirements; (2) development of a transition plan for implementing the enterprise architecture that includes specific elements, such as the acquisition strategy for new systems; (3) inclusion of business system information in DOD's fiscal year 2006 budget submission; (4) establishment of a business system investment approval and accountability structure; (5) establishment of a business system investment review process; and (6) approval of defense business system investments in excess of \$1 million.

To determine whether the architecture addressed the requirements specified in the act, we reviewed Version 3.0 of the business enterprise architecture, which was approved on September 28, 2005. This review included analyzing relevant criteria to identify the important architecture scope and content and comparing Version 3.0 architecture products to determine whether they provided this scope and content.² In reviewing the products, we specifically focused on principles, business processes, business rules, and standards (e.g., process and data) because relevant criteria recognize that these are fundamental elements of a well-defined and enforceable architecture. In addition, we focused on consistency and completeness among the architecture products and their content (e.g.,

¹Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Public Law 108-375, § 332, 118 Stat. 1811, 1851-1856 (Oct. 28, 2004) (codified in part at 10 U.S.C. § 2222).

²See, for example, DOD, *Department of Defense Architecture Framework*, Version 1.0, Volume 1 (August 2003) and Volume 2 (February 2004); Dennis E. Wisnosky with Joseph Vogel and the other Wizards from Wizdom Systems, Inc., *DoDAF Wizdom: A Practical Guide to Planning, Managing and Executing Projects to Build Enterprise Architectures using the Department of Defense Architecture Framework* (Wizdom Press, 2004-2005); J. A. Zachman, "A Framework for Information Systems Architecture," *IBM Systems Journal* 26, no. 3 (1987); Institute of Electrical and Electronics Engineers, *Standard for Recommended Practice for Architectural Description of Software-Intensive Systems* 1471-2000 (Sept. 21, 2000); Business Process Management Initiative, *Business Process Modeling Notation*, Version 1.0 (May 2004); Ronald G. Ross and Gladys S.W. Lam, *Developing the Business Model: Proteus Business Analysis Workshop*, Fourth Edition (August 2005); and Ronald Ross, *Business Rule Concepts: Getting to the Point of Knowledge* (Business Rule Solutions, LLC, 2005).

operational activities and functions to systems), as well as between the architecture and the transition plan. To do this, we traced linkages between the different architecture products to determine if these linkages had been specifically identified to ensure ease of stakeholder navigation and understanding. We also reviewed the traceability matrix prepared by DOD that documented the mapping of the architecture products to the act and interviewed program officials to obtain an understanding of the methodology used to prepare and validate the information in this matrix. In addition, we interviewed key program officials, including the Special Assistant to Business Transformation, Deputy Under Secretary of Defense (Financial Management), the Director of the Transformation Support Office, the Chief Architect, and the Enterprise Transition Plan Team Lead, to discuss the development and maintenance of the architecture products.

To determine whether the transition plan addresses the requirements specified in the act, we reviewed the transition plan approved on September 28, 2005. This review included determining whether the transition plan included elements specified in the act, such as an acquisition strategy for new systems and a statement of financial and nonfinancial resource needs. We also reviewed the transition plan to ascertain the relationship between the plan and the architecture. We reviewed the traceability matrix prepared by DOD that documented the mapping of the transition plan elements to the act and interviewed program officials to obtain an understanding of the methodology used to prepare and validate the information in this matrix. In addition, we interviewed key program officials, including the Special Assistant to Business Transformation, the Deputy Under Secretary of Defense (Financial Management), the Director of the Transformation Support Office, the Enterprise Transition Plan Team Lead, and the Chief Architect, to discuss the development and maintenance of the plan.

To determine whether DOD's fiscal year 2006 information technology (IT) budget submission was prepared in accordance with the criteria set forth in the act, we reviewed and analyzed DOD's approximately \$30 billion fiscal year 2006 IT budget request. As part of our analysis, we determined what portion of the IT budget request related to DOD business systems. In addition, we compared the fiscal year 2005 and 2006 IT budget requests to determine the systems that were reclassified from business to national security systems, as well as from national security to business systems. We analyzed the 23 system reclassifications by using information in the IT budget requests and the department's business system inventory. We also followed up with DOD officials to ascertain the department's efforts to

address our concerns regarding the reclassification of the 56 systems discussed in our April 2005 report.³ We also reviewed and analyzed the fiscal year 2006 IT budget request to ascertain whether the specific types of funds being requested were explicitly identified and whether an approval authority was designated for each business system.

To determine whether DOD has put in place a specifically defined structure that is responsible and accountable for controlling business systems investments to ensure compliance and consistency with the business enterprise architecture, we reviewed applicable memorandums that had been issued by the department and interviewed cognizant departmental officials.

To determine whether DOD has established investment review structures and processes and issued a standard set of investment review and decision-making criteria, we reviewed applicable policies and procedures issued by the department. In this regard, we reviewed the charter for each of the investment review boards. We also met with representatives from the Financial Management and the Weapon Systems Lifecycle Management and Materiel Supply and Services Management investment review boards to obtain an understanding of the specific roles and responsibilities of the investment review boards. We also obtained an understanding of the tiered accountability approach being followed by the department to help improve its control over business system investments. We also reviewed the department's May 17, 2005, document entitled "Investment Review Process Overview and Concept of Operations for Investment Review Boards."

To determine whether the department had established a process for the review of business system modernizations in excess of \$1 million, we determined whether the department had identified the business systems that were subject to the \$1 million threshold. For the 210 systems that the department identified as subject to the criteria set forth in the act, we reviewed the department's July 2005 guidance entitled "DOD Business Systems Investment Review Proposal Submission Guideline." In addition, we met representatives from the Financial Management and Weapon Systems Lifecycle Management and Materiel Supply and Services Management investment review boards to obtain an understanding of how

³GAO, *DOD Business Systems Modernization: Billions Being Invested without Adequate Oversight*, GAO-05-381 (Washington, D.C.: Apr. 29, 2005).

they used the guidance in the review of the systems that they are accountable for.

We did not independently validate the reliability of the cost and budget figures provided by DOD, because the specific amounts were not relevant to our findings.

We conducted our work at DOD headquarters offices in Arlington, Virginia, from August through November 2005 in accordance with U.S. generally accepted government auditing standards.

Comments from the Department of Defense



ACQUISITION,
TECHNOLOGY
AND LOGISTICS

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

NOV 21 2005

Mr. Randolph C. Hite
Director, Information Technology Architecture and Systems Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Hite:

This is the Department of Defense (DoD) response to the GAO Draft Report GAO-06-219, "DOD BUSINESS SYSTEMS MODERNIZATION: Progress Made in Establishing Foundational Architecture Products and Investment Management Practices, but Much Work Remains" dated November 15, 2005 (GAO Code 310607).

GAO has been a vital partner in our efforts to transform the Department's business operations. Their analysis and recommendations on our plans and activities have provided important learning on best practices and guidance in refining our transformation approach. We appreciate their support, particularly their recognition of the Department's recent progress in laying the groundwork for success. In the two areas outlined below, we disagree with GAO's recommendations and findings:

1. **Creation of an "As Is" Architecture**

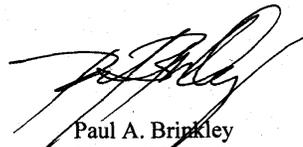
Given the sheer size and scope of the Department's activities, we believe that developing a comprehensive "As Is" architecture would be an ineffective use of time and resources. We fully understand the GAO's concern that there needs to be an easily traceable direct link between the discovery phase's examination of "As Is" conditions and the resulting "To Be" solutions; however, we maintain that this analysis is not required in the architecture itself. Such work is more properly aligned with business process review than architecture management. Regardless, we are committed to working with GAO to arrive at a methodology for documenting the "As Is"- "To Be" relationship that is appropriate to the business conditions found within the Department.



2. **Consistency within and between the Business Enterprise Architecture and Enterprise Transition Plan**

Great efforts were made to fully integrate the various products of the BEA and ETP through unit and integration testing. We are committed to correcting any inconsistencies as they are identified. However, virtually all examples provided by the GAO to demonstrate instances where “product integration was not apparent” would be more accurately described as misunderstandings regarding the scope, purpose or intent of the information presented (many related to understanding the implications of tiered accountability), rather than actual errors. We take these comments as a challenge to better communicate and educate all our stakeholders, including the GAO, on the scope, purpose and use of our transformation tools.

Both of these issues represent opportunities to leverage GAO to assist us in better refining our approach to creating dynamic and easily usable transformation tools. Going forward, as the Department shifts the primary focus of its business transformation efforts from administrative processes and architecture to the achievement of tangible business transformation results, there will be new areas of opportunity for engagement. We welcome GAO’s insights and look forward to their participation in our future efforts.



Paul A. Brinkley
Deputy Under Secretary of Defense,
(Business Transformation)

Summary of Several Architecture Frameworks

Various enterprise architecture frameworks are available for organizations to follow. Although these frameworks differ in their nomenclatures and modeling approaches, they consistently provide for defining an enterprise's operations in both (1) logical terms, such as interrelated business processes and business rules, information needs and flows, and work locations and users, and (2) technical terms, such as hardware, software, data, communications, and security attributes and performance standards. The frameworks also provide for defining these perspectives for both the enterprise's current, or "As Is," environment and its target, or "To Be," environment, as well as a transition plan for moving from the "As Is" to the "To Be" environment.

For example, John A. Zachman developed a structure or framework for defining and capturing an architecture.¹ This framework provides for six windows from which to view the enterprise, which Zachman terms "perspectives" on how a given entity operates: those of (1) the strategic planner, (2) the system user, (3) the system designer, (4) the system developer, (5) the subcontractor, and (6) the system itself. Zachman also proposed six models that are associated with each of these perspectives; these models describe (1) how the entity operates, (2) what the entity uses to operate, (3) where the entity operates, (4) who operates the entity, (5) when entity operations occur, and (6) why the entity operates. Zachman's framework provides a conceptual schema that can be used to identify and describe an entity's existing and planned components and their relationships to one another before beginning the costly and time-consuming efforts associated with developing or transforming the entity.

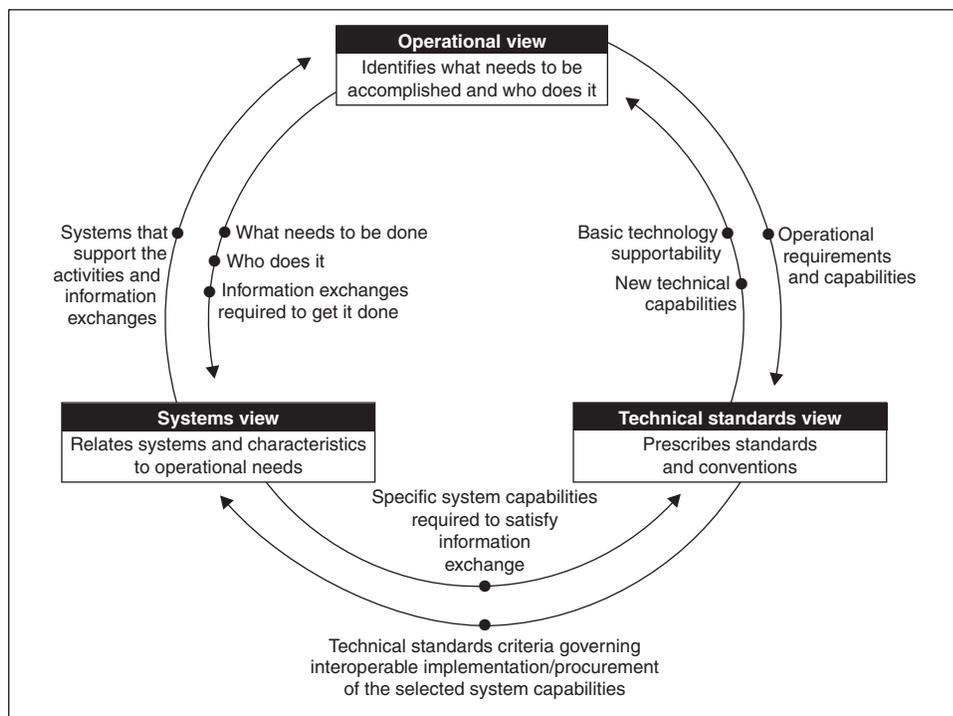
Since Zachman introduced his framework, a number of other frameworks has been proposed. In August 2003, the department released Version 1.0 of the DOD Architecture Framework (DODAF).² The DODAF defines the type and content of the architectural products, as well as the relationships among the products that are needed to produce a useful architecture. (See app. IV for a list of the products prescribed by the DODAF.) Briefly, the framework decomposes an architecture into three primary views:

¹J.A. Zachman, "A Framework for Information Systems Architecture," *IBM Systems Journal* 26, no. 3 (1987).

²DOD, *Department of Defense Architecture Framework*, Version 1.0, Volume 1 (August 2003) and Volume 2 (February 2004).

operational, systems, and technical standards³ (see fig. 1). According to DOD, the three interdependent views are needed to ensure that IT systems support operational needs, and that they are developed and implemented in an interoperable and cost-effective manner.

Figure 1: Interdependent DODAF Views of an Architecture



Source: DOD Architecture Framework Version 1.0, Volume 1.

In September 1999, the federal Chief Information Officer (CIO) Council published the Federal Enterprise Architecture Framework (FEAF), which is intended to provide federal agencies with a common construct on which to base their respective architectures and to facilitate the coordination of common business processes, technology insertion, information flows, and system investments among federal agencies. FEAF describes an approach,

³There are some overarching aspects of architecture that relate to all three of the views. These overarching aspects, such as goals and mission statements and concepts of operations, are captured in the All-view products.

including models and definitions, for developing and documenting architecture descriptions for multiorganizational functional segments of the federal government. Similar to most frameworks, FEAF's proposed models describe an entity's business, the data necessary to conduct the business, applications to manage the data, and technology to support the applications.

In addition, the Office of Management and Budget (OMB) established the Federal Enterprise Architecture (FEA) Program Management Office to develop a federated enterprise architecture in the context of five "reference models, and a security and privacy profile that overlays the five models."

- The Business Reference Model is intended to describe the federal government's businesses, independent of the agencies that perform them. This model consists of four business areas: (1) services for citizens, (2) mode of delivery, (3) support delivery of services, and (4) management of government resources. It serves as the foundation for the FEA. OMB expects agencies to use this model, as part of their capital planning and investment control processes, to help identify opportunities to consolidate IT investments across the federal government. Version 2.0 of this model was released in June 2003.
- The Performance Reference Model is intended to describe a set of performance measures for major IT initiatives and their contribution to program performance. According to OMB, this model will help agencies produce enhanced performance information; improve the alignment and better articulate the contribution of inputs, such as technology, to outputs and outcomes; and identify improvement opportunities that span traditional organizational boundaries. Version 1.0 of this model was released in September 2003.
- The Service Component Reference Model is intended to identify and classify IT service (i.e., application) components that support federal agencies and promote the reuse of components across agencies. This model is intended to provide the foundation for the reuse of applications, application capabilities, components (defined as "a self-contained business process or service with predetermined functionality that may be exposed through a business or technology interface"), and business services. According to OMB, this model is a business-driven, functional framework that classifies service components with respect to how they support business or performance objectives. Version 1.0 of this model was released in June 2003.

- The Data Reference Model is intended to describe, at an aggregate level, the types of data and information that support program and business line operations and the relationships among these types. This model is intended to help describe the types of interactions and information exchanges that occur across the federal government. Version 1.0 of this model was released in September 2004.
- The Technical Reference Model is intended to describe the standards, specifications, and technologies that collectively support the secure delivery, exchange, and construction of service components. Version 1.1 of this model was released in August 2003.
- The Security and Privacy Profile is intended to provide guidance on designing and deploying measures that ensure the protection of information resources. OMB has released Version 1.0 of the profile.

List of the DOD Architecture Framework Products

Product	Product title	Product description
All view (AV)		
AV-1	Overview and Summary Information	Executive-level summary information on the scope, purpose, and context of the architecture
AV-2	Integrated Dictionary	Architecture data repository with definitions of all terms used in all products
Operational view (OV)		
OV-1	High-Level Operational Concept Graphic	High-level graphical/textual description of what the architecture is supposed to do, and how it is supposed to do it
OV-2	Operational Node Connectivity Description	Graphic depiction of the operational nodes (or organizations) with needlines that indicate a need to exchange information
OV-3	Operational Information Exchange Matrix	Information exchanged between nodes and the relevant attributes of that exchange
OV-4	Organizational Relationships Chart	Command structure or relationships among human roles, organizations, or organization types that are the key players in an architecture
OV-5	Operational Activity Model	Operations that are normally conducted in the course of achieving a mission or a business goal, such as capabilities, operational activities (or tasks), input and output flows between activities, and input and output flows to/from activities that are outside the scope of the architecture
OV-6a	Operational Rules Model	One of three products used to describe operational activity—identifies business rules that constrain operations
OV-6b	Operational State Transition Description	One of three products used to describe operational activity—identifies business process responses to events
OV-6c	Operational Event-Trace Description	One of three products used to describe operational activity—traces actions in a scenario or sequence of events
OV-7	Logical Data Model	Documentation of the system data requirements and structural business process rules of the operational view
Systems view (SV)		
SV-1	Systems Interface Description	Identification of systems nodes, systems, and systems items and their interconnections, within and between nodes
SV-2	Systems Communications Description	Specific communications links or communications networks and the details of their configurations through which systems interface
SV-3	Systems-Systems Matrix	Relationships among systems in a given architecture; can be designed to show relationships of interest (e.g., system-type interfaces, planned versus existing interfaces)
SV-4	Systems Functionality Description	System functional hierarchies and system functions, and the system data flow between them
SV-5	Operational Activity to Systems Function Traceability Matrix	Mapping of relationships between the set of operational activities and the set of system functions applicable to that architecture
SV-6	Systems Data Exchange Matrix	Characteristics of the system data exchanged between systems
SV-7	Systems Performance Parameters Matrix	Quantitative characteristics of systems and systems hardware/software items, their interfaces, and their functions

Appendix IV
List of the DOD Architecture Framework
Products

(Continued From Previous Page)

Product	Product title	Product description
SV-8	Systems Evolution Description	Planned incremental steps toward migrating a suite of systems to a more efficient suite, or toward evolving a current system to a future implementation
SV-9	Systems Technology Forecast	Emerging technologies and software/hardware products that are expected to be available in a given set of time frames and that will affect future development of the architecture
SV-10a	Systems Rules Model	One of three products used to describe system functionality—identifies constraints that are imposed on systems functionality due to some aspect of systems design or implementation
SV-10b	Systems State Transition Description	One of three products used to describe system functionality—identifies responses of a system to events
SV-10c	Systems Event-Trace Description	One of three products used to describe system functionality—lays out the sequence of system data exchanges that occur between systems (external and internal), system functions, or human role for a given scenario
SV-11	Physical Schema	Physical implementation of the Logical Data Model entities (e.g., message formats, file structures, and physical schema)
Technical standards view (TV)		
TV-1	Technical Standards Profile	Listing of standards that apply to SV elements in a given architecture
TV-2	Technical Standards Forecast	Description of emerging standards and the potential impact on current systems view elements, within a set of time frames

Source: DOD.

GAO Contact and Staff Acknowledgments

GAO Contact

Randolph C. Hite, (202) 512-3439 or hiter@gao.gov

McCoy Williams, (202) 512-6906 or williamsM1@gao.gov

Acknowledgments

In addition to the contacts named above, key contributors to this report were Cynthia Jackson and Darby Smith, Assistant Directors, and Beatrice Alff, Barbara Collier, Francine DelVecchio, Neelaxi Lakhmani, Anh Le, Mai Nguyen, Tarunkant Mithani, Freda Paintsil, Randolph Tekeley, and William Wadsworth.

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 Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548